UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW JERSEY

M.Z., on behalf of herself and all others Similarly situated, Plaintiffs v. CENTRASTATE HEALTHCARE SYSTEM, INC. Serve Registered Agent: Kim Morin 901 W Main Street Freehold, NJ 07728 and SHAUNNA ELLISON Serve at: 901 W Main Street Freehold, NJ 07728, Defendants.	)	Case No.: 23-cv-1049

CLASS ACTION COMPLAINT FOR DAMAGES

COME NOW M.Z., on behalf of herself, individually, and on behalf of all others similarly situated ("Plaintiffs"), for their Class Action Complaint for Damages against Defendants CentraState Healthcare System, Inc. (hereinafter "CentraState") and Shaunna Ellison (hereinafter sometimes referred to as

"Ellison" and/or "Defendant Ellison") and respectfully state and allege as follows:

NATURE OF THE CASE

1. This is a class action brought by Plaintiff, individually and on behalf of all others similarly situated (i.e. the Class Members) seeking to redress Defendants' willful and reckless violations of their privacy rights. Plaintiff was a patient of Defendant CentraState who entrusted her Protected Health Information ("PHI") and Personally Identifiable Information ("PII") to Defendants. Defendants betrayed Plaintiff's trust by failing to properly safeguard and protect her PHI and PII and publicly disclosing her PHI and PII without authorization in violation of New Jersey common law.

2. This action pertains to Defendants' unauthorized disclosure of the Plaintiff's and other Class Members' PHI and PII that occurred on or around December 29, 2022 (the "Breach").

3. Defendant disclosed Plaintiff's and other Class Members' PHI and PII to unauthorized persons as a direct and/or proximate result of Defendants' failure to safeguard and protect her PHI and PII.

4. The wrongfully disclosed PHI and PII included, *inter alia*, Plaintiff's name, address, date of birth, telephone numbers, patient account numbers, email addresses, and other medical information.

5. Defendants flagrantly disregarded Plaintiff's and other Class Members' privacy and property rights by intentionally, willfully, and recklessly failing to take the necessary precautions required to safeguard and protect Plaintiff's and other Class Members' PHI and PII from unauthorized disclosure. Plaintiff's and other Class Members' PHI and PII was improperly handled, inadequately protected, and not kept in accordance with basic security protocols. Defendants' obtaining of the information and sharing of same also represent a flagrant disregard of Plaintiff's and other Class Members' rights, both as to privacy and property.

6. During the Breach, CentraState maintained its medical record systems in a condition vulnerable to unknown, unsupervised, and unauthorized access by people with neither the required right of nor the need to access those records. This resulted in the improper access and disclosure of Plaintiff's PHI and PII. Upon information and belief, the mechanisms of the unauthorized disclosures of the PHI and PII were known risks to CentraState, and, thus, CentraState was on notice that failing to take steps necessary to secure its medical record systems from those risks left that property in a dangerous condition.

7. Armed with the information accessed in the Breach, information thieves can commit a variety of bad acts including, *inter alia*, opening new financial accounts in Plaintiff's and other Class Members' name, taking out loans

in Plaintiff's and other Class Members' name, using Plaintiff's and other Class Members' name to obtain medical services, using Plaintiff's health information to target other phishing and hacking intrusions based on their individual health needs, using Plaintiff's and other Class Members' information to obtain government benefits and filing fraudulent tax returns using Plaintiff's and other Class Members' information.

8. Because of the Breach, Plaintiff and other Class Members no longer have autonomy and control over their medical and treatment histories. They have no idea who may now have access to this information.

9. As a further consequence of the Breach, Plaintiff and other Class Members have been exposed to a heightened and imminent risk of fraud and identity theft. Plaintiff and other Class Members must now and in the future closely monitor their financial accounts to guard against identity theft.

10. Plaintiff and other Class Members may also incur out of pocket costs for, e.g., purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

11. Plaintiff and other Class Members have standing to bring this action because as a direct and/or proximate result of Defendant's wrongful actions and/or inaction and the resulting Breach, Plaintiff has incurred (and will continue to incur) damages in the form of, *inter alia*, (i) loss of privacy and/or (ii) the

additional damages set forth in detail below, which are incorporated herein by reference.

12. Defendants' wrongful actions and/or inaction and the resulting Breach have ultimately placed Plaintiff at an imminent, immediate and continuing increased risk of identity theft, identity fraud and medical fraud. Indeed, Javelin Strategy & Research ("Javelin"), a leading provider of quantitative and qualitative research, released its 2012 Identity Fraud Report ("the Javelin Report"), quantifying the impact of data breaches. According to the Javelin Report, individuals whose PII is subject to a reported data breach—such as the Data Breach at issue here—are approximately 9.5 times more likely than the general public to suffer identity fraud and/or identity theft. Moreover, there is a high likelihood that significant identity fraud and/or identity theft has not yet been discovered or reported, and a high probability that criminals who may now possess Plaintiff's PII and not yet used the information will do so at a later date or re-sell it.

13. Plaintiff and other Class Members have also suffered and are entitled to damages for the lost benefit of their bargain with Defendants. Plaintiff and other Class Members paid Defendants for their services, which included protecting their PII and PHI. The lost benefit of the bargain is measured by the difference between the value of what Plaintiff should have received when they

paid for their services, and the value of what they actually did receive: services without adequate privacy safeguards. Plaintiff has been harmed in that they: (1) paid more for privacy and confidentiality than they otherwise would have, and, (2) paid for privacy protections they did not receive. In that respect, Plaintiff has not received the benefit of the bargain and has suffered an ascertainable loss.

14. Additionally, because of Defendants' conduct, Plaintiff and other Class Members have been harmed in that Defendants have breached its common law fiduciary duty of confidentiality owed to Plaintiff and other Class Members.

15. Accordingly, Plaintiff and other Class Members seek redress against Defendants for the various counts set forth in this Petition.

