IN THE UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF TENNESSEE

SARA RILEY, individually and on behalf of all others similarly situated, *Plaintiff,* v. CENTERSTONE OF AMERICA, INC., CENTERSTONE OF INDIANA, INC., and CENTERSTONE OF TENNESSEE, INC., *Defendants.*	)	Case No. Jury Trial Demanded

CLASS ACTION COMPLAINT

Plaintiff, Sarah Riley, individually and on behalf of the Class defined below of similarly situated persons, alleges the following against Centerstone of America Inc., Centerstone of Indiana, Inc., and Centerstone of Tennessee, Inc. (collectively referred to herein as "Centerstone") based upon personal knowledge and on information and belief derived from, among other things, investigation of counsel and review of public documents as to all other matters:

INTRODUCTION

1. This class action arises out of the recent data breach at Centerstone's healthcare facilities that occurred between November 2021 and February 2022 ("Data Breach"). As a result of the Data Breach, Plaintiff, who was a patient of Centerstone from on or about May 2021 through in or about October 2021, and similarly situated individuals who are current and former Centerstone patients, suffered irreparable damage when their sensitive personal and protected health information was compromised and unlawfully accessed.

2. Information compromised in the Data Breach included highly sensitive data that represents a gold mine for data thieves. According to Centerstone, this includes current and former patient **names, dates of birth, social security numbers, driver's license or state identification**

card numbers, medical diagnosis or treatment information, Medicare and/or Medicaid information, and health insurance information (collectively the "Private Information"). Compromised information may also include other protected health information ("PHI") as defined by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), and additional personally identifiable information ("PII") that Centerstone collected and maintained.

3. Centerstone claims it learned about the data breach on February 14, 2022. However, according to the company it did not begin notifying affected individuals until August 2, 2022, nearly six months later. Despite this delay, Centerstone did not offer the victims any protection or compensation in its notification letter, not even complementary credit monitoring, a common precaution that many companies affected by data breaches will offer to victims to help protect the sensitive information the company permitted to be stolen.

4. Armed with the Private Information accessed in the Data Breach, and a six month head start, data thieves can commit a variety of crimes including, e.g., opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' names to obtain medical services, using Class Members' health information to target other phishing and hacking intrusions based on their individual health needs, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

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

6. Therefore, Plaintiff and Class Members will show that they have suffered ascertainable losses in the form of the loss of the benefit of their bargain, out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the attack.

7. Centerstone is well aware of the dangers of a data breach and the importance of protecting Private Information. A similar data breach by Centerstone occurred in 2019 that resulted in the compromise of sensitive data of tens of thousands of patients. Centerstone settled a class action suit regarding that data theft in 2021. *See Kenney et al., v. Centerstone of America et al.,* No. 3:20-cv-1007, ECF No. 44 (M.D. Tenn. August 9, 2021) (Order granting final approval of class settlement).

8. Plaintiff brings this class action lawsuit to address Centerstone's inadequate safeguarding of Class Members' Private Information that it collected and maintained, and for failing to provide timely and adequate notice to Plaintiff and Class Members that their information had been subject to unauthorized access.

9. The potential for improper disclosure of Plaintiff's and Class Members' Private Information was a known risk to Centerstone, and thus Centerstone was on notice that failing to take steps necessary to secure the Private Information from those risks left that property in a dangerous condition.

10. Centerstone and its employees failed to properly monitor the computer network and systems that housed the Private Information. Had Centerstone properly monitored its networks, it would have discovered the breach sooner.

11. Plaintiff's and Class Members' identities are now at risk because of Centerstone's negligent conduct since the Private Information that Centerstone collected and maintained is now likely in the hands of data thieves and unauthorized third-parties.

12. Plaintiff seeks to remedy these harms on behalf of herself and all similarly situated individuals whose Private Information was accessed and/or compromised during the Data Breach.

13. Plaintiff seeks remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, and injunctive relief including improvements to

Centerstone's data security systems, future annual audits, and adequate credit monitoring services funded by Centerstone.

PARTIES

14. Plaintiff Sara Riley is, and at all times mentioned herein was, an individual citizen of the State of Indiana residing in the City of Austin in Scott County.

15. Centerstone of America, Inc. ("Centerstone of America") is a healthcare services provider with its principal place of business at 44 Vantage Way, Suite 400, Nashville, TN 37228.

16. Centerstone of Indiana, Inc. ("Centerstone of Indiana") is a healthcare services provider with its principal place of business at 645 South Rogers Street, Bloomington, IN, 47403. Upon information and belief, Centerstone of Indiana is a wholly owned subsidiary of Centerstone of America.

17. Centerstone of Tennessee, Inc. ("Centerstone of Tennessee") is a healthcare services provider with its principal place of business at 44 Vantage Way, Suite 400, Nashville, TN 37228. Upon information and belief, Centerstone of Tennessee is a wholly owned subsidiary of Centerstone of America.

18. As the parent company, Centerstone of America controls Centerstone of Indiana and Centerstone of Tennessee and other related entities with the purpose of carrying out healthcare services from its headquarters in this District. On information and belief, Centerstone of America and/or Centerstone of Tennessee maintained the Private Information of Plaintiff and Class Members that they provided to Centerstone in the course of obtaining healthcare. On information and belief, Centerstone of America and/or Centerstone of Tennessee maintained the Private Information of Plaintiff and Class Members in this judicial district.

JURISDICTION AND VENUE

19. The Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. Upon information and belief, the number of class members is over 100, many of whom have different citizenship from Defendants Centerstone of America, Inc. and Centerstone

of Indiana, Inc. including the named Plaintiff here. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

20. This Court has jurisdiction over each of the Defendants because they operate and/or are incorporated in this District, and the computer systems implicated in this Data Breach are likely based in this District.

21. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events giving rise to this action occurred in this District. Centerstone have caused harm to Class Members residing in this District.

CENTERSTONE HEALTH SYSTEM

22. Centerstone is a health system providing mental health and substance use disorder treatments. Services are available nationally through the operation of outpatient clinics, residential programs, the use of telehealth and an inpatient hospital programs. Centerstone also features specialized programs for the military community, therapeutic foster care, children's services and employee assistance programs. Centerstone operates in over 170 locations and serves over 120,000 clients a year.

23. As a condition of receiving medical care and treatment at its facilities, Centerstone requires that its patients entrust it with highly sensitive personal information. In the ordinary course of receiving treatment and health care services from Centerstone, patients are required to provide sensitive personal and private information such as:

- Names;
- Dates of birth;
- Social Security numbers;
- Driver's license numbers and information;
- Financial account information;
- Payment card information;
- Medical histories including all medical records from outside physicians;
- Treatment information;

- Medication or prescription information;
- Beneficiary information;
- Provider information;
- Address, phone number, and email address;
- Health insurance information; and
- Sensitive personal information, including past habits and pattern of life activity, disclosed through counseling and treatment.

24. Additionally, Centerstone may receive private and personal information from other individuals and/or organizations that are part of a patient's "circle of care," such as referring physicians, patients' other doctors, patient's health plan(s), close friends, and/or family members.

25. Centerstone maintains a Notice of Privacy Practices (the "Privacy Notice"),[1] in respect to how it handles patients' sensitive information, as it is required to maintain under HIPAA. Centerstone links to this Privacy Notice on its website. On information and belief, Centerstone provides each of its patients with a copy of this Privacy Notice and requires each to sign an acknowledgment with regard to the Privacy Notice.

26. Because of the highly sensitive and personal nature of the information Centerstone acquires and stores with respect to its patients, Centerstone promises in its Privacy Notice to, among other things, maintain the privacy of patients' health information:

> Centerstone ACE is committed to protecting the privacy and security of your medical, mental health and substance abuse information. We are required by law to maintain the privacy and security of your health information, to provide you this notice and to comply with its terms.

27. According to the Privacy Notice, all of Centerstone's employees, staff, entities, clinics, sites, and locations may share patient information with each other for various purposes without a written authorization.

[1] https://centerstone.org/wp-content/uploads/AFFILIATED-COVERED-ENTITY-NPP-V5-English-09102020-Revision.pdf

28. On information and belief, Centerstone of America, Centerstone of Tennessee, and Centerstone of Indiana use centralized servers for their employee email systems, and pass emails containing patient PII and PHI to each other via one email system that all three entities utilize.

29. In its Privacy Notice, Centerstone promises that it will provide notification to affected individuals within 60 days of a data breach incident:

> **Breach Notification.** We will let you know promptly if a breach occurs that may have compromised the privacy or security of your health information. In no event will notification be more than 60 days from the date of the breach.

30. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Private Information, Centerstone assumed legal and equitable duties and knew or should have known, based, *inter alia*, on the prior data breach and settlement, that it was responsible for protecting Plaintiff's and Class Members' Private Information from disclosure.

31. Plaintiff and the Class Members have taken reasonable steps to maintain the confidentiality of their Private Information.

32. Plaintiff and the Class Members relied on Centerstone to keep their Private Information confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

DATA BREACHES IN HEALTHCARE

33. According to the Ponemon Institute and Verizon Data Breach Investigations Report, the health industry experiences more data breaches than any other sector.[2] Regular PII can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[3] However, PHI can sell for as much as $363 according to the Infosec Institute.[4] This is because one's personal health history, can't be changed, unlike credit card information.

