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

CODY KENNEY and MELISSA SKINNER, individually and on behalf of all similarly situated persons, Plaintiffs, v. CENTERSTONE OF AMERICA, INC., CENTERSTONE OF INDIANA, INC., and CENTERSTONE OF TENNESSEE, INC., Defendants.	**CASE NO.** **CLASS ACTION COMPLAINT FOR DAMAGES, EQUITABLE, DECLARATORY AND INJUNCTIVE RELIEF** **JURY DEMAND**

CLASS ACTION COMPLAINT

Plaintiffs Cody Kenney and Melissa Skinner, individually, and on behalf of all others similarly situated, bring this action against Defendants Centerstone of America, Inc., Centerstone of Indiana, Inc., and Centerstone of Tennessee, Inc. (collectively referred to herein as "Centerstone") to obtain damages, restitution and injunctive relief for the Class, as defined below, from Centerstone. Plaintiffs make the following allegations upon information and belief, except as to their own actions, the investigation of counsel, and the facts that are a matter of public record:

NATURE OF THE ACTION

1. This class action arises out of the recent data breach ("Data Breach") at Centerstone's healthcare facilities. As a result of the Data Breach, Plaintiffs and approximately 62,000 current and former Centerstone patients and employees from Indiana and Tennessee 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.

2. In addition, Plaintiffs' and Class Members' sensitive personal and protected health information—which was entrusted to Centerstone—was compromised and unlawfully accessed due to the Data Breach.

3. Information compromised in the Data Breach may include current and former patient and employee 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"). In addition, compromised information may include other protected health information as defined by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), and additional personally identifiable information ("PII") and protected health information ("PHI") that Centerstone collected and maintained.

4. Plaintiffs bring 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 Plaintiffs and Class Members that their information had been subject to the unauthorized access and precisely what specific type of information was accessed.

5. Centerstone maintained the Private Information in a reckless manner.

6. Upon information and belief, the potential for improper disclosure of Plaintiffs' 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.

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

8. Plaintiffs' 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.

9. Armed with the Private Information accessed in the Data Breach, 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.

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

11. Plaintiffs 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.

12. Plaintiffs seek to remedy these harms on behalf of themselves and all similarly situated individuals whose Private Information was accessed during the Data Breach.

13. Plaintiffs seek 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 Melissa Skinner is, and at all times mentioned herein was, an individual citizen of the State of Indiana residing in the City of Paragon.

15. Plaintiff Cody Kenney is, and at all times mentioned herein was, an individual citizen of the State of Indiana residing in the City of Columbus.

16. Centerstone of America, Inc. ("Centerstone of America") is a healthcare services provider with its principal place of business at 44 Vantage Way, Suite 200, Nashville, TN 37228.

17. Centerstone of Tennessee, Inc. ("Centerstone of Tennessee") is a healthcare services provider with its principal place of business at 44 Vantage Way, Suite 200, Nashville, TN 37228. Upon information and belief, Centerstone of Tennessee is a wholly owned subsidiary of Centerstone of America.

18. 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, USA. Upon information and belief, Centerstone of Indiana is a wholly owned subsidiary of Centerstone of America.

19. Centerstone of Indiana and Tennessee are both subsidiaries of Centerstone of America. As the parent company, Centerstone of America controls both of these entities 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 maintained the Private Information

of Plaintiffs and Class Members that they provided to Centerstone of Indiana and Centerstone Tennessee in the course of obtaining healthcare. On information and belief, Centerstone of America maintained the Private Information of Plaintiffs and Class Members in this judicial district.

JURISDICTION AND VENUE

20. 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 in the tens of thousands, many of whom have different citizenship from Defendants Centerstone of America, Inc. and Centerstone of Tennessee, Inc. including the named Plaintiffs here. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

21. 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.

22. 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. Defendants are based in this District, maintain Class Members' personally identifiable information ("PII") in the District and have caused harm to Class Members residing in this District.

CENTERSTONE'S BUSINESS

23. Centerstone is a healthcare services provider offering a range of mental health, substance use disorder treatment, pharmaceutical, and social services throughout Tennessee and other States, including Illinois, Indiana, Kentucky and Florida.

24. 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;
- Tribal identification numbers
- Financial account information;
- Payment card information;
- Medical histories;
- Treatment information;
- Medication or prescription information;
- Beneficiary information;
- Provider information;
- Address, phone number, and email address, and;
- Health insurance information.

25. 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.

26. 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, as disclosed in the Centerstone's Notice of Privacy Practices (the "Privacy Notice"), a notice it is required to maintain under HIPAA. See Exhibit A attached hereto.

27. 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.

28. On information and belief, Centerstone provides each of its patients with its HIPAA compliant notice of its privacy practices (the "Privacy Notice") in respect to how it handles patients' sensitive information.

29. 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.

Ex. A.