16. Plaintiff and other Class Members seek all (i) actual damages, economic damages, and/or nominal damages, (ii) injunctive relief, and (iii) attorneys' fees, litigation expenses, costs and any applicable prejudgment and post-judgment interest.

JURISDICTION AND VENUE

17. Plaintiffs were first injured by conduct occurring in Monmouth County, New Jersey.

18. This Court has diversity jurisdiction over this action under the Class Action Fairness Act (CAFA), 28 U.S.C. § 1332(d) because this is a class action involving more than 100 class members, the amount in controversy exceeds

$5,000,000, exclusive of interest and costs, and Plaintiffs and members of the Class are citizens of states that differ from Defendant.

19. Venue is proper in the District of New Jersey, pursuant to 28 U.S. Code § 1391 because the acts complained of occurred and Defendant are located in the District of New Jersey.

PARTIES

20. Plaintiff M.Z. is an adult residing in Dunwoody, Georgia and is a citizen of Georgia. She was a patient of CentraState when it collected and received Protected Information that CentraState then maintained in its database, email, computer systems, and other medical records systems. M.Z.'s Protected Information was compromised in the Breach.

21. Subject matter jurisdiction in this civil action is authorized pursuant to 28 U.S.C. § 1332(d) because there are more than 100 Class Members, at least one class member is a citizen of a state different from that of Defendant, and the amount in controversy exceeds $5 million, exclusive of interest and costs.

22. Defendant CentraState at all relevant times, was doing business as CentraState and operated a hospital and clinics in various parts of New Jersey. It has the capacity to be sued.

23. Defendant CentraState is an entity organized and existing under the laws of the State of New Jersey. It has the capacity to be sued. CentraState also does business throughout the state of CentraState under a variety of names.

CLASS ACTION ALLEGATIONS

24. Pursuant to Rule 23 of the Federal Rules of Civil Procedure, Plaintiff brings this action on behalf of herself and the following proposed Nationwide Class, defined as follows:

Nationwide Class

> All persons residing in the United States who are current or former patients of CentraState or any CentraState affiliate, parent, or subsidiary, and had their PII compromised by an unknown third-party cybercriminal as a result of the Data Breach.

In addition, Plaintiff brings this action on behalf of the following proposed New Jersey Subclass, defined as follows:

New Jersey Subclass

25. Both the proposed Nationwide Class and the proposed New Jersey Subclass will be collectively referred to as the Class, except where it is necessary to differentiate them.

26. Excluded from the proposed Class are any officer or director of Defendant; any officer or director of any affiliate, parent, or subsidiary of CentraState; anyone employed by counsel in this action; and any judge to whom

this case is assigned, his or her spouse, and members of the judge's staff.

27. **Numerosity.** Members of the proposed Class likely number in the tens of thousands and are thus too numerous to practically join in a single action. Membership in the Class is readily ascertainable from Defendant's own records.

28. **Commonality and Predominance.** Common questions of law and fact exist as to all proposed Class Members and predominate over questions affecting only individual Class Members. These common questions include:

(i) Whether Defendant engaged in the wrongful conduct alleged herein;

(ii) Whether Defendant's inadequate data security measures were a cause of the Data Breach;

(iii) Whether Defendant owed a legal duty to Plaintiff and the other Class Members to exercise due care in collecting, storing, and safeguarding their PII;

(iv) Whether Defendant negligently or recklessly breached legal duties owed to Plaintiff and the Class Members to exercise due care in collecting, storing, and safeguarding their PII;

(v) Whether Plaintiff and the Class are at an increased risk for identity theft because of the Data Breach;

(vi) Whether Defendant failed to implement and maintain reasonable security procedures and practices for Plaintiff's and Class Members' PII in violation Section 5 of the FTC Act;

(vii) Whether Plaintiff and the other Class Members are entitled to actual, statutory, or other forms of damages, and other monetary relief; and

(viii) Whether Plaintiff and the other Class Members are entitled to equitable relief, including, but not limited to, injunctive relief and restitution.

29. Defendant engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiff individually and on behalf of the other Class Members. Similar or identical statutory and common law violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quantity and quality, to the numerous questions that dominate this action.

30. **Typicality:** Plaintiff's claims are typical of the claims of the Members of the Class. All Class Members were subject to the Data Breach and had their PII accessed by and/or disclosed to unauthorized third parties. Defendant's misconduct affected all Class Members in the same manner.

31. **Adequacy of Representation:** Plaintiff is an adequate representative of the Class because their interests do not conflict with the interests of the other Class Members they seek to represent; they have retained counsel competent and experienced in complex class action litigation, and Plaintiff will prosecute this action vigorously. The interests of the Class will be fairly and adequately protected by Plaintiff and their counsel.

32. **Superiority:** A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this matter as a class action. The damages, harm, or other financial detriment suffered individually by Plaintiff and

the other Class Members are relatively small compared to the burden and expense that would be required to litigate their claims on an individual basis against Defendant, making it impracticable for Class Members to individually seek redress for Defendant's wrongful conduct. Even if Class Members could afford individual litigation, the court system could not. Individualized litigation would create a potential for inconsistent or contradictory judgments and increase the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court.

BACKGROUND FACTS

33. CentraState is a health care provider pursuant to state and federal law, providing health care and medical services to the general public throughout the State of New Jersey.

34. Plaintiffs and the Class Members are patients of CentraState. As a part of its business operations, CentraState collects and maintains PHI and PII of its patients.

35. Plaintiff and other Class Members were patients of CentraState and, as a result, provided their PHI and PII to CentraState.

36. Plaintiff and other Class Members entered into a contract or an implied contract with CentraState for the adequate protection of their PHI and PII.

37. CentraState is required to maintain the strictest privacy and confidentiality of Plaintiffs' medical records and other PHI and PII.

38. All of CentraState's patients (and those of its related entities) are required to agree to the terms of a "Consent and Agreement." The parties to those contracts exchange mutual promises regarding CentraState's provision of health care. Among the terms of that agreement is a specific incorporation of CentraState's Notice of Privacy Practices.