---

[2] *Data Breaches: In the Healthcare Sector*, Center for Internet Security, *available at* https://www.cisecurity.org/insights/blog/data-breaches-in-the-healthcare-sector (last visited August 10, 2022).
[3] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends (October 16, 2019), *available at* https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/.
[4] *Data Breaches: In the Healthcare Sector*, Center for Internet Security, *available at* https://www.cisecurity.org/insights/blog/data-breaches-in-the-healthcare-sector (last visited August 10, 2022).

34. PHI has increased value because criminals can use it to target victims with frauds and scams that take advantage of the victim's medical conditions or victim settlements. It can also be used to create fake insurance claims, allowing for the purchase and resale of medical equipment. Some criminals use PHI to illegally gain access to prescriptions for their own use or resale.

CENTERSTONE 2019 DATA BREACH

35. In or around August of 2020, Centerstone became aware of suspicious activity related to several of its employees' email accounts. An investigation revealed that certain employee email accounts were accessed without authorization between December 12 and December 16, 2019.

36. Centerstone does not appear to have discovered the unauthorized intrusion until August of 2020—approximately eight months after-the-fact. Despite acknowledging that data thieves likely accessed patients' sensitive information, Centerstone did not begin to notify affected patients until October 22, 2020.

37. Patients were notified that the data breach included the following information: patient names, dates of birth, Social Security numbers, driver's license or state identification card numbers, medical diagnosis or treatment information, Medicaid and/or Medicare information, and/or health insurance information.

38. A class action complaint was filed in the U.S. District Court for the Middle District of Tennessee against Centerstone on November 20, 2020, alleging that Centerstone employees were targeted by a phishing cyberattack, which allowed hackers to gain access to employees' email accounts, expressly designed to gain access to private and confidential data, including (among other things) the Private Information of patients. *See Kenney et al., v. Centerstone of America et al.,* No. 3:20-cv-1007, ECF No. 1 (M.D. Tenn. November 20, 2020) (Class action complaint).

39. The complaint also alleged that the emails containing the Private Information that were accessed were not encrypted, and furthermore, that the stolen Private Information was subsequently sold on the Dark Web. *Id.*

40. On August 9, 2021, the Court granted final approval of the class settlement whereby Centerstone agreed to compensate the named Plaintiff and Class Members affected by the data breach. As part of the settlement, Centerstone represented that it had enhanced information security, including third party security monitoring, third party logging, network monitoring, firewall enhancements, email enhancements, and equipment upgrades, and it committed to implementing additional enhancements in years 2021 and 2022. *See Kenney et al., v. Centerstone of America et al.,* No. 3:20-cv-1007, ECF No. 34 (M.D. Tenn. May 6, 2021) (Settlement Agreement).

CENTERSTONE'S 2021-2022 DATA BREACH AND NOTICE TO PLAINTIFF

41. From in or about May 2021 through in or about October 2021, Plaintiff Ms. Riley was a patient at Centerstone Scottsburg – West Community Way, located at 1092 West Community Way, Scottsburg, Indiana 47170.

42. As a mandatory part of the new patient intake, Ms. Riley provided a release of her medical records from her family care physician to Centerstone. Ms. Riley also provided her family medical history and sensitive information about her husband and pattern of life.

43. Centerstone collected financial information and driver's license information for both Ms. Riley and her husband.

44. During the course of her time as a Centerstone patient from May to October 2021, Centerstone created medical records that contained sensitive health information regarding Ms. Riley.

45. According to the company, in February 2022, Centerstone again learned of suspicious activity involving an employee's email account. Upon discovering this activity, Centerstone claims it began an investigation which concluded that an unauthorized party accessed three employee email accounts between November 4, 2021 and February 14, 2022, a period of more than three months.

46. Upon information and belief, the affected employee email accounts were part of the single employee email system used by defendants, a system that utilizes centralized servers.

47. Centerstone concluded its review of the data breach on July 12, 2022, however, the company did not notify individuals affected until August 2022, approximately six months after the suspicious activity was discovered.

48. Ms. Riley received a letter from Centerstone, dated August 2, 2022, with the subject "Notice of Data Security Incident." This letter informed her that her data may have been compromised by the data security incident discovered in February 2022. Nevertheless, Centerstone's notice letter to Ms. Riley failed to identify with certainty precisely what specific information was compromised and/or accessed. Instead, it states only that the information accessed "*may have included*" Ms. Riley's name, date of birth, Client ID, and doctor's name.

49. The notice letter then attached several pages entitled "Additional Steps You Can Take to Protect Information of an Adult" and "Additional Steps You Can Take to Protect Information of a Minor," which listed generic steps that victims of data security incidents can take, such as getting a copy of a credit report or notifying law enforcement about suspicious financial account activity. Other than providing a call center number that victims could contact "with any questions," Centerstone offered no other substantive steps to help victims like Plaintiff and the Class Members to protect themselves.

50. On information and belief, Centerstone sent a similar generic letter to all individuals affected

51. However, according to a press release from Centerstone released on or about August 5, 2022, the data breach involved far more than the information revealed in the letter. According to the company:

> The following personal and protected health information may have been involved in the incident: name, address, Social Security number, date of birth, client ID, medical diagnosis / treatment information, and/or health insurance information.

52. Centerstone had obligations created by HIPAA, contract, industry standards, common law, and representations made to Plaintiff and Class Members to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

53. Plaintiff and Class Members provided their Private Information to Centerstone with the reasonable expectation and mutual understanding that Centerstone would comply with its obligations to keep such information confidential and secure from unauthorized access and to provide timely notice of security breaches.

54. Centerstone's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in the healthcare industry preceding the date of the breach, including its own data breach only two years prior.

55. As further evidence of Centerstone's knowledge of the threat from cyberattacks, Centerstone represented to this Court in a settlement agreement that it would commit to additional information security enhancements in 2021 and 2022. *See Kenney et al., v. Centerstone of America et al.,* No. 3:20-cv-1007, ECF No. 34 (M.D. Tenn. May 6, 2021) (Settlement Agreement).

56. Centerstone knew or should have known that its electronic records would be once again targeted by cybercriminals.

57. On information and belief, Centerstone failed to implement sufficient additional measures to prevent cyberattacks following the discovery of the 2019 data breach.

CENTERSTONE FAILED TO COMPLY WITH FTC GUIDELINES

58. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision making.

59. In October 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer

networks; understand their network's vulnerabilities; and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

60. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

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

62. On information and belief, Centerstone failed to properly implement basic data security practices. Centerstone's failure to employ reasonable and appropriate measures to protect against unauthorized access to patient PII and PHI constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

63. Centerstone was at all times fully aware of its obligation to protect the PII and PHI of its patients. Centerstone was also aware of the significant repercussions that would result from its failure to do so, particularly in light of the settlement agreement approved by the U.S. District Court Judge in August 2021, only months prior to the data breach that commenced in early November 2021.

CENTERSTONE FAILED TO COMPLY WITH INDUSTRY STANDARDS

64. Experts studying cyber security routinely identify healthcare providers as being particularly vulnerable to cyberattacks because of the value of the PII and PHI which they collect and maintain.

65. Several best practices have been identified that a minimum should be implemented by healthcare providers like Centerstone, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data, and; limiting which employees can access sensitive data.

66. A number of industry and national best practices have been published and should be used as a go-to resource when developing an institution's cybersecurity standards. The Center for Internet Security ("CIS") released its Critical Security Controls, and all healthcare institutions are strongly advised to follow these actions.[5] The CIS Benchmarks are the only consensus-based, best-practice security configuration guides both developed and accepted by government, business, industry, and academia.[6]

67. Other best cybersecurity practices that are standard in the healthcare industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points.

68. On information and belief, Centerstone of America establishes data security procedures for itself and all its subsidiaries; and Centerstone failed to meet the minimum standards of the following frameworks: the National Institute of Standards and Technology ("NIST") Cybersecurity Framework, the HIPAA Security Rule and Breach Notification Rule, the CIS

[5] *Data Breaches: In the Healthcare Sector*, Center for Internet Security, *available at* https://www.cisecurity.org/insights/blog/data-breaches-in-the-healthcare-sector (last visited August 10, 2022).
[6] *CIS Benchmarks FAQ*, Center for Internet Security, *available at* https://www.cisecurity.org/cis-benchmarks/cis-benchmarks-faq (last visited August 10, 2022).

Critical Security Controls, the Control Objectives for Information Related Technology ("COBIT"), ISO/IEC 27001, and HITRUST Common Security Framework, which are all established standards in reasonable cybersecurity readiness.

CENTERSTONE'S PRACTICES VIOLATE HIPAA

69. HIPAA requires covered entities to protect against reasonably anticipated threats to the security of sensitive patient health information.

70. Covered entities must implement safeguards to ensure the confidentiality, integrity, and availability of PHI. Safeguards must include physical, technical, and administrative components.

71. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§ 1301, *et seq.* These provisions require, among other things, that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling PII like the data Centerstone permitted to be stolen. The HHS subsequently promulgated multiple regulations under authority of the Administrative Simplification provisions of HIPAA. These rules include 45 C.F.R. § 164.306(a)(1-4); 45 C.F.R. § 164.312(a)(1); 45 C.F.R. § 164.308(a)(1)(i); 45 C.F.R. § 164.308(a)(1)(ii)(D), and 45 C.F.R. § 164.530(b).