30. As a condition of receiving medical care and treatment at its facilities, Centerstone requires that its patients entrust it with highly sensitive personal information.

31. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' PII, Centerstone assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiffs' and Class Members' PII from disclosure.

32. Plaintiffs and the Class Members have taken reasonable steps to maintain the confidentiality of their PII.

33. Plaintiffs and the Class Members relied on Centerstone to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

THE CYBERATTACK AND DATA BREACH

34. Data breaches can occur in myriad ways. Phishing, a common tool deployed to carry out a data breach, is a type of social engineering attack often used to steal user data, including login credentials and credit card numbers. It occurs when an attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message, or text message. The recipient is then tricked into clicking a malicious link, which can lead to the installation of malware, the freezing of the system as part of a ransomware attack or the revealing of sensitive information.

35. In or around August of 2020, CENTERSTONE became aware of suspicious activity related to several of its employees' email accounts.

36. Upon information and belief, the affected employee email accounts were part of the single employee email system utilized by all three defendants, a system that utilizes centralized servers maintained in this judicial district.

37. CENTERSTONE launched an investigation into this suspicious activity and determined that certain employee email accounts were accessed without authorization between December 12 and December 16, 2019.

38. Upon information and belief, Centerstone employees were duped into responding to a phishing scam, which allowed hackers to gain access to employees' email accounts.

39. Upon information and belief, the phishing cyberattack was targeted at Centerstone due to its status as a healthcare entity that collects, creates, and maintains both PII and PHI.

40. Upon information and belief, the targeted phishing cyberattack was expressly designed to gain access to private and confidential data, including (among other things) the Private Information of patients like Plaintiffs and the Class Members.

41. Because of this targeted phishing attack, data thieves were able to gain access to the employees' email accounts and subsequently forward messages from these accounts to an outside email account without CENTERSTONE's knowledge.

42. Incredibly, CENTERSTONE does not appear to have discovered the unauthorized intrusion until August of 2020—approximately eight (8) months after-the-fact.

43. The email accounts and messages contained therein affected by this incident contained some combination of 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.

44. The Private Information contained in the emails was not encrypted.

45. Plaintiffs' Private Information was stolen in the Data Breach as evidenced by the Notices of Data Breach each of them received. See Exhibits B and C, attached. Plaintiffs further believe their stolen Private Information was subsequently sold on the Dark Web.

46. Unsurprisingly, CENTERSTONE could not rule out that Private Information was viewed or accessed in the Data Breach.[1] Rather, Centerstone informed impacted patients that they should take steps "to protect their information."[2]

47. Despite acknowledging that data thieves likely accessed Plaintiffs' and the Class Members' Private Information, Centerstone did not begin to notify affected patients until October 22, 2020.

---

1 https://centerstone.org/notice-of-security-incident/ (last accessed November 19, 2020).

2 *Id.*

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

49. Plaintiffs 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.

50. 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.

51. In light of recent high profile data breaches at other healthcare companies, including, University of Washington Medicine (974,000 patients, December 2018), Wolverine Solutions Group (600,000 patients, September 2018), Oregon Department of Human Services (645,000 patients, March 2019), Columbia Surgical Specialist of Spokane (400,000 patients, January 2019), UConn Health (326,629 patients, February 2019), Navicent Health (278,016 patients, July 2018), CENTERSTONE knew or should have known that its electronic records would be targeted by cybercriminals

52. Indeed, cyberattacks have become so notorious that the Federal Bureau of Investigation and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive to ransomware criminals . . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly."

53. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in CENTERSTONE's industry, including Centerstone.

54. Phishing attacks of the type that the unauthorized persons used to gain access to Centerstone's employee email accounts are among the oldest, most common, and well known form of cyberattacks.

55. "Phishing is a cyber-attack that uses disguised email as a weapon. The goal is to trick the email recipient into believing that the message is something they want or need — a request from their bank, for instance, or a note from someone in their company — and to click a link or download an attachment."[3] The fake link will typically mimic a familiar website and require the input of credentials. Once inputted, the credentials are then used to gain unauthorized access into a system. "It's one of the oldest types of cyber-attacks, dating back to the 1990s" and one that every organization with an internet presence is aware."[4] It remains the "simplest kind of cyberattack and, at the same time, the most dangerous and effective."[5]

56. Phishing attacks are generally preventable with the implementation of a variety of proactive measures such as purchasing and using some sort of commonly available anti-malware security software (such as the ubiquitous Malwarebites). Most cybersecurity tools have the ability to detect when a link or an attachment is not what it seems.[6]

---

[3] Frulingher, J., "What is phishing? How this cyber-attack works and how to prevent it," CSO Online, April 7, 2020 https://www.csoonline.com/article/2117843/what-is-phishing-how-this-cyber-attack-works-and-how-to-prevent-it.html (last visited June 20, 2020).