39. CentraState outlines its Duties in its online HIPAA Privacy Practices.[1]

40. CentraState's HIPAA Privacy Practices acknowledges CentraState's duty to keep patients' Protected Information private.

41. CentraState further had obligations created by HIPAA, industry standards, common law, and other representations made to Plaintiff, to keep their PHI and PII confidential and to protect it from unauthorized access and disclosure.

42. Plaintiff and other Class Members provided their PHI and PII to CentraState with the reasonable expectation and mutual understanding that CentraState would comply with their obligations to keep such information confidential and secure from unauthorized access and disclosure.

[1] https://www.centrastate.com/hipaa-privacy-practices/

43. CentraState's medical records security obligations were particularly important given the substantial increase in information security failures in the healthcare industry preceding the date of the Breach. The increase in personal and medical information security failures – and the attendant risks of the same – was widely known to the public and to anyone in CentraState's industry, including CentraState.

44. On or about December 29, 2022, Defendant discovered that Plaintiffs' PHI and PII was disclosed to unauthorized criminal third parties in the Breach.

45. On or about February 8, 2023 Plaintiff M.Z. received a letter from CentraState confirming, "[o]n December 29, 2022, CentraState detected unusual activity involving our computer systems. We immediately took steps to contain the incident and initiated an investigation which included a forensics form. We also reported the incident to law enforcement including the Federal Bureau of Investigation…"

46. Plaintiffs' PHI and PII was compromised in the Breach.

47. The disclosure of the PHI and PII at issue was a result of CentraState's inadequate safety and security protocols governing PHI and PII.

48. The wrongfully disclosed PHI and PII included, *inter alia*, Plaintiff's and other Class Members' names, addresses, dates of birth, other demographic

information, medical record numbers, treatment and other clinical information and/or radiological images.

49. Upon information and belief, the Breach affected many of CentraState's patients and their parents/guardians.

50. As a direct and/or proximate result of CentraState's failure to properly safeguard and protect the PHI and PII of its patients and their parents/guardians, Plaintiff's and other Class Members' PHI and PII was stolen, compromised, and wrongfully disseminated without authorization.

51. CentraState had a duty to its patients to protect them from wrongful disclosures.

52. As a health care provider, CentraState is required to train and supervise its employees regarding the policies and procedures as well as the State and Federal laws for safeguarding patient information.

53. CentraState is a covered entity(ies) pursuant to the Health Insurance Portability and Accountability Act ("HIPAA"). *See* 45 C.F.R. § 160.102. CentraState 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.

54. CentraState is a covered entity(ies) pursuant to the Health Information Technology Act ("HITECH")[2]. *See* 42 U.S.C. § 17921, 45 C.F.R. § 160.103.

[2] HIPAA and HITECH work in tandem to provide guidelines and rules for maintaining protected health

55. The HIPAA and HITECH rules work in conjunction with the already established laws of privacy New Jersey. HIPAA and HITECH do not recognize an individual right of claim for violation but provide the guidelines for the standard of procedure dictating how patient medical information should be kept private.

56. HIPAA's Privacy Rule, otherwise known as "Standards for Privacy of Individually Identifiable Health Information," establishes national standards for the protection of health information.

57. HIPAA's Security Rule, otherwise known as "Security Standards for the Protection of Electronic Protected Health Information," establishes national security standards for the protection of health information that is held or transferred in electronic form. See 42 C.F.R. §§ 164.302-164.318.

58. HIPAA limits the permissible uses of "protected health information" and prohibits the unauthorized disclosure of "protected health information." 45 C.F.R. § 164.502. HIPAA requires that covered entities implement appropriate administrative, technical, and physical safeguards for this information and requires that covered entities reasonably safeguard protected health information from any intentional or unintentional use or disclosure that is in violation of the standards,

information. HITECH references and incorporates HIPAA.

implementation specifications or other requirements of this subpart. *See* 45 C.F.R. § 164.530(c).

59. HIPAA requires a covered entity to have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the covered entity or the requirements of 45 C.F.R. Part 164, Subparts D or E. *See* 45 C.F.R. § 164.530(e).

60. HIPAA requires a covered entity to mitigate, to the extent practicable, any harmful effect that is known to the covered entity of a use or disclosure of protected health information in violation of its policies and procedures or the requirements of 45 C.F.R. Part 164, Subpart E by the covered entity or its business associate. *See* 45 C.F.R. § 164.530(f).

61. Under HIPAA:

> Protected health information means individually identifiable health information:
>
> (1) Except as provided in paragraph (2) of this definition, that is:
>
> (i) Transmitted by electronic media;
>
> (ii) Maintained in electronic media; or
>
> (iii) Transmitted or maintained in any other form or medium.[3]

[3] 45 C.F.R. § 160.103.

62. HIPAA and HITECH obligated CentraState to implement technical policies and procedures for electronic information systems that maintain electronic protected health information so that such systems were accessible only to those persons or software programs that had been granted access rights and who have a working need to access and view the information. *See* 45 C.F.R. § 164.312(a)(1); *see also* 42 U.S.C. § 17902.

63. HIPAA and HITECH also obligated CentraState to implement policies and procedures to prevent, detect, contain, and correct security violations, and to protect against uses or disclosures of electronic protected health information that are reasonably anticipated but not permitted by the privacy rules. *See* 45 C.F.R. § 164.306(a)(1) and § 164.306(a)(3); *see also* 42 U.S.C. § 17902.

64. HIPAA further obligated CentraState to ensure that its workforce complied with HIPAA security standard rules (*see* 45 C.F.R. § 164.306(a)(4)) to effectively train its workforces on the policies and procedures with respect to protected health information, as necessary and appropriate for those individuals to carry out their functions and maintain the security of protected health information. *See* 45 C.F.R. § 164.530(b)(1).