72. On information and belief, Centerstone's Data Breach resulted from a combination of insufficiencies that demonstrate they failed to comply with safeguards mandated by HIPAA regulations.

CENTERSTONE'S SECURITY BREACH

73. Centerstone breached its obligations to Plaintiff and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and data. Centerstone's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. Failing to adequately protect patients' Private Information;

c. Failing to properly monitor its own data security systems for existing intrusions;

d. Failing to sufficiently train its employees in the proper handling of emails containing PII and PHI;

e. Failing to ensure the confidentiality and integrity of electronic PHI it created, received, maintained, and/or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

f. Failing to properly 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);

g. Failing to sufficiently implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. § 164.308(a)(1)(i);

h. Failing to adequately implement procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);

i. Failing to properly protect against reasonably anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);

j. Failing to properly protect against 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);

k. Failing to ensure compliance with HIPAA security standard rules by its workforces in violation of 45 C.F.R. § 164.306(a)(4);

l. Failing to adequately train all members of its workforce effectively on the policies and procedures regarding PHI as necessary and appropriate for the

members of its workforces to carry out their functions and to maintain security of PHI, in violation of 45 C.F.R. § 164.530(b);

m. Failing to render the electronic PHI it maintained unusable, unreadable, or indecipherable to unauthorized individuals, as it had not encrypted the electronic PHI as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key" (45 CFR § 164.304's definition of "encryption");

n. Failing to fully comply with FTC guidelines for cybersecurity, in violation of Section 5 of the FTC Act, and;

o. Failing to adhere to industry standards for cybersecurity.

74. As the result of computer systems in need of security upgrading, inadequate procedures for handling emails containing viruses or other malignant computer code, and employees who opened files containing the virus or malignant code that perpetrated the cyberattack, Centerstone negligently and unlawfully failed to safeguard Plaintiff's and Class Members' Private Information.

75. Centerstone was put on notice of the need to upgrade security measures and train employees regarding cybersecurity practices upon the discovery of the 2019 data breach in August 2020. However, despite Centerstone agreeing in April 2021 to compensate victims of the 2019 data breach, representing that it had upgraded information security enhancements and committing to additional information security enhancements in 2021 and 2022, Centerstone failed to sufficiently implement additional cybersecurity measures which resulted in a second data breach in early November 2021.

76. Accordingly, as outlined below, Plaintiff's and Class Members' daily lives were severely disrupted. What's more, they now face an increased risk of fraud and identity theft. Plaintiff and the Class Members also lost the benefit of the bargain they made with Centerstone.

HEALTHCARE DATA BREACHES, FRAUD AND IDENTITY THEFT

77. Cyberattacks are considered a breach under the HIPAA Rules because there is an access of PHI not permitted under the HIPAA Privacy Rule: A breach under the HIPAA Rules is defined as "the acquisition, access, use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of the PHI." *See* 45 C.F.R. 164.40.10.

78. The FTC hosted a workshop to discuss "informational injuries" which are injuries that consumers suffer from privacy and security incidents, such as data breaches or unauthorized disclosure of data.[7] Exposure of personal information that a consumer wishes to keep private, such as sensitive medical information, sexual orientation, or gender identity, may cause both market and non-market harm to the consumer, such as the ability to obtain or keep employment and negative impact on consumer's relationships with family, friends and coworkers. Healthcare data breaches can erode patients' trust in the ability of providers to protect their data, and may be less willing to seek treatment. Consumers loss of trust in e-commerce also deprives them of the benefits provided by the full range of goods and services available which can have negative impacts on daily life.

79. Any victim of a data breach is exposed to serious ramifications regardless of the nature of the data. Indeed, the reason criminals steal information is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims, or take over victims' identities in order to engage in illegal financial transactions under the victims' names. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity, or otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social

[7] *FTC Information Injury Workshop, BE and BCP Staff Perspective,* Federal Trade Commission, (October 2018), *available at* https://www.ftc.gov/system/files/documents/reports/ftc-informational-injury-workshop-be-bcp-staff-perspective/informational_injury_workshop_staff_report_-_oct_2018_0.pdf.

engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

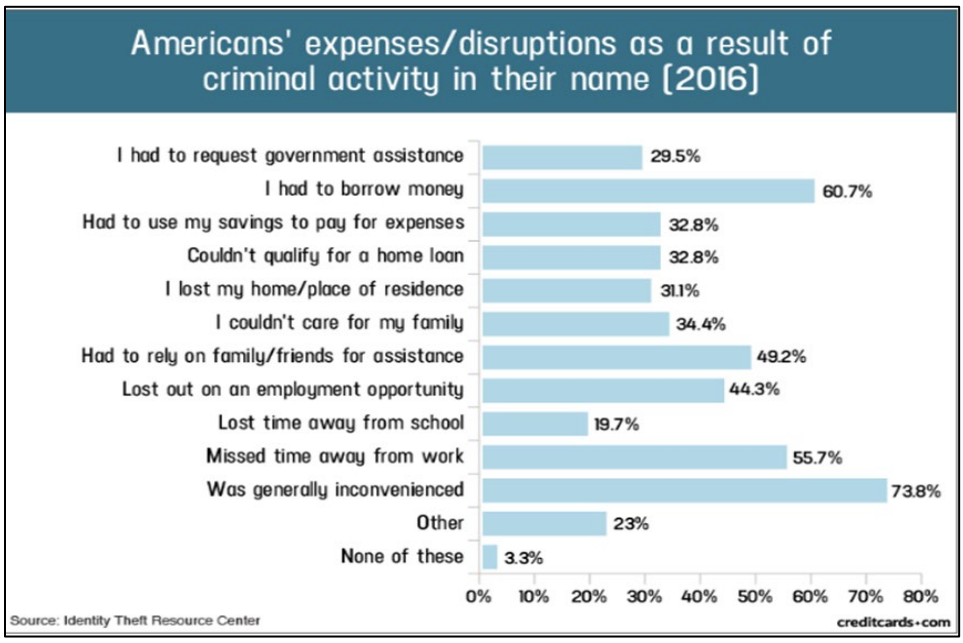
80. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[8]

81. Identity thieves use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

82. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

83. A study by Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of PII:[9]

[8] *See IdentityTheft.gov,* Federal Trade Commission, *available at* https://www.identitytheft.gov/Steps (last visited August 11, 2022).
[9] Steele, Jason, *Credit Card and ID Theft Statistics*, CreditCards.com (October 23, 2017), *available at* https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276/.



84. Moreover, theft of Private Information is also gravely serious. Its value is axiomatic, considering the value of "big data" in corporate America and the fact that the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

85. Theft of PHI is gravely serious and can result in medical identity theft, where a thief uses the victim's information to see a doctor, get prescription drugs, buy medical devices, submit insurance claims, or get other medical care.[10] If the thief's health information is mixed with the victim's health information, it can negatively impact the victim's health insurance benefits and credit.

86. Drug manufacturers, medical device manufacturers, pharmacies, hospitals and other healthcare service providers often purchase PII/PHI on the black market for the purpose of target marketing their products and services to the physical maladies of the data breach victims themselves. Insurance companies purchase and use wrongfully disclosed PHI to adjust their insureds' medical insurance premiums.

[10] *What To Know About Medical Identity Theft*, Federal Trade Commission (May 2021), *available at* https://consumer.ftc.gov/articles/what-know-about-medical-identity-theft.

87. It must also be noted there may be a substantial time lag – measured in years -- between when harm occurs and when it is discovered, and also between when Private Information and/or financial information is stolen and when it is used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:[11]

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

88. Private Information is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black market" for years.

89. There is a strong probability that entire batches of stolen information have been dumped on the black market and are yet to be dumped on the black market, meaning Plaintiff and Class Members are at an increased risk of fraud and identity theft for many years into the future. Thus, Plaintiff and Class Members must vigilantly monitor their financial and medical accounts for many years to come.

90. Because of its value, the medical industry has experienced disproportionally higher numbers of data theft events than other industries. Centerstone therefore knew or should have known this and strengthened its data and email handling systems accordingly. For Centerstone, this was not a theoretical threat. It was put on notice of the substantial and foreseeable risk of harm of *another* data breach following the 2019 breach, yet it apparently failed to properly prepare for that *known* risk.

PLAINTIFF AND CLASS MEMBERS' DAMAGES

91. Plaintiff and Class Members have been damaged by the compromise of their Private Information in the Data Breach.

[11] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO (June 2007), *available at* https://www.gao.gov/assets/270/262904.html.

92. Plaintiff's Private Information, including her sensitive PII and PHI, was compromised as a direct and proximate result of the Data Breach.

93. As a direct and proximate result of Centerstone's conduct, Plaintiff and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft.

94. As a direct and proximate result of Centerstone's conduct, Plaintiff and Class Members have been forced to expend time dealing with the effects of the Data Breach.

95. Plaintiff and Class Members face substantial risk of out-of-pocket fraud losses such as medical services billed in their names, loans opened in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

96. Plaintiff and Class Members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their Private Information as potential fraudsters could use that information to target such schemes more effectively to Plaintiff and Class Members.