[4] *Id.*

[5] *Phishing*, Malwarebytes, https://www.malwarebytes.com/phishing/ (last visited June 20, 2020).

[6] *Id.*

57. Other proactive measures include sandboxing inbound e-mail (*i.e.*, an automated process that segregates e-mail with attachments and links to an isolated test environment, or a "sandbox," wherein a suspicious file or URL may be executed safely), inspecting and analyzing web traffic, penetration testing (which can be used to test an organization's security policy, its adherence to compliance requirements, its employees' security awareness and the organization's ability to identify and respond to security incidents), and employee education, just to name some of the well-known tools and techniques to prevent phishing attacks.

Centerstone Fails 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 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. These FTC enforcement actions include actions against healthcare providers like Centerstone. *See, e.g., In the Matter of Labmd, Inc., A Corp*, 2016-2 Trade Cas. (CCH) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) ("[T]he Commission concludes that LabMD's data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.")

63. 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.

64. 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.

Centerstone Fails to Comply with Industry Standards

65. As shown above, 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.

66. 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.

67. 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. The CIS Benchmarks are the overwhelming option of choice for auditors worldwide when advising organizations on the adoption of a secure build standard for any governance and security initiative, including PCI DSS, HIPAA, NIST 800-53, SOX, FISMA, ISO/IEC 27002, Graham Leach Bliley and ITIL.[7]

68. 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.

[7] https://www.cisecurity.org/cis-benchmarks/cis-benchmarks-faq/ (last visited November 19, 2020)

69. Centerstone failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework, NIST Special Publications 800-53, 53A, or 800-171; General Accounting Office (GAO) standards; the Federal Risk and Authorization Management Program (FEDRAMP); and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

Centerstone's Conduct Violates HIPAA and Evidences Its Insufficient Data Security

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

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

72. 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 left unguarded. 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).

73. Centerstone's Data Breach resulted from a combination of insufficiencies that demonstrate they failed to comply with safeguards mandated by HIPAA regulations.

CENTERSTONE'S BREACH

74. Centerstone breached its obligations to Plaintiffs 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 ensure that its vendors with access to its computer systems and data employed reasonable security procedures;

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

f. 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);

g. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

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

i. Failing to 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);

j. Failing to 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);

k. Failing to 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);

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

m. Failing to train all members of its workforces 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);

n. 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");

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

p. Failing to adhere to industry standards for cybersecurity.

75. As the result of computer systems in dire 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 Plaintiffs' and Class Members' Private Information.

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

CYBERATTACKS AND DATA BREACHES CAUSE DISRUPTION AND PUT CONSUMERS AT AN INCREASED RISK OF FRAUD AND IDENTIFY THEFT

77. Cyberattacks and data breaches at medical facilities like CENTERSTONE are especially problematic because of the disruption they cause to the medical treatment and overall daily lives of patients affected by the attack.

78. Researchers have found that at medical facilities that experienced a data security incident, the death rate among patients increased in the months and years after the attack.[8]

79. Researchers have further found that at medical facilities that experienced a data security incident, the incident was associated with deterioration in timeliness and patient outcomes, generally.[9]

80. 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]

[8] *See* https://www.pbs.org/newshour/science/ransomware-and-other-data-breaches-linked-to-uptick-in-fatal-heart-attacks (last visited November 19, 2020)

[9] *See* https://onlinelibrary.wiley.com/doi/full/10.1111/1475-6773.13203 (last visited November 19, 2020)

[10] *Id.*

81. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[11]

82. That is because any victim of a data breach is exposed to serious ramifications regardless of the nature of the data. Indeed, the reason criminals steal personally identifiable 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, 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 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.

83. 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

[11] *See* "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown," p. 2, U.S. Government Accountability Office, June 2007, https://www.gao.gov/new.items/d07737.pdf (last visited Apr. 12, 2019) ("GAO Report").

charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[12]