65. HIPAA also requires the Office of Civil Rights ("OCR"), within the Department of Health and Human Services ("HHS"), to issue annual guidance documents on the provisions in the HIPAA Security Rule. *See* 45 C.F.R. §§ 164.302-

164.318. For example, "HHS has developed guidance and tools to assist HIPAA covered entities in identifying and implementing the most cost effective and appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of e-PHI and comply with the risk analysis requirements of the Security Rule." *See* US Department of Health & Human Services, Security Rule Guidance Material.[4] The list of resources includes a link to guidelines set by the National Institute of Standards and Technology (NIST), which OCR says, "represent the industry standard for good business practices with respect to standards for securing e-PHI." *See* US Department of Health & Human Services, Guidance on Risk Analysis.[5]

66. Should a health care provider experience an unauthorized disclosure, it is required to conduct a Four Factor Risk Assessment (HIPAA Omnibus Rule). This standard requires, "A covered entity or business associate must now undertake a four-factor risk assessment to determine whether or not PHI has been compromised and overcome the presumption that the breach must be reported." The four-factor risk assessment focuses on:

[4] http://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html.

[5] https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html.

(1) the nature and extent of the PHI involved in the incident (e.g., whether the incident involved sensitive information like social security numbers or infectious disease test results);

(2) the recipient of the PHI;

(3) whether the PHI was actually acquired or viewed; and,

(4) the extent to which the risk that the PHI was compromised has been mitigated following unauthorized disclosure (e.g., whether it was immediately sequestered and destroyed)."[6]

67. The HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, requires HIPAA covered entities and their business associates to provide notification following a breach of unsecured protected health information.

68. The HIPAA Contingency Operations Rule, 45 C.F.R. §164.301(a), requires a healthcare provider to have security measures in place and train its employees and staff so that all its staff and employees know their roles in facility security.

69. In addition, CentraState had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45 ("FTCA"), which prohibits "unfair or deceptive acts or practices in or affecting

[6] 78 Fed. Reg. 5641-46; *see also* 45 C.F.R. § 164.304.

commerce," including, as interpreted and enforced by the Federal Trade Commission, the unfair practice of failing to use reasonable measures to protect confidential information.

70. CentraState failed to conduct or improperly conducted the four-factor risk assessment following the unauthorized disclosure.

71. As a direct and/or proximate result of CentraState's wrongful actions and/or inaction and the resulting Breach, the criminal(s) and/or their customers now have Plaintiff's compromised PHI and PII.

72. There is a robust international market for the purloined PHI and PII, specifically medical information. CentraState's wrongful actions and/or inaction and the resulting Breach have also placed Plaintiff at an imminent, immediate and continuing increased risk of identity theft, identity fraud[7] and medical fraud.

73. Identity theft occurs when someone uses an individual's PHI and PII, such as the person's name, Social Security number, or credit card number, without the individual's permission, to commit fraud or other crimes. *See* Federal Trade Commission, Fighting Back against Identity Theft.[8] The Federal Trade Commission

[7] According to the United States Government Accounting Office (GAO), the terms "identity theft" or "identity fraud" are broad terms encompassing various types of criminal activities. Identity theft occurs when PII is used to commit fraud or other crimes. These crimes include, *inter alia,* credit card fraud, phone or utilities fraud, bank fraud and government fraud (theft of government services).

[8] https://consumer.ftc.gov/consumer-alerts/2019/01/fight-back-against-tax-identity-theft.

estimates that the identities of as many as nine million Americans are stolen each year.

74. The Federal Trade Commission correctly sets forth that, "Identity theft is serious. While some identity theft victims can resolve their problems quickly, others spend hundreds of dollars and many days repairing damage to their good name and credit record. Some consumers victimized by identity theft may lose out on job opportunities, or be denied loans for education, housing or cars because of negative information on their credit reports. In rare cases, they may even be arrested for crimes they did not commit." *Id.*

75. Identity theft crimes often involve more than just crimes of financial loss, such as various types of government fraud (such as obtaining a driver's license or official identification card in the victim's name but with their picture), using a victim's name and Social Security number to obtain government benefits and/or filing a fraudulent tax return using a victim's information. Identity thieves also obtain jobs using stolen Social Security numbers, rent houses and apartments and/or obtain medical services in a victim's name. Identity thieves also have been known to give a victim's PHI and PII to police during an arrest, resulting in the issuance of an arrest warrant in the victim's name and an unwarranted criminal record.

76. According to the FTC, "the range of privacy-related harms is more expansive than economic or physical harm or unwarranted intrusions and that any

privacy framework should recognize additional harms that might arise from unanticipated uses of data."[9] Furthermore, there is significant evidence demonstrating that technological advances and the ability to combine disparate pieces of data can lead to identification of a consumer, computer or device even if the individual pieces of data do not constitute PII.[10]

77. According to the Javelin Report, in 2011, the mean consumer cost of rectifying identity fraud was $354 while the mean resolution time of identity fraud was 12 hours. Javelin Report, *supra*, at 6. In 2011, the consumer cost for new account fraud and existing non-card fraud increased 33% and 50% respectively. *Id.* at 9. Consumers who received a data breach notification had a fraud incidence rate of 19% in 2011 and, of those experiencing fraud, 43% reported their credit card numbers were stolen and 22% of the victims reported their debit card numbers were stolen. *Id.* at 10. More important, consumers who were notified that their PHI and PII had been breached were 9.5 times more likely to experience identity fraud than consumers who did not receive such a notification. *Id.* at 39.

---

[9] *Protecting Consumer Privacy in an Era of Rapid Change* FTC, Report March 2012 https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

[10] *See Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers*, *Preliminary FTC Staff Report*, 35-38 (Dec. 2010), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-bureau-consumer-protection-preliminary-ftc-staff-report-protecting-consumer/101201privacyreport.pdf.

78. The unauthorized disclosure of a person's Social Security number can be particularly damaging since Social Security numbers cannot be easily replaced like a credit card or debit card. In order to obtain a new Social Security number, a person must show evidence that someone is using the number fraudulently or is being disadvantaged by the misuse. *See* Identity Theft and Your Social Security Number, SSA Publication No. 05-10064.[11] Thus, a person whose PII has been stolen cannot obtain a new Social Security number until the damage has already been done.