97. Plaintiff and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

98. In addition to the foregoing, Plaintiff Ms. Riley is suffering from substantial increased anxiety and mental anguish. Beyond the normal risks presented by a data breach, Ms. Riley and the other Class Members need to be concerned about the increased risk that her family, friends and associates will learn about her confidential and sensitive medical history, including but not limited to her treatment records at Centerstone, her prior medical history records provided to Centerstone by her family care physician, and other non-medical information that was provided to Centerstone, including her personal family history and relationships. Additionally, Centerstone collected sensitive information regarding Ms. Riley's husband, which she is worried could also become public.

99. The information that Centerstone maintains regarding Ms. Riley, when combined with publicly available information, would allow nefarious actors to paint a complete health, financial and personal history of Ms. Riley. According to Ms. Riley, Centerstone has her entire life documented.

100. Ms. Riley now receives approximately 25 scam phone calls per day, which she believes is a result of the information leaked in the data breach, and as a result is deterred from answering the phone.

101. Plaintiff and Class Members were also damaged via benefit-of-the-bargain damages. Plaintiff and Class Members overpaid, or authorized their insurance companies to overpay, for a service that was intended to be accompanied by adequate data security but was not. Part of the price Plaintiff and Class Members paid, or that was paid on their behalf, to Centerstone was intended to be used by Centerstone to fund adequate security of Centerstone's computer property and protect Plaintiff's and Class Members' Private Information. Thus, Plaintiff and the Class Members did not get what they paid for.

102. Plaintiff and Class Members have spent and will continue to spend significant amounts of time to monitor their financial and medical accounts and records for misuse.

103. Plaintiff and Class Members have suffered or will suffer actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

a. Finding fraudulent charges;

b. Canceling and reissuing credit and debit cards;

c. Purchasing credit monitoring and identity theft prevention;

d. Addressing their inability to withdraw funds linked to compromised accounts;

e. Taking trips to banks and waiting in line to obtain funds held in limited accounts;

f. Placing “freezes” and “alerts” with credit reporting agencies;

g. Spending time on the phone with or at a financial institution to dispute fraudulent charges;

h. Contacting financial institutions and closing or modifying financial accounts;

i. Resetting automatic billing and payment instructions from compromised credit and debit cards to new ones;

j. Paying late fees and declined payment fees imposed as a result of failed automatic payments that were tied to compromised cards that had to be cancelled, and;

k. Closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

104. Moreover, Plaintiff and Class Members have an interest in ensuring that their Private Information, which is believed to remain in the possession of Centerstone, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing personal and financial information is not accessible online, that access to such data is password-protected, and that such data is properly encrypted.

105. Further, as a result of Centerstone’s conduct, Plaintiff and Class Members are forced to live with the anxiety that their Private Information—which contains the most intimate details about a person’s life, including what ailments they suffer, whether physical or mental—may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

106. As a direct and proximate result of Centerstone’s actions and inactions, Plaintiff and Class Members have suffered a loss of privacy and either have suffered harm or are at an imminent and increased risk of future harm.

CLASS ALLEGATIONS

107. Plaintiff brings this action pursuant to Rule 23 of the Federal Rules of Civil Procedure on behalf of herself and on behalf of all other persons similarly situated (the "Class").

108. Plaintiff proposes the following Class definitions, subject to amendment as appropriate:

> **Nationwide Class**
> All individuals in the United States who had Private Information stolen as a result of the Data Breach, including all who were sent a notice of the Data Breach.
>
> **Indiana Subclass**
> All residents of Indiana who had Private Information stolen as a result of the Data Breach, including all who were sent a notice of the Data Breach.

109. Excluded from each of the above Classes are Defendant and its parents or subsidiaries, any entities in which it has a controlling interest, as well as its officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns. Also excluded are any Judge to whom this case is assigned as well as his or her judicial staff and immediate family members.

110. Plaintiff reserves the right to modify or amend the definitions of the proposed Classes before the Court determines whether certification is appropriate.

111. Each of the proposed classes meet the criteria for certification under Fed. R. Civ. P. 23(a), (b)(2), and (b)(3).

112. Numerosity**.** The Class Members are so numerous that joinder of all members is impracticable. Though the exact number and identities of Class Members are unknown at this time, based on information and belief, the Class consists of thousands of patients of Centerstone whose data was compromised in the Data Breach. The identities of Class Members are ascertainable through Centerstone's records, Class Members' records, publication notice, self-identification, and other means.

113. Commonality. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Centerstone engaged in the conduct alleged herein;

b. Whether Centerstone's conduct violated the Indiana Deceptive Consumer Sales Act, invoked below;

c. When Centerstone actually learned of the data breach and whether its response was adequate;

d. Whether Centerstone unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' Private Information;

e. Whether Centerstone failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

f. Whether Centerstone's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

g. Whether Centerstone's data security systems prior to and during the Data Breach were consistent with industry standards;

h. Whether Centerstone owed a duty to Class Members to safeguard their Private Information;

i. Whether Centerstone breached its duty to Class Members to safeguard their Private Information;

j. Whether computer hackers obtained Class Members' Private Information in the Data Breach;

k. Whether Centerstone had a legal duty to provide timely and accurate notice of the data breach to Plaintiff and the Class Members;

l. Whether Centerstone breached its duty to provide timely and accurate notice of the data breach to Plaintiff and the Class Members;

m. Whether Centerstone knew or should have known that its data security systems and monitoring processes were deficient;

n. What damages Plaintiff and Class Members suffered as a result of Centerstone's misconduct;

o. Whether Centerstone's conduct was negligent;

p. Whether Centerstone's conduct was *per se* negligent;

q. Whether Centerstone was unjustly enriched;

r. Whether Centerstone breached an implied contract with Plaintiff and Class Members;

s. Whether Plaintiff and Class Members are entitled to actual and/or statutory damages;

t. Whether Plaintiff and the other Class Members are entitled to additional credit or identity monitoring and are entitled to other monetary relief; and

u. Whether Plaintiff and the Class Members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

114. Typicality. Plaintiff's claims are typical of those of other Class Members because Plaintiff's Private Information, like that of every other Class member, was compromised in the Data Breach.

115. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiff's Counsel is competent and experienced in litigating class actions, including data privacy litigation of this kind.

116. Predominance**.** Centerstone has engaged in a common course of conduct toward Plaintiff and Class Members, in that all the Plaintiff's and Class Members' data was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from Centerstone's conduct affecting Class Members set out above predominate over any

individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

117. Superiority**.** A Class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a Class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Centerstone. In contrast, the conduct of this action as a Class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class member.

118. Class certification also is appropriate under Fed. R. Civ. P. 23(b)(2). Centerstone has acted or has refused to act on grounds generally applicable to the Class, so that final injunctive relief or corresponding declaratory relief is appropriate as to the Class as a whole.

119. Finally, all members of the proposed Class are readily ascertainable. Centerstone has access to Class Members' names and addresses affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by Centerstone.

CLAIMS FOR RELIEF

COUNT I
NEGLIGENCE

(On behalf of Plaintiff and the Nationwide Class or alternatively the Indiana Class)

120. Plaintiff restates and realleges all proceeding allegations above and hereafter as if fully set forth herein.

121. Centerstone knowingly collected, came into possession of, and maintained Plaintiff's and Class Members' Private Information, and had a duty to exercise reasonable care in

safeguarding, securing and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties.

122. Centerstone experienced a nearly identical data breach in 2019 and agreed to a settlement as a result of a class action complaint only months prior to the data breach in early November 2021.

123. Centerstone knew, or should have known, of the risks inherent in collecting the Private Information of Plaintiff and the Class Members and the importance of adequate security. Centerstone was on notice due to its own data breach, and knew or should have known that healthcare entities are an attractive target for cyberattacks.

124. Centerstone owed a duty of care to Plaintiff and the Class Members whose Private Information was entrusted to it. Centerstone's duties included, but were not limited to, the following:

a. To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting Private Information in its possession;
b. To protect customers' Private Information using reasonable and adequate security procedures and systems that are compliant with the industry standards;
c. To have procedures in place to prevent the loss or unauthorized dissemination of Private Information in its possession;
d. To employ reasonable security measures and otherwise protect the Private Information of Plaintiff and Class Members pursuant to the Indiana Deceptive Consumer Sales Act;
e. To implement processes to quickly detect a data breach and to timely act on warnings about data breaches, and
f. To promptly notify Plaintiff and the Class Members of the data breach, and to disclose precisely the type(s) of information compromise.

125. Centerstone knew based on the 2019 data breach that *another* breach of its systems could damage thousands of its patients, including Plaintiff and the Class Members, and therefore had a duty to adequately protect their Private Information.

126. Plaintiff and the Class Members were foreseeable and probable victims of any inadequate security practices, and Centerstone owed them a duty of care not to subject them to an unreasonable risk of harm.

127. As a result of the 2019 data breach, Centerstone knew, or should have known, that its computer systems did not adequately safeguard the Private Information of Plaintiff and the Class Members.

128. Centerstone, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class members by failing to exercise reasonable care in protecting and safeguarding Plaintiff's and Class Members' Private Information within Centerstone's possession.

129. Centerstone, by its actions and/or omissions, breached its duty of care by failing to provide, or by acting with reckless disregard for, fair, reasonable, or adequate computer systems and data security practices to safeguard the Private Information of Plaintiff and the Class Members.