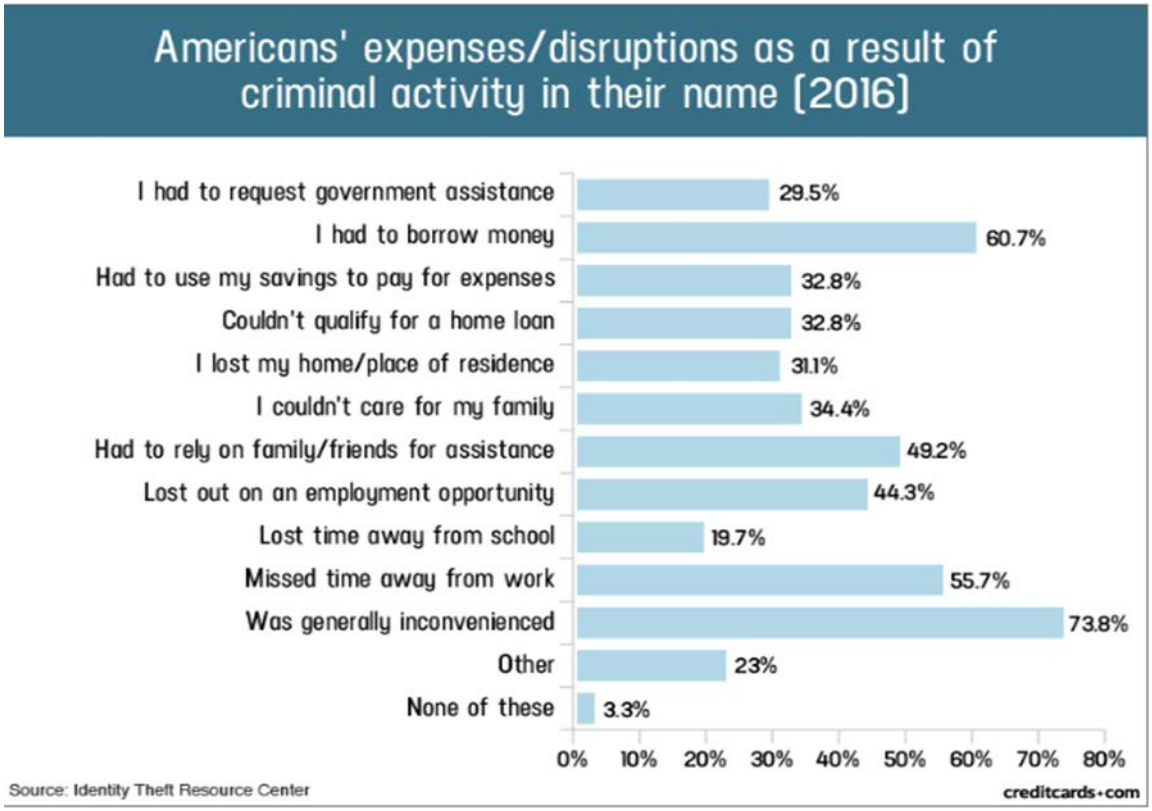
84. Identity thieves use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

85. 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. A study by Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information:[13]

---

12 *See* https://www.identitytheft.gov/Steps (last visited April 12, 2019).

13 Credit Card and ID Theft Statistics" by Jason Steele, 10/24/2017, at: https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php (last visited June 20, 2019).



86. Moreover, theft of Private Information is also gravely serious. PII/PHI is a valuable property right.[14] 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.

87. Theft of PHI, in particular, is gravely serious: "[a] thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance

[14] *See, e.g.*, John T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

provider, or get other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."[15]

88. 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.

89. 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:

> [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.

See GAO Report, at p. 29.

90. 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.

91. 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 Plaintiffs and Class Members are at an increased risk of fraud and identity theft for many years into the future.

---

[15] *See* Federal Trade Commission, Medical Identity Theft, http://www.consumer.ftc.gov/articles/0171-medical-identity-theft (last visited March 18, 2020).

Thus, Plaintiffs and Class Members must vigilantly monitor their financial and medical accounts for many years to come.

92. Medical information is especially valuable to identity thieves. According to account monitoring company LogDog, coveted Social Security numbers were selling on the dark web for just $1 in 2016 – the same as a Facebook account. That pales in comparison with the asking price for medical data, which was selling for $50 and up.[16]

93. 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. Centerstone was put on notice of the substantial and foreseeable risk of harm from a data breach, yet it failed to properly prepare for that risk.

PLAINTIFFS' AND CLASS MEMBERS' DAMAGES

94. To date, Centerstone has done absolutely nothing to provide Plaintiffs and the Class Members with relief for the damages they have suffered as a result of the Data Breach. Centerstone does not even appear to be offering free credit monitoring.

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

96. After the Data Breach, Plaintiff Kenney discovered unauthorized use of his Private Information. In or around October of 2020, Plaintiff Kenney was notified by the Social Security Administration that his Social Security Number was being used in other States without his permission. Also, Plaintiff Kenney was recently made aware that a Free Application for Federal

[16] https://nakedsecurity.sophos.com/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals/#content. (last accessed November 19, 2020)

Student Aid ("FAFSA Application") had been filed in his name without his permission or knowledge in another State.

97. Similarly, after the Data Breach occurred, Plaintiff Skinner received scam phone calls, which appeared to be placed with the intent to obtain personal information to commit identity theft by way of a social engineering attack.

98. Plaintiffs' PII and PHI was compromised as a direct and proximate result of the Data Breach.

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

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

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

102. Plaintiffs 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 Plaintiffs and Class Members.

103. Plaintiffs 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.

104. Plaintiffs and Class Members also suffered a loss of value of their Private Information when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in related cases.