79. Obtaining a new Social Security number also is not an absolute prevention against identity theft. Government agencies, private businesses and credit reporting companies likely still have the person's records under the old number, so using a new number will not guarantee a fresh start. For some victims of identity theft, a new number may actually create new problems; because prior positive credit information is not associated with the new Social Security number, it is more difficult to obtain credit due to the absence of a credit history.

80. Medical fraud (or medical identity theft) occurs when a person's personal information is used without authorization to obtain, or receive payment for, medical treatment, services or goods. *See* Federal Trade Commission, What to Know About Medical Identity Theft.[12] Victims of medical identity theft may find that their

[11] https://www.ssa.gov/pubs/EN-05-10064.pdf.
[12] https://consumer.ftc.gov/articles/what-know-about-medical-identity-theft.

medical records are inaccurate, which can have a serious impact on their ability to obtain proper medical care and insurance benefits.

81. CentraState flagrantly disregarded and/or violated Plaintiff's and other Class Members' privacy and property rights, and harmed her in the process, by not obtaining Plaintiff's prior written consent to disclose their PHI and PII to any other person—as required by laws, regulations, industry standards and/or internal company standards.

82. CentraState flagrantly disregarded and/or violated Plaintiff's and other Class Members' privacy and property rights, and harmed them in the process, by failing to safeguard and protect and, in fact, wrongfully disseminating Plaintiff's PHI and PII to unauthorized persons.

83. Upon information and belief, CentraState flagrantly disregarded and/or violated Plaintiff's privacy and property rights, and harmed them in the process, by failing to keep or maintain an accurate accounting of the PHI and PII wrongfully disclosed in the Breach.

84. CentraState flagrantly disregarded and/or violated Plaintiff's privacy rights, and harmed her in the process, by failing to establish and/or implement appropriate administrative, technical and/or physical safeguards to ensure the security and confidentiality of Plaintiff's PHI and PII to protect against anticipated threats to the security or integrity of such information. CentraState's unwillingness

or inability to establish and maintain the proper information security procedures and controls is an abuse of discretion and confirms its intentional and willful failure to observe procedures required by law, industry standards and/or their own internal policies and procedures.

85. Because of CentraState's failure to adequately apply security controls to its medical records systems, one or more unauthorized employees were able to easily gain access to the sensitive information of thousands of CentraState patients – even though the individual(s) were not authorized to access such information.

86. The unauthorized employee(s) were presumably supervised in some capacity. Nevertheless, these employee(s) were able to access Plaintiff's PHI and PII when such information had nothing to do with the employees' job responsibilities and duties.

87. The actual harm and adverse effects to Plaintiff, including the imminent, immediate and continuing increased risk of harm for identity theft, identity fraud and/or medical fraud directly and/or proximately caused by CentraState above wrongful actions and/or inaction and the resulting Breach requires Plaintiff to take affirmative acts to recover her peace of mind, and personal security including, without limitation, purchasing credit reporting services, purchasing credit monitoring and/or internet monitoring services, frequently obtaining, purchasing and reviewing credit reports, bank statements, and other similar information,

instituting and/or removing credit freezes and/or closing or modifying financial accounts – for which there is a financial and temporal cost. Plaintiff has suffered, and will continue to suffer, such damages for the foreseeable future.

88. Victims and potential victims of identity theft, identity fraud and/or medical fraud – such as Plaintiff– typically spend hundreds of hours in personal time and hundreds of dollars in personal funds to resolve credit and other financial issues resulting from data breaches. According to the Javelin Report, not only is there a substantially increased risk of identity theft and identity fraud for data breach victims, those who are further victimized by identity theft or identity fraud will incur an average fraud-related economic loss of $1,513 and incur an average of $354 of out-of-pocket expenses attempting to rectify the situation. Javelin Report, *supra*, at 6.

89. Other statistical analyses are in accord. The GAO found that identity thieves use PII to open financial accounts and payment card accounts and incur charges in a victim's name. This type of identity theft is the "most damaging" because it may take some time for the victim to become aware of the theft, in the meantime causing significant harm to the victim's credit rating and finances. Moreover, unlike other PHI and PII, Social Security numbers are incredibly difficult to change and their misuse can continue for years into the future. The GAO states

that victims of identity theft face "substantial costs and inconvenience repairing damage to their credit records," as well the damage to their "good name."

90. CentraState's wrongful actions and/or inaction directly and/or proximately caused the theft and dissemination into the public domain of Plaintiff's PHI and PII without her knowledge, authorization and/or consent. As a direct and/or proximate result of CentraState's wrongful actions and/or inaction and the resulting Breach, Plaintiff has incurred (and will continue to incur) damages in the form of, *inter alia*, (i) loss of privacy, (ii) the imminent, immediate and continuing increased risk of identity theft, identity fraud and/or medical fraud, (iii) out-of-pocket expenses to purchase credit monitoring, internet monitoring, identity theft insurance and/or other Breach risk mitigation products, (iv) out-of-pocket expenses incurred to mitigate the increased risk of identity theft, identity fraud and/or medical fraud pressed upon them by the Breach, including the costs of placing a credit freeze and subsequently removing a credit freeze, (v) the value of their time spent mitigating the increased risk of identity theft, identity fraud and/or medical fraud pressed upon them by the Breach, (vi) the lost benefit of their bargain when they paid for their privacy to be protected and it was not, and (vii) emotional distress.

COUNT I
BREACH OF CONTRACT

91. The previous paragraphs are incorporated as if fully stated in this Count.

92. Plaintiff and other Class Members, as part of their agreements with Defendant, provided Defendant their PHI and PII.

93. CentraState solicited and invited Plaintiff and other Class Members to provide PHI and PII as part of CentraState's regular business practices. Plaintiff and other Class Members accepted CentraState's offers and provided their PHI and PII to CentraState.