130. Centerstone, by its actions and/or omissions, breached its duty of care by failing to promptly identify the Data Breach and then provide prompt notice of the Data Breach (at the longest within 60 days of learning of the breach) to the persons whose Private Information was compromised. By failing to provide prompt and adequate individual notice of the data breach, Centerstone acted with reckless disregard for the rights of Plaintiff and the Class Members because by failing to provide notice Centerstone prevented Plaintiff and the Class Members from taking measures to protect themselves from damages caused by the fraudulent use of the Private Information compromised in the data breach.

131. Centerstone had a special relationship with Plaintiff and the Class Members. Plaintiff's and the Class Members' willingness to entrust Centerstone with their Private Information was predicated on the understanding that Centerstone would take adequate security

precautions. Moreover, only Centerstone had the ability to protect its systems (and the Private Information that it stored on them) from attack.

132. Centerstone's breach of duties owed to Plaintiff and Class Members caused Plaintiff's and Class Members' Private Information to be compromised.

133. As a result of Centerstone's ongoing failure to notify Plaintiff and Class Members regarding exactly what Private Information has been compromised, Plaintiff and Class Members are unable to take all the necessary precautions to mitigate damages by preventing future fraud.

134. Centerstone's breaches of duty caused a foreseeable risk of harm to Plaintiff and Class Members to suffer from identity theft, loss of time and money to monitor their finances for fraud, and loss of control over their Private Information.

135. As a result of Centerstone's negligence and breach of duties, Plaintiff and Class Members are in danger of imminent harm in that their Private Information, which is still in the possession of third parties, and will be used for fraudulent purposes.

136. Centerstone also had independent duties under state laws that required it to reasonably safeguard Plaintiff's and the Class Members' Private Information and promptly notify them about the data breach.

137. But for Centerstone's wrongful and negligent breach of the duties it owed Plaintiff and the Class Members, their Private Information either would not have been compromised or they would have been able to prevent some or all of their damages.

138. As a direct and proximate result of Centerstone's negligent conduct, Plaintiff and the Class Members have suffered damages and are at imminent risk of further harm.

139. The injury and harm that Plaintiff and the Class Members suffered (as alleged above) was reasonably foreseeable.

140. The injury and harm that Plaintiff and the Class Members suffered (as alleged above) was the direct and proximate result of Centerstone's negligent conduct.

141. Plaintiff and the Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

142. In addition to monetary relief, Plaintiff and the Class Members also are entitled to injunctive relief requiring Centerstone to, *inter alia*, strengthen its data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiff and the Class Members.

COUNT II
NEGLIGENCE *PER SE*
(On behalf of Plaintiff and the Nationwide Class or alternatively the Indiana Class)

143. Plaintiff restates and realleges the allegations in paragraphs 1-119 as if fully set forth herein.

144. Pursuant to Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45, the Tennessee Consumer Protection Act of 1977 ("Tenn. CPA"), Tenn. Code § 47-18- 104 and the Indiana Deceptive Consumer Sales Act ("IDCSA"), Ind. Code § 24-5-0.5-3(a), Centerstone had a duty to provide fair and adequate computer systems and data security to safeguard the Private Information, including PII and PHI, of Plaintiff and the Class Members.

145. Plaintiff and the Class Members are within the class of persons that the FTCA, the Tenn. CPA and the IDCSA were intended to protect.

146. The FTCA prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice of failing to use reasonable measures to protect Private Information. The FTC publications described above, and the industry standard data and cybersecurity measures, also form part of the basis of Centerstone's duty in this regard.

147. Centerstone violated the FTCA by failing to use reasonable measures to protect Private Information of Plaintiff and the Class and not complying with applicable industry standards, as described herein.

148. Centerstone's violations of the FTCA, Tenn. CPA and IDCSA constitutes negligence *per se*.

149. In connection with its consumer transactions, Centerstone engaged in unfair, abusive or deceptive acts, omissions or practices by, misrepresenting material facts to Plaintiff and the Class, in connection with providing health care services, by representing that Centerstone did

and would comply with the requirements of relevant federal and state law pertaining to the privacy and security of Plaintiff and the Class Members' Private Information, such requirements included, but are not limited to, those imposed by laws such as the FTCA, Tenn. CPA and IDCSA.

150. It was reasonably foreseeable, particularly given the growing number of data breaches of health information, and its own recent data breach in 2019, that the failure to reasonably protect and secure Plaintiff's and Class Members' Private Information in compliance with applicable laws would result in an unauthorized third-party gaining access to Centerstone's email servers, networks, databases, and/or computers that stored or contained Plaintiff's and Class Members' Private Information.

151. Plaintiff's and Class Members' Private Information constitutes personal property that was stolen due to Centerstone's negligence, resulting in harm, injury and damages to Plaintiff and Class Members.

152. As a direct and proximate result of Centerstone's negligence *per se*, Plaintiff and the Class have suffered, and continue to suffer, injuries and damages arising from the unauthorized access of their Private Information, including PII and PHI, as a result of the data breach including but not limited to damages from lost time and effort to mitigate the actual and potential impact of the data breach on their lives.

153. Centerstone breached its duties to Plaintiff and the Class under these laws by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and the Class Members' Private Information.

154. But for Centerstone'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.

155. The injury and harm suffered by Plaintiff and the Class Members was the reasonably foreseeable result of Centerstone's breach of its duties. As a result of its 2019 data breach and resulting settlement in August 2021, Centerstone knew or should have known that it was failing to meet its duties, and that Centerstone's breach would cause Plaintiff and the Class

Members to experience the foreseeable harms associated with the exposure of their Private Information only a few months later in November 2021.

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

157. In addition to monetary relief, Plaintiff and the Class Members also are entitled to injunctive relief requiring Centerstone to, *inter alia*, strengthen its data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiff and the Class Members.

COUNT III
BREACH OF CONTRACT
(On behalf of Plaintiff and the Nationwide Class or alternatively the Indiana Class)

158. Plaintiff restates and realleges the allegations in paragraphs 1-119 as if fully set forth herein.

159. Plaintiff and Class Members entered into a valid and enforceable contract when they paid money to Centerstone in exchange for services, which included promises to secure, safeguard, protect, keep private, and not disclose Plaintiff's and Class Members' Private Information.

160. Centerstone's Privacy Notice, effective September 14, 2020, memorialized the rights and obligations of Centerstone and its patients. The Privacy Notice includes a Client's Acknowledgment page, which has a signature line for the patients. On information and belief, Centerstone requires all patients, or their guardians, including Plaintiff, to sign the Privacy Notice on the Client's Acknowledgment page.

161. This document was provided to Plaintiff in a manner and during a time where it became part of the agreement for services.

162. In the Privacy Notice, Centerstone commits to protecting the privacy and security of medical and mental health information and promises to never share patient information unless given written permission or if state or federal law requires it.

163. Centerstone further states in the Privacy Notice that it is required by law to maintain the privacy and security of PHI and promises not to use or share PHI other than as described in the Privacy Notice.

164. Centerstone also promises in the Privacy Notice that it will notify patients promptly if a breach occurs. It then clarifies that "[i]n no event will notification be more than 60 days from the date of the breach."

165. Centerstone promised to comply with all HIPAA standards, state and federal law, and to ensure Plaintiff's and Class Members' patient information and PHI was protected, secured, kept private, and not disclosed.

166. Plaintiff and the Class Members fully performed their obligations under their contracts with Centerstone.

167. Centerstone did not secure, safeguard, protect, and/or keep private Plaintiff' and Class Members' PHI and/or it disclosed their PHI to third parties, and therefore Centerstone breached its contract with Plaintiff and Class Members.

168. Centerstone allowed third parties to access, copy, and/or transfer Plaintiff's and Class Members' health information and PHI, without permission, and therefore Centerstone breached its contracts with Plaintiff and Class Members.

169. In addition, Centerstone failed to provide adequate notice of the Data Breach within 60 days from the date the breach was discovered in February 2022, which further breached its obligations to Plaintiff and Class Members.

170. Centerstone's failure to satisfy its confidentiality and privacy obligations resulted in Centerstone providing services to Plaintiff and Class Members that were of a diminished value.

171. As a result, Plaintiff and Class Members have been harmed, damaged, and/or injured as described herein.

172. In addition to monetary relief, Plaintiff and the Class Members also are entitled to injunctive relief requiring Centerstone to, *inter alia*, strengthen its data security systems and

monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiff and the Class Members.

COUNT IV
BREACH OF IMPLIED CONTRACT
(On behalf of Plaintiff and the Nationwide Class or alternatively the Indiana Class)

173. Plaintiff restates and realleges the allegations in paragraphs 1-119 as if fully set forth herein.

174. Through their course of conduct, Centerstone, Plaintiff, and Class Members entered into implied contracts for the provision of medical care and treatment, as well as implied contracts for Centerstone to implement data security adequate to safeguard and protect the privacy of Plaintiff and Class Members' Private Information, and timely notify them in the event of a data breach.

175. Specifically, Plaintiff and Class Members entered into valid and enforceable implied contracts with Centerstone when they first went for medical care and treatment at one of Centerstone's facilities.