105. Plaintiffs and Class Members were also damaged via benefit-of-the-bargain damages. Plaintiffs and Class Members overpaid for a service that was intended to be accompanied by adequate data security but was not. Part of the price Plaintiffs and Class Members paid to Centerstone was intended to be used by Centerstone to fund adequate security of CENTERSTONE's computer property and protect Plaintiffs' and Class Members' Private Information. Thus, Plaintiffs and the Class Members did not get what they paid for.

106. Plaintiffs 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. Indeed, Centerstone's own notice of data breach provides instructions to Plaintiffs and Class Members about all the time that they will need to spend monitor their own accounts, or to establish a "security freeze" on their credit report.[17]

107. Plaintiffs 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;

[17] https://centerstone.org/notice-of-security-incident/ (last accessed November 19, 2020).

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.

108. Moreover, Plaintiffs 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.

109. Further, as a result of CENTERSTONE's conduct, Plaintiffs 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.

110. As a direct and proximate result of CENTERSTONE's actions and inactions, Plaintiffs and Class Members have suffered a loss of privacy and are at an imminent and increased risk of future harm.

CLASS REPRESENTATION ALLEGATIONS

111. Plaintiffs bring this suit on behalf of themselves and a class of similarly situated individuals under Federal Rule of Civil Procedure 23, which is preliminarily defined as:

> All persons Centerstone identified as being among those individuals impacted by the Data Breach, including all who were sent a notice of the Data Breach.

Excluded from the class are any judges presiding over this matter and court personnel assigned to this case.

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, the Class reportedly includes at least 62,000 individuals. 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 unlawfully used, maintained, lost, or disclosed Plaintiffs' and Class Members' Private Information;

b. 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;

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

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

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

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

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

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

i. Whether Plaintiffs and Class Members suffered legally cognizable damages as a result of Centerstone's misconduct;

j. Whether Centerstone's conduct was negligent;

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

l. Whether Centerstone was unjustly enriched;

m. Whether Centerstone breached an implied contract with Plaintiffs and Class Members, and;

n. Whether Plaintiffs and Class Members are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

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

115. **Adequacy of Representation**. Plaintiffs will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiffs' 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 Plaintiffs and Class Members, in that all the Plaintiffs' and Class Members' data was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from Defendants' 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. Centerstone has acted on grounds that apply generally to the Class as a whole, so that Class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

119. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Centerstone owed a legal duty to Plaintiffs and the Class to exercise due care in collecting, storing, and safeguarding their Private Information;

b. Whether Centerstone's security measures to protect their data systems were reasonable in light of best practices recommended by data security experts;

c. Whether Centerstone's failure to institute adequate protective security measures amounted to negligence;

d. Whether Centerstone failed to take commercially reasonable steps to safeguard consumer Private Information; and

e. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the data breach.

120. 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

121. Plaintiffs repeat and re-allege each and every factual allegation contained in paragraphs 1-120 as if fully set forth herein. Plaintiffs brings this claim on behalf of himself and the Class. Plaintiffs bring this claim individually and on behalf of the Class members.

122. Centerstone knowingly collected, came into possession of, and maintained Plaintiffs' 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.

123. Centerstone had, and continues to have, a duty to timely disclose that Plaintiffs' and Class Members' Private Information within its possession was compromised and precisely the type(s) of information that was compromised.

124. Centerstone had a duty under common law to have procedures in place to detect and prevent the loss or unauthorized dissemination of Plaintiffs' and Class Members' Private Information.

125. Centerstone had a duty to employ reasonable security measures and otherwise protect the Private Information of Plaintiffs and Class Members pursuant to Tenn. Code. §§ 47-18-2105 to 2107 (2005).

126. Centerstone had a duty to employ reasonable security measures and otherwise protect the Private Information of Plaintiffs and Class Members pursuant to Tenn. Code. § 47-18-2110 (2018).

127. Centerstone had a duty to employ reasonable security measures and otherwise protect the Private Information of Plaintiffs and Class Members pursuant to Tenn. Code. § 39-14-150(G).

128. Centerstone systematically failed to provide adequate security for data in its possession.

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

130. Centerstone, through its actions and/or omissions, unlawfully breached its duty to Plaintiffs and Class members by failing to have appropriate procedures in place to detect and prevent dissemination of Plaintiffs' and Class Members' Private Information.

131. Centerstone, through its actions and/or omissions, unlawfully breached its duty to timely disclose to Plaintiffs and Class Members that the Private Information within Centerstone's possession might have been compromised and precisely the type of information compromised.

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

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

134. Centerstone's breaches of duty caused Plaintiffs 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, Plaintiffs and Class Members are in danger of imminent harm in that their Private Information, which is still in the possession of third parties, will be used for fraudulent purposes.

136. Plaintiffs seek the award of actual damages on behalf of themselves and the Class.

137. In failing to secure Plaintiffs' and Class Members' Private Information and promptly notify them of the Data Breach, Centerstone is guilty of oppression, fraud, or malice, in that Centerstone acted or failed to act with a willful and conscious disregard of Plaintiffs' and Class Members' rights. Plaintiffs, therefore, in addition to seeking actual damages, seek punitive damages on behalf of themselves and the Class.