94. In providing such PHI and PII, Plaintiff and other Class Members entered into an implied contract with CentraState, whereby CentraState became obligated to reasonably safeguard Plaintiff's and other Class Members' PHI and PII.

95. Under the contract, CentraState was obligated to not only safeguard the PHI and PII, but also to provide Plaintiff and other Class Members with prompt, adequate notice of any Data Breach or unauthorized access of said information.

96. Plaintiff and other Class Members, who paid money to CentraState, reasonably believed and expected that CentraState would use part of those funds to obtain adequate information security. CentraState failed to do so.

97. Plaintiff and other Class Members fully and adequately performed their obligations under the contracts with CentraState.

98. CentraState breached the implied contract with Plaintiff and other Class Members by failing to take reasonable measures to safeguard their PHI and PII.

99. Plaintiff and other Class Members suffered and will continue to suffer

damages including, but not limited to: (i) the untimely and/or inadequate notification of the Breach; (ii) improper disclosure of their PHI and PII; (iii) loss of privacy; (iv) out-of-pocket expenses incurred to mitigate the increased risk of identity theft and/or identity fraud pressed upon them by the Breach; (v) the value of their time spent mitigating identity theft and/or identity fraud and/or the increased risk of identity theft and/or identity fraud; and, (vi) the increased risk of identity theft. At the very least, Plaintiff is entitled to nominal damages.

COUNT II
NEGLIGENCE

100. The previous paragraphs are incorporated as if fully stated in this Count.

101. CentraState owed a duty to Plaintiff and other Class Members to safeguard and protect their PHI and PII.

102. CentraState breached its duty by failing to exercise reasonable care and failing to safeguard and protect Plaintiff's and other Class Members' PHI and PII.

103. It was reasonably foreseeable that CentraState's failure to exercise reasonable care in safeguarding and protecting Plaintiff's and other Class Members' PHI and PII would result in an unauthorized third-party gaining access to such information for no lawful purpose.

104. It was therefore foreseeable that the failure to adequately safeguard Plaintiff's and other Class Members' PHI and PII would result in one or more types of injuries to Plaintiff.

105. Plaintiff and other Class Members suffered and will continue to suffer damages including, but not limited to: (i) the untimely and/or inadequate notification of the Breach; (ii) improper disclosure of their PHI and PII; (iii) loss of privacy; (iv) out-of-pocket expenses incurred to mitigate the increased risk of identity theft and/or identity fraud pressed upon them by the Breach; (v) the value of their time spent mitigating identity theft and/or identity fraud and/or the increased risk of identity theft and/or identity fraud; and, (vi) the increased risk of identity theft. At the very least, Plaintiff is entitled to nominal damages.

106. CentraState's wrongful actions and/or inaction and the resulting Breach (as described above) constituted (and continue to constitute) negligence at common law.

COUNT III
INVASION OF PRIVACY BY PUBLIC DISCLOSURE OF PRIVATE FACTS

107. The previous allegations are incorporated as if fully stated in this Count.

108. Plaintiff's and other Class Members' PHI and PII was (and continues to be) sensitive and personal private information.

109. By virtue of CentraState's failure to safeguard and protect Plaintiff's and other Class Members' PHI and PII and the resulting Breach, CentraState wrongfully disseminated Plaintiff's PHI and PII to unauthorized persons.

110. Dissemination of Plaintiff's and other Class Members' PHI and PII is not of a legitimate public concern; publicity of their PHI and PII was, is and will continue to be offensive to Plaintiff and other Class Members and all reasonable people. The unlawful disclosure of same violates public mores.

111. Plaintiff and other Class Members suffered and will continue to suffer damages including, but not limited to: (i) the untimely and/or inadequate notification of the Breach; (ii) improper disclosure of their PHI and PII; (iii) loss of privacy; (iv) out-of-pocket expenses incurred to mitigate the increased risk of identity theft and/or identity fraud pressed upon them by the Breach; (v) the value of their time spent mitigating identity theft and/or identity fraud and/or the increased risk of identity theft and/or identity fraud; and, (vi) the increased risk of identity theft. At the very least, Plaintiff and other Class Members are entitled to nominal damages.

112. CentraState's wrongful actions and/or inaction and the resulting Breach (as described above) constituted (and continue to constitute) an invasion of Plaintiff's and other Class Members' privacy by publicly and wrongfully disclosing their private facts (*i.e.*, their PHI and PII) without their authorization or consent.

COUNT IV
BREACH OF FIDUCIARY DUTY

113. The previous paragraphs are incorporated as if fully stated in this Count.

114. At all times relevant to this Petition, CentraState owed, and owes, a fiduciary duty to Plaintiff and other Class Members, pursuant to New Jersey common law, to keep their medical and other PHI and PII information confidential.

115. The fiduciary duty of privacy imposed by New Jersey law is explicated under the procedures set forth in the Health Insurance Portability and Accountability Act Privacy Rule, including, without limitation the procedures and definitions of 45 C.F.R. § 160.103 and 45 C.F.R. § 164.530 which requires a covered entity, health care provider, to apply appropriate administrative, technical, and physical safeguards to protect the privacy of patient medical records.

116. CentraState breached its fiduciary duties owed to Plaintiff and other Class Members by failing to ensure the confidentiality and integrity of electronic PHI CentraState created, received, maintained, and transmitted, in violation of 45 C.F.R. § 164.306(a)(1).

117. CentraState breached its fiduciary duties owed to Plaintiff and other Class Members by failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to

those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1).

118. CentraState breached its fiduciary duties owed to Plaintiff and other Class Members by failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. § 164.308(a)(1).

119. CentraState breached its fiduciary duties owed to Plaintiff and other Class Members by failing to identify and respond to suspected or known security incidents and mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 C.F.R. § 164.308(a)(6)(ii).

120. CentraState breached its fiduciary duties owed to Plaintiff and other Class Members by failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2).

121. CentraState breached its fiduciary duties owed to Plaintiff and other Class Members by failing to protect against any reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3).