176. The valid and enforceable implied contracts to provide medical and health care services that Plaintiff and Class Members entered into with Centerstone include Centerstone's promise to protect Private Information given to Centerstone or that Centerstone create on its own from disclosure.

177. An implicit part of the offer was that Centerstone would safeguard the Private Information using reasonable or industry-standard means and would timely notify Plaintiff and the Class Members in the event of a data breach.

178. Plaintiff and Class Members accepted Centerstone's offer and provided their Private Information to Centerstone.

179. In entering into such implied contracts, Plaintiff and Class Members reasonably believed and expected that Centerstone's data security practices complied with relevant laws and regulations, including HIPAA, and were consistent with industry standards.

180. Under the implied contracts, Centerstone and/or their affiliated healthcare providers, promised and were obligated to: (a) provide healthcare to Plaintiff and Class Members; and (b) protect Plaintiff's and the Class Members' PII/PHI: (i) provided to obtain such healthcare; and/or (ii) created as a result of providing such healthcare. In exchange, Plaintiff and Members of the Class agreed to pay money for these services, and to turn over their Private Information.

181. Centerstone also affirmatively represented in its Privacy Policy that it protected the Private Information of Plaintiff and the Class Members in several ways, as described above.

182. Plaintiff and Class Members who paid money to Centerstone reasonably believed and expected that Centerstone would use part of those funds to obtain adequate data security. Centerstone failed to do so.

183. Plaintiff and the Class Members would not have provided their Private Information to Centerstone had they known that Centerstone would not safeguard their Private Information as promised or provide timely notice of a data breach.

184. Both the provision of medical services and the protection of Plaintiff's and Class Members' Private Information were material aspects of these implied contracts.

185. The implied contracts for the provision of medical services – contracts that include the contractual obligations to maintain the privacy of Plaintiff's and Class Members' Private Information—are also acknowledged, memorialized, and embodied in multiple documents, including (among other documents) Centerstone's Privacy Notice.

186. Centerstone's express representations, including, but not limited to the express representations found in the Privacy Notice, memorialize and embody the implied contractual obligation requiring Centerstone to implement data security adequate to safeguard and protect the privacy of Plaintiff's and Class Members' Private Information.

187. Consumers of healthcare value their privacy, the privacy of their dependents, and the ability to keep their Private Information associated with obtaining healthcare private. To customers such as Plaintiff and Class Members, healthcare that does not adhere to industry standard data security protocols to protect Private Information is fundamentally less useful and

less valuable than healthcare that adheres to industry-standard data security. Plaintiff and Class Members would not have entrusted their Private Information to Centerstone and entered into these implied contracts with Centerstone and/or their affiliated healthcare providers without an understanding that their Private Information would be safeguarded and protected, or entrusted their Private Information to Centerstone in the absence of its implied promise to monitor their computer systems and networks to ensure that it adopted reasonable data security measures.

188. Plaintiff and the Class Members fully performed their obligations under the implied contracts with Centerstone.

189. Centerstone materially breached the implied contracts by failing to safeguard Plaintiff's and the Class Members' Private Information and failing to provide them with timely and accurate notice when their Private Information was compromised in the data breach.

190. Centerstone materially breached the terms of the implied contracts, including, but not limited to, the terms stated in the Privacy Notice. Centerstone did not comply with industry standards, standards of conduct embodied in statutes like HIPAA and Section 5 of the FTCA, or otherwise protect Plaintiff's and the Class Members' Private Information, as set forth above.

191. The Data Breach was a reasonably foreseeable consequence of Centerstone's actions in breach of these contracts.

192. The losses and actual damages Plaintiff and the Class Members have suffered and will continue to suffer (as described above) were the direct and proximate result of Centerstone's breaches of its implied contracts with them.

193. Plaintiff and the Class Members also are entitled to injunctive relief requiring Centerstone to, *inter alia*, strengthen its data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiff and the Class Members.

COUNT V
VIOLATION OF TENNESEE CONSUMER PROTECTION ACT OF 1977
TENN. CODE ANN. §§ 47-18-101, *ET SEQ.*
(On behalf of Plaintiff and the Nationwide Class)

194. Plaintiff restates and realleges the allegations in paragraphs 1-119 as if fully set forth herein.

195. Plaintiff and Class Members are "natural persons" and "consumers" within the meaning of Tenn. Code § 47-18-103(2).

196. Centerstone is engaged in "trade" or "commerce" or "consumer transactions" within the meaning Tenn. Code § 47-18-103(9).

197. The Tenn. CPA prohibits "unfair or deceptive acts or practices affecting the conduct of any trade or commerce." Tenn. Code § 47-18- 104.

198. By the acts and conduct alleged herein, Centerstone committed unfair or deceptive acts and practices by:

a. failing to maintain adequate computer systems and data security practices to safeguard Private Information;
b. making and using false promises, set out in the Privacy Notice, about the privacy and security of Private Information of Plaintiff and Class Members;
c. failing to disclose that their computer systems and data security practices were inadequate to safeguard Private Information from theft;
d. continuing to gather and store Private Information and other PII and PHI after Centerstone knew or should have known about the Data Breach without publicly disclosing the Data Breach; and
e. continuing to gather and store Private Information and other PII and PHI after Centerstone knew or should have known of the security vulnerabilities of their computer systems that were exploited in the Data Breach and before Centerstone remediated the security vulnerabilities, without publicly disclosing the Data Breach.

199. These unfair acts and practices violated duties imposed by laws, including but not limited to the FTCA, HIPAA, and Tenn. CPA.

200. The foregoing deceptive acts and practices were directed at consumers.

201. The foregoing deceptive acts and practices are misleading in a material way because they fundamentally misrepresent the character of the services provided, specifically as to the safety and security of Private Information.

202. Centerstone's unconscionable commercial practices, false promises, misrepresentations, and omissions set forth in this Complaint are material in that they relate to matters which reasonable persons, including Plaintiff and members of the Class, would attach importance to in making their decisions and/or conducting themselves regarding the services received from Centerstone.

203. Plaintiff and Class members are consumers who made payments to Centerstone for the furnishing of healthcare services that were primarily for personal, family, or household purposes.

204. Centerstone engaged in the conduct alleged in this Complaint, entering into transactions intended to result, and which did result, in the furnishing of employment benefit services to consumers, including Plaintiff and Class Members.

205. Centerstone engaged in, and its acts and omissions affect, trade and commerce, or the furnishing of services in the State of Tennessee.

206. Centerstone's acts, practices, and omissions were done in the course of Centerstone's business of furnishing healthcare services and overseeing subsidiaries from its headquarters located in the State of Tennessee. On information and belief, Centerstone subsidiaries used a centralized server for their employee email system located at the Centerstone headquarters in Tennessee.

207. As a direct and proximate result of Centerstone's multiple, separate violations of the Tenn. CPA, Plaintiff and the Class Members suffered damages including, but not limited to: (i) the compromise, publication, and/or theft of their Private Information; (ii) out-of-pocket

expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Private Information; (iii) 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; (iv) the continued risk to their Private Information, which remains in Centerstone's possession and is subject to further unauthorized disclosures so long as Centerstone fails to undertake appropriate and adequate measures to protect the Private Information in its continued possession; (v) 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 Plaintiffs and Class Members; and (vi) the diminished value of Centerstone's services they received.

208. Also, as a direct result of Centerstone's violation of the Tenn. CPA, Plaintiff and the Class Members are entitled to damages as well as injunctive relief, including, but not limited to, ordering Centerstone to: (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide lifetime credit monitoring and identity theft insurance to Plaintiff and the Class Members.

209. Plaintiffs bring this action on behalf of themselves and Class Members for the relief requested above and for the public benefit in order to promote the public interests in the provision of truthful, fair information to allow consumers to make informed purchasing decisions and to protect Plaintiff, Class Members and the public from Centerstone's unfair, deceptive, and unlawful practices. Centerstone's wrongful conduct as alleged in this Complaint has had widespread impact on the public at large.

210. Centerstone knew or should have known that its computer systems and data security practices were inadequate to safeguard Class Members' Private Information, based on the 2019 data breach, and that the risk of a data security incident was high.

211. Plaintiff and Class Members were injured because: a) they would not have paid for healthcare services from Centerstone had they known the true nature and character of

Centerstone's data security practices; b) Plaintiff and Class Members would not have entrusted their Private Information to Centerstone in the absence of promises that Centerstone would keep their information reasonably secure, and c) Plaintiff and Class Members would not have entrusted their Private Information to Centerstone in the absence of the promise to monitor its computer systems and networks to ensure that it adopted reasonable data security measures.

212. As a result, Plaintiff and the Class Members have been damaged in an amount to be proven at trial.

213. On behalf of themselves and other members of the Class, Plaintiff seek to enjoin the unlawful acts and practices described herein, to recover his actual damages, three times actual damages, and reasonable attorneys' fees.

COUNT VI
VIOLATION OF INDIANA DECEPTIVE CONSUMER SALES ACT
IND. CODE §§ 24-5-0.5-0.1, *ET SEQ.*
(On behalf of Plaintiff and the Indiana Class)

214. Plaintiff restates and realleges the allegations in paragraphs 1-119 as if fully set forth herein.

215. Indiana's Deceptive Consumer Sales Act, Ind. Code § 24-5-0.5-3(a) ("IDCSA") prohibits suppliers from engaging in deceptive, unfair, and abusive acts or omissions in consumer transactions.