138. Plaintiffs seek injunctive relief on behalf of the Class in the form of an order (1) compelling Centerstone to institute appropriate data collection and safeguarding methods and policies with regard to patient information; and (2) compelling Centerstone to provide detailed and specific disclosure of what types of Private Information have been compromised as a result of the data breach.

COUNT II
Negligence *Per Se*

139. Plaintiffs repeat and re-allege each and every factual allegation contained in paragraphs 1-120 as if fully set forth herein. Plaintiffs bring this claim on behalf of themselves and the Class.

140. Pursuant to Section 5 of the FTC Act, and Tennessee law (*E.g.*, Tenn. Code. §§ 47-18-2105 to 2107 (2005)), CENTERSTONE was required by law to maintain adequate and reasonable data and cybersecurity measures to maintain the security and privacy of Plaintiffs' and Class Members' Private Information.

141. Plaintiffs and Class Members are within the class of persons whom Section 5 of the FTC Act and Tenn. Code. §§ 47-18-2105 to 2107 were among the specific class of people that these statutes were designed to protect.

142. CENTERSTONE breached its duties by failing to employ industry standard data and cybersecurity measures to gain compliance with those laws, including, but not limited to,

proper segregation, access controls, password protection, encryption, intrusion detection, secure destruction of unnecessary data, and penetration testing.

143. It was reasonably foreseeable, particularly given the growing number of data breaches of health information, that the failure to reasonably protect and secure Plaintiffs' and Class Members' Private Information in compliance with applicable laws would result in an unauthorized third-party gaining access to CENTERSTONE's networks, databases, and computers that stored or contained Plaintiffs' and Class Members' Private Information.

144. Plaintiffs' and Class Members' Private Information constitutes personal property that was stolen due to CENTERSTONE's negligence, resulting in harm, injury and damages to Plaintiffs and Class Members.

145. CENTERSTONE's conduct in violation of applicable laws directly and proximately caused the unauthorized access and disclosure of Plaintiffs' and Class Members' unencrypted Private Information and Plaintiffs and Class Members have suffered and will continue to suffer damages as a result of CENTERSTONE's conduct. Plaintiffs and Class Members seek damages and other relief as a result of CENTERSTONE's negligence.

COUNT III
Breach of Implied Contract in Fact

146. Plaintiffs repeat and re-allege each and every factual allegation contained in paragraphs 1-120 as if fully set forth herein. Plaintiffs brings this claim on behalf of themselves and the Class.

147. Through their course of conduct, Defendants, Plaintiffs, and Class Members entered into implied contracts for the provision of medical care and treatment, as well as implied contracts for the Defendants to implement data security adequate to safeguard and protect the privacy of Plaintiffs and Class Members' Private Information.

148. Specifically, Plaintiffs entered into a valid and enforceable implied contract with Defendants when they first went for medical care and treatment at one of Defendants' facilities.

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

150. When Plaintiffs and Class Members provided their Private Information to Defendants in exchange for Defendants' services, they entered into implied contracts with Defendants pursuant to which Defendants agreed to reasonably protect such information.

151. Defendants solicited and invited Class Members to provide their Private Information as part of Defendants' regular business practices. Plaintiffs and Class Members accepted Defendants' offers and provided their Private Information to Defendants.

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

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

154. Under the implied contracts, Defendants and/or their affiliated healthcare providers, promised and were obligated to: (a) provide healthcare to Plaintiffs and Class Members; and (b) protect Plaintiffs' 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, Plaintiffs

and Members of the Class agreed to pay money for these services, and to turn over their Private Information.

155. Both the provision of medical services healthcare and the protection of Plaintiffs' and Class Members' Private Information were material aspects of these implied contracts.

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

157. Defendants' express representations, including, but not limited to the express representations found in the Privacy Notice, memorializes and embodies the implied contractual obligation requiring Defendants to implement data security adequate to safeguard and protect the privacy of Plaintiffs' and Class Members' Private Information.

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

159. A meeting of the minds occurred, as Plaintiffs and Members of the Class agreed to and did provide their Private Information to Defendants and/or their affiliated healthcare providers, and paid for the provided healthcare in exchange for, amongst other things, both the provision of healthcare and medical services and the protection of their Private Information.

160. Plaintiffs and Class Members performed their obligations under the contract when they paid for their health care services and provided their Private Information.

161. Defendants materially breached the contractual obligation to protect the nonpublic Private Information Defendants gathered when the information was accessed and exfiltrated by unauthorized personnel as part of the Data Breach.