122. CentraState breached its fiduciary duties owed to Plaintiff and other Class Members by failing to ensure compliance with the HIPAA security standard rules by its workforce in violation of 45 C.F.R. § 164.306(a)(4).

123. CentraState breached its fiduciary duties owed to Plaintiff and other Class Members by impermissibly and improperly using and disclosing PHI that is and remains accessible to unauthorized persons in violation of 45 C.F.R. § 164.502, *et seq*.

124. CentraState breached its fiduciary duties owed to Plaintiff and other Class Members by failing to effectively train and supervise all members of its workforce (including independent contractors) regarding its policies and procedures with respect to PHI as necessary and appropriate for the members of its workforce to carry out their functions and to maintain security of PHI in violation of 45 C.F.R. § 164.530(b) and 45 C.F.R. § 164.308(a)(5).

125. CentraState breached its fiduciary duties owed to Plaintiff and other Class Members by failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard PHI, in compliance with 45 C.F.R. § 164.530(c).

126. In light of the special relationship between CentraState and Plaintiff, and other Class Members whereby CentraState became guardians of Plaintiff's PHI and PII, CentraState became a fiduciary created by its undertaking and guardianship

of the Protected Information, to act primarily for the benefit of its patients, including Plaintiff: (1) for the safeguarding of Plaintiff's Protected Information; (2) to timely notify Plaintiff of a medical records security failure and disclosure; and (3) maintain complete and accurate records of what and where CentraState's patients' PHI and PII was and is stored.

127. CentraState breached its fiduciary duty to Plaintiff by disclosing Plaintiff's and other Class Members' PHI and PII to unauthorized third parties.

128. As a direct result of CentraState's breach of fiduciary duty of confidentiality and the disclosure of Plaintiff's and other Class Members' confidential medical information, Plaintiff and other Class Members suffered damages.

129. Plaintiff and other Class Members suffered and will continue to suffer damages including, but not limited to: (i) the untimely and/or inadequate notification of the Breach; (ii) improper disclosure of their PHI and PII; (iii) loss of privacy; (iv) out-of-pocket expenses incurred to mitigate the increased risk of identity theft and/or identity fraud pressed upon them by the Breach; (v) the value of their time spent mitigating identity theft and/or identity fraud and/or the increased risk of identity theft and/or identity fraud; and (vi) the increased risk of identity theft. At the very least, Plaintiff is entitled to nominal damages.

COUNT V
VIOLATIONS OF NEW JERSEY CONSUMER FRAUD ACT ("NJCFA"), NJ Rev. Stat. § 56:1, et seq.

130. The previous paragraphs are incorporated by reference as if fully stated in this Count.

131. NJ Rev. Stat. § 56:1 states, "[t]he act, use or employment by any person of any unconscionable commercial practice, deception, fraud, false pretense, false promise, misrepresentation, or the knowing, concealment, suppression, or omission of any material fact with intent that others rely upon such concealment, suppression or omission, in connection with the sale or advertisement of any merchandise or real estate, or with the subsequent performance of such person as aforesaid, whether or not any person has in fact been misled, deceived or damaged thereby, is declared to be an unlawful practice…" NJ Rev. Stat. § 56:8-2.

132. Plaintiff, the other Class Members, and CentraState are "persons" within the meaning of NJ Rev. Stat. § 56:1, et seq.

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

134. Efforts to maintain the privacy and confidentiality of medical records are part of the healthcare services associated with a good.

135. Maintenance of medical records are "merchandise" within the meaning of NJ Rev. Stat. § 56:1, et seq.

136. Plaintiff's and other Class Members' goods and services purchased from CentraState were for "personal, family or household purposes" within the meaning of the NJCFA.

137. CentraState's acts, practices and conduct violate NJ Rev. Stat. § 56:1, et seq. in that, among other things, CentraState 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 offends the public policy established by New Jersey statute and constitute an "unfair practice" as that term is used in the NJCA.

138. CentraState's unfair, unlawful and deceptive acts, practices and conduct include, but are not limited to: (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) omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's Personal Information; and, (4) failing to train personnel.

139. Defendant's conduct also violates the enabling regulations for the NJCFA 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.

140. As a direct and proximate cause of Defendant's unfair and deceptive acts, Plaintiff and other Class Members 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, Plaintiff has not received the benefit of the bargain and has suffered an ascertainable loss.

141. CentraState engaged in unlawful, unfair, and deceptive acts and practices, in connection with the sale or advertisement of merchandise in trade or commerce, in violation of NJ Rev. Stat. § 56:1, et seq.

(i) Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's Protected Information, which was a direct and proximate cause of the Breach;

(ii) Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous

security incidents, which was a direct and proximate cause of the Breach;

(iii) Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's Protected Information, including duties imposed by the FTCA, 15 U.S.C. § 45, the Fair Credit Reporting Act, 15 U.S.C. § 1681e ("FRCA"), and the Gramm-Leach-Bliley Act ("GLBA"), 15 U.S.C. § 6801, *et seq.*, which was a direct and proximate cause of the Breach;

(iv) Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs' Protected Information, including implementing and maintaining reasonable security measures;

(v) Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' Protected Information, including duties imposed by the FTCA, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq.*;

(vi) Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and New Jersey Plaintiffs' Personal Information; and,

(vii) Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and New Jersey Plaintiffs' Protected Information, including duties imposed by the FTCA, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq*.

142. Plaintiff and other Class Members seek all relief under the NJCFA including actual damages, injunctive relief, and attorneys' fees.

COUNT VI
NEGLIGENT TRAINING AND SUPERVISION

143. The previous paragraphs are incorporated by reference as if fully stated in this Count.

144. At all times relevant to this Petition, CentraState owed a duty to Plaintiff and other Class Members to hire competent employees, and to train and supervise them to ensure they recognize the duties owed to their patients and their parents.

145. CentraState breached its duty to Plaintiff and other Class Members by allowing its employees to give access to patient medical records to an unauthorized user.