216. Centerstone is a "supplier" of consumer services as provided by Ind. Code § 24-5-0.5-2. Plaintiff and Class Members are "consumers" of Centerstone's services.

217. Centerstone engaged in deceptive, unfair, and unlawful trade acts or practices in the conduct of "consumer transactions," in violation of the IDCSA. As a regular part of its business, Centerstone operates health care facilities in Indiana. It accepts payments from customers, like Plaintiff, for Centerstone services. On information and belief, consumer transactions were processed in Indiana and health care services were performed in Indiana.

218. In connection with its consumer transactions, Centerstone engaged in unfair, abusive or deceptive acts, omissions or practices by, *inter alia*, engaging in the following conduct:

a. failing to maintain sufficient security to keep Plaintiff's and the Class Members' sensitive Private Information from being hacked and stolen;

b. misrepresenting material facts to Plaintiff and the Class Members, in connection with providing health care services, by representing that it would maintain adequate data privacy and security practices and procedures to safeguard Plaintiff's and the Class Members' Private Information as contained in its Privacy Policy;

c. misrepresenting material facts to Plaintiff and the Class, in connection with providing health care services, by representing that Centerstone did and would comply with the requirements of relevant federal and state law pertaining to the privacy and security of Plaintiff and the Class Members' Private Information, such requirements included, but are not limited to, those imposed by laws such as the Federal Trade Commission Act (15 U.S.C. § 45) and Indiana's data breach statute (Ind. Code § 24-4.9-3.5); and

d. failing to take proper action following the Data Breach to enact adequate privacy and security measures and protect Plaintiff and the Class Members' Private Information and other personal information from further unauthorized disclosure, release, data breaches, and theft.

219. Centerstone knew that its computer systems and data security practices were inadequate to safeguard Plaintiff's and the Class Members' Private Information and that risk of a data breach or theft was highly likely. Nevertheless, it did nothing to warn Plaintiff and the Class Members about its data insecurities, and instead affirmatively promised that it would maintain adequate security. This was a deliberate effort to mislead consumers, such as Plaintiff and the Class Members, in order to encourage them to receive health care services even while Centerstone knew that its consumers' sensitive Private Information was vulnerable.

220. The above unfair and deceptive practices and acts or omissions by Centerstone were done as a part of a scheme, artifice, or device with intent to defraud or mislead and constitute incurable deceptive acts under the IDCSA.

221. As a direct and proximate result of Centerstone's deceptive trade practices, Plaintiff and the Class Members suffered damages and injuries, including the loss of their legally protected interest in the confidentiality and privacy of their Private Information.

222. As a direct and proximate result of Centerstone's deceptive trade practices, Plaintiff and the Class Members are now likely to suffer identity theft crimes, and face a lifetime risk of identity theft crimes.

223. Plaintiff and the Class Members seek relief under Ind. Code § 24-5-0.5-4, including, but not limited to damages, restitution, penalties, injunctive relief, and/or attorneys' fees and costs.

224. Plaintiff and the Class Members injured by Defendant's unfair and deceptive trade practices also seek treble damages pursuant to Ind. Code §24-5-0.5-4(i).

COUNT VII
INTRUSION UPON SECLUSION / INVASION OF PRIVACY
(On behalf of Plaintiff and the Nationwide Class or alternatively the Indiana Class)

225. Plaintiff restates and realleges the allegations in paragraphs 1-119 as if fully set forth herein.

226. Plaintiff and Class Members maintain a privacy interest in their Private Information, which is private, confidential information that is also protected from disclosure by applicable laws set forth above.

227. Plaintiff and Class Members' Private Information was contained, stored, and managed electronically in Centerstone's records, computers, and databases that was intended to be secured from unauthorized access to third-parties because it contained highly sensitive, confidential matters regarding Plaintiff's and Class Members' identities, unique identification numbers, medical histories, treatment records, and financial records that were only shared with

Centerstone for the limited purpose of obtaining and paying for healthcare, medical goods and services.

228. Additionally, Plaintiff's and Class Members' Private Information, when contained in electronic form, is highly attractive to criminals who can nefariously use their Private Information for fraud, identity theft, and other crimes without their knowledge and consent.

229. Centerstone's disclosure of Plaintiff's and Class Members' Private Information to unauthorized third parties as a result of its failure to adequately secure and safeguard their Private Information is offensive to a reasonable person. Centerstone's disclosure of Plaintiff's and Class Members' Private Information to unauthorized third parties permitted the physical and electronic intrusion into Plaintiff's and Class Members' private quarters where their Private Information was stored and disclosed private facts about their health into the public domain.

230. Plaintiff and Class Members have been damaged by Centerstone's conduct, including by paying for data and cybersecurity protection that they did not receive, as well as by incurring the harms and injuries arising from the Data Breach now and in the future.

COUNT VIII
UNJUST ENRICHMENT
(On behalf of Plaintiff and the Nationwide Class or alternatively the Indiana Class)

231. Plaintiff restates and realleges the allegations in paragraphs 1-119 as if fully set forth herein.

232. This count is plead in the alternative to Count III above.

233. Centerstone has retained the benefits of its unlawful conduct including the amounts received for data and cybersecurity practices that it did not provide. Due to Centerstone's conduct alleged herein, it would be unjust and inequitable under the circumstances for Centerstone to be permitted to retain the benefit of its wrongful conduct.

234. Plaintiff and Class Members are entitled to full refunds, restitution and/or damages from Centerstone and/or an order of this Court proportionally disgorging all profits, benefits, and other compensation obtained by Centerstone from its wrongful conduct. If necessary, the

establishment of a constructive trust from which the Plaintiff and Class Members may seek restitution or compensation may be created.

235. Additionally, Plaintiff and the Class Members may not have an adequate remedy at law against Centerstone, and accordingly plead this claim for unjust enrichment in addition to or, in the alternative to, other claims pleaded herein.

236. Plaintiff and members of the Nationwide class conferred a benefit on Centerstone by paying for data and cybersecurity procedures to protect their Private Information that they did not receive.

COUNT IX
DECLARATORY JUDGMENT
(On behalf of Plaintiff and the Nationwide Class or alternatively the Indiana Class)

237. Plaintiff restates and realleges the allegations in paragraphs 1-119 as if fully set forth herein.

238. Under the Declaratory Judgment Act, 28 U.S.C. § 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statute described in this Complaint.

239. Centerstone owes a duty of care to Plaintiff and the Class Members which required it to adequately secure Private Information.

240. Centerstone still possesses Private Information regarding Plaintiff and the Class Members.

241. Plaintiff alleges that Centerstone's data security measures remain inadequate. Furthermore, Plaintiff continues to suffer injury as a result of the compromise of her Private Information and remain at imminent risk that further compromises of her Private Information will occur in the future.

242. Under its authority pursuant to the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Centerstone owes a legal duty to secure patients' Private Information and to timely notify patients of a data breach under the common law and Section 5 of the FTCA;

b. Centerstone's existing security measures do not comply with its explicit or implicit contractual obligations and duties of care to provide reasonable security procedures and practices appropriate to the nature of the information to protect patients' Private Information; and

c. Centerstone continues to breach this legal duty by failing to employ reasonable measures to secure patients' Private Information.

243. This Court also should issue corresponding prospective injunctive relief requiring Centerstone to employ adequate security protocols consistent with law and industry standards to protect patients' Private Information, including the following:

a. Order Centerstone to provide lifetime credit monitoring and identity theft insurance to Plaintiff and the Class Members.

b. Order Centerstone to comply with its explicit or implicit contractual obligations and duties of care, Centerstone must implement and maintain reasonable security measures, including, but not limited to:

i. engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Centerstone's systems on a periodic basis, and ordering Centerstone to promptly correct any problems or issues detected by such third-party security auditors;

ii. engaging third-party security auditors and internal personnel to run automated security monitoring;

iii. auditing, testing, and training its security personnel regarding any new or modified procedures;

iv. segmenting its user applications by, among other things, creating firewalls and access controls so that if one area is compromised, hackers cannot gain access to other portions of Centerstone's systems;

v. conducting regular database scanning and securing checks;

vi. routinely and continually conducting 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;

vii. meaningfully educating its users about the threats they face as a result of the loss of their Private Information to third parties, as well as the steps Centerstone's patients must take to protect themselves.

244. If an injunction is not issued, Plaintiff will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at Centerstone. The risk of another such breach is real, immediate, and substantial, particularly in light of the fact that this data breach occurred only a few months after Centerstone's settlement as a result of the 2019 data breach. If another breach at Centerstone occurs, Plaintiff will not have an adequate remedy at law because many of the resulting injuries are not readily quantifiable.

245. The hardship to Plaintiff if an injunction does not issue exceeds the hardship to Centerstone if an injunction is issued. Plaintiff will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to Centerstone of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Centerstone has a pre-existing legal obligation to employ such measures.

246. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing *a third* data breach at Centerstone, thus eliminating the additional injuries that would result to Plaintiff and patients whose Private Information would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and the Classes described above, seek the following relief:

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

b. Judgment in favor of Plaintiff and the Class Members awarding them appropriate monetary relief, including actual damages, statutory damages, equitable relief, restitution, disgorgement, and statutory costs;

c. An order providing injunctive and other equitable relief as necessary to protect the interests of the Classes as requested herein;

d. An order instructing Centerstone to purchase or provide funds for lifetime credit monitoring and identity theft insurance to Plaintiff and the Class Members;

e. An order requiring Centerstone to pay the costs involved in notifying the Class Members about the judgment and administering the claims process;

f. A judgment in favor of Plaintiff and the Classes awarding them pre-judgment and post judgment interest, reasonable attorneys' fees, costs and expenses as allowable by law, and

g. An award of such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury on all triable issues.

DATED: August 29, 2022

Respectfully submitted,

By: /s/ *Edwin E. Wallis III*

Edwin E. Wallis III (TN #23950)
GLASSMAN, WYATT, TUTTLE & COX, P.C.
26 North Second Street
Memphis, Tennessee 38103
Tel: (901) 527-4673
Fax: (901) 521-0940
E: ewallis@gwtclaw.com

SIRI & GLIMSTAD LLP
Mason A. Barney (*pro hac vice* to be filed)
Sean Nation (*pro hac vice* to be filed)
Ursula Smith (*pro hac vice* to be filed)
745 Fifth Avenue, Suite 500
New York, New York 10151
Tel: (212) 532-1091
E: mbarney@sirillp.com
E: snation@sirillp.com
E: usmith@sirillp.com

JS 44 (Rev. 04/21)

CIVIL COVER SHEET

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. *(SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)*

I. (a) PLAINTIFFS

Sara Riley

(b) County of Residence of First Listed Plaintiff Scott County, IN
(EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys *(Firm Name, Address, and Telephone Number)*
Edwin E. Wallis III, Esq. / Glassman, Wyatt, Tuttle & Cox, P.C.
26 N. Second Street, Memphis, TN 38103
(901) 527-4673

DEFENDANTS

Centerstone Of America, Inc.; Centerstone Of Indiana, Inc.; and Centerstone Of Tennessee, Inc.

County of Residence of First Listed Defendant Davidson County, TN
(IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

Attorneys *(If Known)*

II. BASIS OF JURISDICTION *(Place an "X" in One Box Only)*

- ☐ 1 U.S. Government Plaintiff
- ☐ 3 Federal Question *(U.S. Government Not a Party)*
- ☐ 2 U.S. Government Defendant
- ☒ 4 Diversity *(Indicate Citizenship of Parties in Item III)*

III. CITIZENSHIP OF PRINCIPAL PARTIES *(Place an "X" in One Box for Plaintiff and One Box for Defendant)*

(For Diversity Cases Only)

	PTF	DEF		PTF	DEF
Citizen of This State	☐ 1	☐ 1	Incorporated *or* Principal Place of Business In This State	☐ 4	☒ 4
Citizen of Another State	☒ 2	☐ 2	Incorporated *and* Principal Place of Business In Another State	☐ 5	☐ 5
Citizen or Subject of a Foreign Country	☐ 3	☐ 3	Foreign Nation	☐ 6	☐ 6

IV. NATURE OF SUIT *(Place an "X" in One Box Only)*

Click here for: Nature of Suit Code Descriptions.

CONTRACT
- ☐ 110 Insurance
- ☐ 120 Marine
- ☐ 130 Miller Act
- ☐ 140 Negotiable Instrument
- ☐ 150 Recovery of Overpayment & Enforcement of Judgment
- ☐ 151 Medicare Act
- ☐ 152 Recovery of Defaulted Student Loans (Excludes Veterans)
- ☐ 153 Recovery of Overpayment of Veteran's Benefits
- ☐ 160 Stockholders' Suits
- ☐ 190 Other Contract
- ☐ 195 Contract Product Liability
- ☐ 196 Franchise

TORTS

PERSONAL INJURY
- ☐ 310 Airplane
- ☐ 315 Airplane Product Liability
- ☐ 320 Assault, Libel & Slander
- ☐ 330 Federal Employers' Liability
- ☐ 340 Marine
- ☐ 345 Marine Product Liability
- ☐ 350 Motor Vehicle
- ☐ 355 Motor Vehicle Product Liability
- ☒ 360 Other Personal Injury
- ☐ 362 Personal Injury - Medical Malpractice

PERSONAL INJURY
- ☐ 365 Personal Injury - Product Liability
- ☐ 367 Health Care/ Pharmaceutical Personal Injury Product Liability
- ☐ 368 Asbestos Personal Injury Product Liability

PERSONAL PROPERTY
- ☐ 370 Other Fraud
- ☐ 371 Truth in Lending
- ☐ 380 Other Personal Property Damage
- ☐ 385 Property Damage Product Liability

FORFEITURE/PENALTY
- ☐ 625 Drug Related Seizure of Property 21 USC 881
- ☐ 690 Other

LABOR
- ☐ 710 Fair Labor Standards Act
- ☐ 720 Labor/Management Relations
- ☐ 740 Railway Labor Act
- ☐ 751 Family and Medical Leave Act
- ☐ 790 Other Labor Litigation
- ☐ 791 Employee Retirement Income Security Act

IMMIGRATION
- ☐ 462 Naturalization Application
- ☐ 465 Other Immigration Actions

BANKRUPTCY
- ☐ 422 Appeal 28 USC 158
- ☐ 423 Withdrawal 28 USC 157

INTELLECTUAL PROPERTY RIGHTS
- ☐ 820 Copyrights
- ☐ 830 Patent
- ☐ 835 Patent - Abbreviated New Drug Application
- ☐ 840 Trademark
- ☐ 880 Defend Trade Secrets Act of 2016

SOCIAL SECURITY
- ☐ 861 HIA (1395ff)
- ☐ 862 Black Lung (923)
- ☐ 863 DIWC/DIWW (405(g))
- ☐ 864 SSID Title XVI
- ☐ 865 RSI (405(g))

FEDERAL TAX SUITS
- ☐ 870 Taxes (U.S. Plaintiff or Defendant)
- ☐ 871 IRS—Third Party 26 USC 7609

OTHER STATUTES
- ☐ 375 False Claims Act
- ☐ 376 Qui Tam (31 USC 3729(a))
- ☐ 400 State Reapportionment
- ☐ 410 Antitrust
- ☐ 430 Banks and Banking
- ☐ 450 Commerce
- ☐ 460 Deportation
- ☐ 470 Racketeer Influenced and Corrupt Organizations
- ☐ 480 Consumer Credit (15 USC 1681 or 1692)
- ☐ 485 Telephone Consumer Protection Act
- ☐ 490 Cable/Sat TV
- ☐ 850 Securities/Commodities/ Exchange
- ☐ 890 Other Statutory Actions
- ☐ 891 Agricultural Acts
- ☐ 893 Environmental Matters
- ☐ 895 Freedom of Information Act
- ☐ 896 Arbitration
- ☐ 899 Administrative Procedure Act/Review or Appeal of Agency Decision
- ☐ 950 Constitutionality of State Statutes

REAL PROPERTY
- ☐ 210 Land Condemnation
- ☐ 220 Foreclosure
- ☐ 230 Rent Lease & Ejectment
- ☐ 240 Torts to Land
- ☐ 245 Tort Product Liability
- ☐ 290 All Other Real Property

CIVIL RIGHTS
- ☐ 440 Other Civil Rights
- ☐ 441 Voting
- ☐ 442 Employment
- ☐ 443 Housing/ Accommodations
- ☐ 445 Amer. w/Disabilities - Employment
- ☐ 446 Amer. w/Disabilities - Other
- ☐ 448 Education

PRISONER PETITIONS

Habeas Corpus:
- ☐ 463 Alien Detainee
- ☐ 510 Motions to Vacate Sentence
- ☐ 530 General
- ☐ 535 Death Penalty

Other:
- ☐ 540 Mandamus & Other
- ☐ 550 Civil Rights
- ☐ 555 Prison Condition
- ☐ 560 Civil Detainee - Conditions of Confinement

V. ORIGIN *(Place an "X" in One Box Only)*

☒ 1 Original Proceeding ☐ 2 Removed from State Court ☐ 3 Remanded from Appellate Court ☐ 4 Reinstated or Reopened ☐ 5 Transferred from Another District *(specify)* ☐ 6 Multidistrict Litigation - Transfer ☐ 8 Multidistrict Litigation - Direct File

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing ***(Do not cite jurisdictional statutes unless diversity)***:
28 U.S.C. § 1332(d)(2)

Brief description of cause:
Failure to safeguard patients' private information and failure to provide timely and adequate notice of unauthorized access to this information

VII. REQUESTED IN COMPLAINT:

☒ CHECK IF THIS IS A **CLASS ACTION** UNDER RULE 23, F.R.Cv.P.

DEMAND $

CHECK YES only if demanded in complaint:
JURY DEMAND: ☒ Yes ☐ No

VIII. RELATED CASE(S) IF ANY

(See instructions): JUDGE _____ DOCKET NUMBER _____

DATE
08/29/2022

SIGNATURE OF ATTORNEY OF RECORD
/s/ Edwin E. Wallis III

FOR OFFICE USE ONLY

RECEIPT # _____ AMOUNT _____ APPLYING IFP _____ JUDGE _____ MAG. JUDGE _____