162. Defendants materially breached the terms of the implied contracts, including, but not limited to, the terms stated in the Privacy Notice. Defendants did not maintain the privacy of Plaintiffs' and Class Members' Private Information as evidenced by Defendants' notifications of the Data Breach to Plaintiffs and approximately 62,000 Class Members. Specifically, Defendants did not comply with industry standards, standards of conduct embodied in statutes like HIPAA and Section 5 of the FTCA, or otherwise protect Plaintiffs' and the Class Members' Private Information, as set forth above.

163. The Data Breach was a reasonably foreseeable consequence of Defendants' actions in breach of these contracts.

164. As a result of Defendants' failure to fulfill the data security protections promised in these contracts, Plaintiffs and Members of the Class did not receive the full benefit of the bargain, and instead received healthcare and other services that were of a diminished value to that described in the contracts. Plaintiffs and Class Members therefore were damaged in an

amount at least equal to the difference in the value of the healthcare with data security protection they paid for and the healthcare they received.

165. Had Defendants disclosed that their data security was inadequate or that they did not adhere to industry-standard security measures, neither the Plaintiffs, the Class Members, nor any reasonable person would have purchased healthcare from Defendants and/or their affiliated healthcare providers.

166. As a direct and proximate result of the Data Breach, Plaintiffs and Class Members have been harmed and have suffered, and will continue to suffer, actual damages and injuries, including without limitation the release and disclosure of their Private Information, the loss of control of their Private Information, the imminent risk of suffering additional damages in the future, disruption of their medical care and treatment, out-of-pocket expenses, and the loss of the benefit of the bargain they had struck with Defendants.

167. Plaintiffs and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

168. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendants to, *e.g.*, (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

COUNT IV
Violations of the Tennessee Consumer Protection Act of 1977
Tenn. Code Ann. § 47-18-101, *et seq*.

169. Plaintiffs re-allege and incorporates by reference Paragraphs 1 through 120 above as if fully set forth herein.

170. Plaintiffs bring this cause of action pursuant to Federal Rule of Civil Procedure 23, which, procedurally, displaces any state procedural statutory ban on class actions under the Tennessee Consumer Protection Act ("TCPA").

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

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

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

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

a) failing to maintain adequate computer systems and data security practices to safeguard Private Information;

b) failing to disclose that their computer systems and data security practices were inadequate to safeguard Private Information from theft;

c) continued gathering and storage of Private Information and other personal information after Defendants knew or should have known of the security vulnerabilities of their computer systems that were exploited in the Data Breach;

d) making and using false promises, set out in the Privacy Notice, about the privacy and security of Private Information of Plaintiffs and Class Members, and;

e) continued gathering and storage of PII and other personal information after Defendants knew or should have known of the Data Breach and before Defendants allegedly remediated the data security incident.

175. These unfair acts and practices violated duties imposed by laws, including but not limited to the Federal Trade Commission Act, HIPAA, and Tenn. Code Ann. § 47-18-101, *et seq*.

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

177. 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.

178. 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 Plaintiffs and members of the Class, would attach importance to in making their decisions and/or conducting themselves regarding the services received from Centerstone.

179. Plaintiffs 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.

180. 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 Plaintiffs and Class Members.

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

182. Centerstone's acts, practices, and omissions were done in the course of Centerstone's business of furnishing healthcare services in the State of Tennessee.

183. As a direct and proximate result of Centerstone's multiple, separate violations of the TCPA, Plaintiffs and the Class Members suffered damages including, but not limited to: (i)

actual identity theft; (ii) the compromise, publication, and/or theft of their Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Private Information; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (v) the continued risk to their 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; (vi) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members; and (vii) the diminished value of Centerstone's services they received.

184. Also as a direct result of Centerstone's violation of the TCPA, Plaintiffs 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 adequate credit monitoring to all Class Members.

185. 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.

186. Centerstone knew or should have known that its computer systems and data security practices were inadequate to safeguard Class Members' PII and that the risk of a data security incident was high.

187. Plaintiffs and Class Members were injured because: a) they would not have paid for healthcare services from Defendants had they known the true nature and character of Centerstone's data security practices; b) Plaintiffs 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) Plaintiffs 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.

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

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

COUNT V
Intrusion Upon Seclusion/Invasion of Privacy (Electronic Intrusion)

190. Plaintiffs re-allege each and every allegation contained in Paragraphs 1-120 above, and incorporate by reference those paragraphs as if fully set forth herein. Plaintiffs bring this claim on behalf of the Class set forth above.

191. Plaintiffs 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.

192. Plaintiffs 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 Plaintiffs' and Class Members' identities, unique identification numbers, medical histories, and financial records that were only shared with Centerstone for the limited purpose of obtaining and paying for healthcare, medical goods and services.

193. Additionally, Plaintiffs' 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.

194. CENTERSTONE's disclosure of Plaintiffs' 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 Plaintiffs' and Class Members' Private Information to unauthorized third parties permitted the physical and electronic intrusion into Plaintiffs' and Class Members' private quarters where their Private Information was stored and disclosed private facts about their health into the public domain.