146. As a direct result of CentraState's breach of its duty of confidentiality and privacy and the disclosure of Plaintiff's and other Class Members confidential

medical information, Plaintiff suffered damages, including, without limitation, loss of the benefit of the bargain, exposure to heightened future risk of identity theft, loss of privacy, confidentiality, embarrassment, humiliation and loss of enjoyment of life.

COUNT VII
NEGLIGENCE *PER SE*

147. Plaintiff and other Class Members incorporate the previous paragraphs as if fully stated in this Count.

148. Plaintiff and other Class Members was under the medical care of the Defendant.

149. Defendant is a covered entity for purposes of HIPAA.

150. Plaintiff and other Class Members is a member of the class HIPAA and HITECH were created to protect.

151. Plaintiff's and other Class Members' private health information is the type of information HIPAA and HITECH were created to protect. HIPAA and HITECH were created to protect against the wrongful and unauthorized disclosure of an individual's health information.

152. Defendant gave protected medical information to an unauthorized third party or unauthorized third parties without the written consent or authorization of Plaintiff and other Class Members.

153. Defendant gave protected medical information to unauthorized third parties without Plaintiff's oral consent or written authorization.

154. The information disclosed to an unauthorized third party or unauthorized third parties included private health information about medical treatment.

155. Defendant's disclosure of the private health information of Plaintiff without consent or authorization is a violation of HIPAA and HITECH and is negligence *per se*.

156. Alternatively, Defendant violated HIPAA and HITECH in that it did not reasonably safeguard the private health information of Plaintiff from any intentional or unintentional use or disclosure that is in violation of the standards, implementation specifications or other requirements pursuant to HIPAA and HITECH including, but not limited to, 42 C.F.R. §§ 164.302-164.318, 45 C.F.R. § 164.500, *et seq*, and 42 U.S.C. §17902, and was therefore negligent *per se*.

157. Pursuant to the FTCA (15 U.S.C. § 45), CentraState had a duty to provide fair and adequate computer systems and information security practices to safeguard Plaintiff's PHI and PII.

158. Pursuant to the Gramm-Leach-Bliley Act (15 U.S.C. § 6801) ("GLBA"), CentraState had a duty to protect the security and confidentiality of Plaintiff's and PII.

159. CentraState's failure to comply with applicable laws and regulations constitutes negligence per se.

160. But for CentraState's wrongful and negligent breach of its duties owed to Plaintiff, Plaintiff would not have been injured.

161. The injury and harm suffered by Plaintiff was the reasonably foreseeable result of CentraState's breach of its duties. CentraState knew or should have known that they were failing to meet its duties, and that CentraState's breach would cause Plaintiff to experience the foreseeable harms associated with the exposure of its Protected Information.

162. As a direct result of CentraState's negligence, Plaintiff suffered damages and injuries, including, without limitation, loss of the benefit of their bargain, a reduction in value of their private health information, loss of privacy, loss of medical expenses, loss of trust, loss of confidentiality, embarrassment, humiliation, emotional distress, and loss of enjoyment of life.

163. As a direct result of CentraState's negligence, Plaintiff has a significantly increased risk of being future victims of identity theft relative to what would be the case in the absence of the CentraState's wrongful acts.

164. As a direct result of CentraState's negligence, future monitoring, in the form of identity-theft or related identity protection is necessary in order to properly warn Plaintiff of, and/or protect Plaintiff from, being a victim of identity theft or other identity-related crimes.

165. Plaintiff and other Class Members seeks actual damages for all monies paid to Defendant in violation of the applicable statutes. In addition, Plaintiff seeks attorneys' fees.

REQUEST FOR RELIEF

WHEREFORE, Plaintiff respectfully request that the Court enter judgment in their favor and against CentraState, as follows:

A. Declaring that this action is a proper class action, certifying the Class as requested herein, designating Plaintiffs as Class Representatives and appointing Plaintiffs' counsel as Lead Counsel for the Class;

B. Declaring that CentraState breached its contracts with Plaintiff and other Class Members;

C. Declaring that CentraState negligently disclosed Plaintiff's and other Class Members' PHI and PII;

D. Declaring that CentraState has invaded Plaintiff's and other Class Members' privacy;

E. Declaring that CentraState breached its fiduciary duty to Plaintiff and other Class Members;

F. Declaring that CentraState breached its contracts with Plaintiff and other Class Members;

G. Declaring that Defendant violated the New Jersey Consumer Fraud Act;

H. Declaring that CentraState negligent by negligently hiring, training and supervising its employees;

I. Ordering CentraState to pay actual damages to Plaintiff and other Class Members;

J. For an Order enjoining CentraState from continuing to engage in the unlawful practices alleged herein;

K. Ordering CentraState to pay attorneys' fees and litigation costs to Plaintiff and other Class Members;

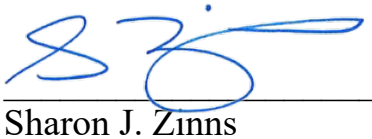
L. Ordering CentraState to pay both pre- and post-judgment interest on any amounts awarded; and,

M. Ordering such other and further relief as may be just and proper.

JURY DEMAND

Plaintiff and other Class Members respectfully demand a trial by jury on all of their claims and causes of action so triable.

Respectfully submitted,



Sharon J. Zinns
NJ Bar No. 033192008
Zinns Law, LLC
1800 Peachtree St. NW
Suite 370
Atlanta, GA 30309
Ph: (404) 882-9002
Email: sharon@zinnslaw.com

and

Maureen M. Brady
MO#57800
Lucy McShane

MO#57957
McSHANE & BRADY, LLC
1656 Washington Street, Suite 120
Kansas City, MO 64108
Phone: (816) 888-8010
Fax: (816) 332-6295
E-mail:
mbrady@mcshanebradylaw.com
lmcshane@mcshanebradylaw.com
To be admitted pro hac vice

ATTORNEYS FOR PLAINTIFFS

ClassAction.org