195. Plaintiffs 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 VI
Unjust Enrichment

196. Plaintiffs re-allege each and every allegation contained in Paragraphs 1-120 above, and incorporate by reference those paragraphs of this Complaint as if fully set forth herein. Plaintiffs bring this claim on behalf of the Class set forth above.

197. This count is plead in the alternative to the breach of contract count.

198. Plaintiffs and Class Members conferred a benefit on CENTERSTONE by paying for data and cybersecurity procedures to protect their Private Information that they did not receive.

199. 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.

200. Plaintiffs 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 Plaintiffs and Class Members may seek restitution or compensation may be created.

201. Additionally, Plaintiffs 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.

COUNT VII
Breach of Confidence

202. Plaintiffs repeat and re-allege each and every factual allegation contained in paragraphs 1-120 as if fully set forth herein. Plaintiffs brings this claim on behalf of themselves and the Class.

203. At all times during Plaintiffs' and Class Members' interaction with Centerstone, Centerstone was fully aware of the confidential and sensitive nature of Plaintiffs' and Class Members' Private Information.

204. As alleged herein and above, Centerstone's relationship with Plaintiffs' and Class Members was governed by terms and expectations that Plaintiffs' and Class Members' Private Information would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

205. Plaintiffs and Class Members provided their Private Information to Centerstone with the explicit and implicit understandings that Centerstone would protect and not permit Private Information to be disseminated to any unauthorized parties.

206. Plaintiffs and Class Members also provided their Private Information to Centerstone with the explicit and implicit understandings that Centerstone would take precautions to protect such Private Information from unauthorized disclosure.

207. Centerstone voluntarily received in confidence Plaintiffs' and Class Members' Private Information with the understanding that the Private Information would not be disclosed or disseminated to the public or any unauthorized third parties.

208. Due to Centerstone's failure to prevent, detect, or avoid the Data Breach from occurring by, *inter alia*, following industry standard information security practices to secure Plaintiffs' and Class Members' Private Information, Plaintiffs' and Class Members' Private Information was disclosed and misappropriated to unauthorized third parties beyond Plaintiffs' and Class Members' confidence, and without their express permission.

209. As a direct and proximate cause of Centerstone's actions and/or omissions, Plaintiffs and Class Members have suffered damages.

210. But for Centerstone's disclosure of Plaintiffs' and Class Members' Private Information in violation of the parties' understanding of confidence, their protected Private Information would not have been compromised, stolen, viewed, accessed, and used by

unauthorized third parties. Centerstone's Data Breach was the direct and legal cause of the theft of Plaintiffs' and Class Members' protected Private Information, as well as the resulting damages.

211. The injury and harm Plaintiffs and Class Members suffered was the reasonably foreseeable result of Centerstone's unauthorized disclosure of Plaintiffs' and Class Members' Private Information.

212. As a direct and proximate result of Centerstone's breaches of confidence, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the compromise, publication, and/or theft of their Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Private Information; (iv) lost opportunity costs associated with effort expended to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching to prevent, detect, contest, and recover from medical fraud, financial fraud, and identity theft; (v) costs associated with placing freezes on credit reports; (vi) the continued risk to their Private Information, which remain 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 of patients in their continued possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

213. As a direct and proximate result of Centerstone's breaches of confidence, Plaintiffs and Class Members have suffered and will continue to suffer injury and/or harm.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on their own and behalf of all others similarly situated, pray for relief as follows:

A. For an Order certifying this case as a class action pursuant to Federal Rule of Civil Procedure 23, appointing Plaintiffs as Class Representatives, and the undersigned as Class Counsel;

B. Awarding monetary, punitive and actual damages and/or restitution, as appropriate;

C. Awarding declaratory and injunctive relief as permitted by law or equity to assure that the Class has an effective remedy, including enjoining CENTERSTONE from continuing the unlawful practices as set forth above;

D. Prejudgment interest to the extent allowed by the law;

E. Awarding all costs, experts' fees and attorneys' fees, expenses and costs of prosecuting this action; and

F. Such other and further relief as the Court may deem just and proper.

Dated: November 20, 2020

Respectfully submitted,

John Spragens, TN BPR No. 31445
SPRAGENS LAW PLC
311 22nd Ave. N.
Nashville, TN 37203
T: (615) 983-8900
F: (615) 682-8533
john@spragenslaw.com

Gary E. Mason*
David K. Lietz*
MASON LIETZ & KLINGER LLP
5301 Wisconsin Avenue, NW
Suite 305

Washington, DC 20016
Tel: (202) 429-2290
gmason@masonllp.com
dlietz@masonllp.com

Gary M. Klinger*
MASON LIETZ & KLINGER LLP
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Tel: (202) 429-2290
gklinger@masonllp.com

**pro hac vice to be filed*

Attorneys for Plaintiffs and the Proposed Class