UNITED STATES DISTRICT COURT
DISTRICT OF COLORADO

YANNA MEREI, as next of friend for S.M., a minor, on behalf of herself and on behalf of all other similarly situated individuals, Plaintiff, v. **CLINIC SERVICE CO. and CHILDREN'S EYE PHYSICIANS, P.C.,** Defendants.	Case No. 1:26-cv-460 **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Yanna Merei, as next of friend for S.M., a minor, ("Plaintiff"), individually and on behalf of all other similarly situated individuals (the "Class" or "Class Members," as defined below), by and through her undersigned counsel, files this Class Action Complaint against Clinic Service Co. ("CSC") and Children's Eye Physicians, P.C. ("CEP") (together, "Defendants") and alleges the following based on personal knowledge of facts, upon information and belief, and based on the investigation of her counsel as to all other matters.

I. NATURE OF THE ACTION

1. Plaintiff brings this class action lawsuit against Defendants for their failure to protect and safeguard Plaintiff's and the Class's highly sensitive personally identifiable information ("PII") and protected health information ("PHI") (together, "Private Information"). As a result of Defendants' negligence and insufficient data security practices, cybercriminals easily infiltrated CSC's inadequately protected network and from approximately August 10, 2025 to August 17, 2025, and accessed the Private Information of Plaintiff and the Class (the "Data Breach" or "Breach"). Now, Plaintiff's and the Class's Private Information is in the hands of

cybercriminals who will undoubtedly use their Private Information for nefarious purposes for the rest of their lives.

2. CSC is a third-party medical billing provider based in Colorado that services medical providers nationwide.[1]

3. CEP is a Colorado based provider of pediatric ophthalmology and adult strabismus medical services.[2]

4. CEP hired CSC to provide records medical billing services in relation to CEP's medical services with its patients. Through this relationship, CSC collected and maintained and/or was given access to the PII and PHI of Plaintiff and the Class.

5. CEP was negligent and/or failed to confirm when hiring CSC that Plaintiff's and Class Members' Private Information would be protected from unauthorized access, that CSC maintained adequate data security, procedures, practices, infrastructure, and protocols, and that Plaintiff's and the Class's Private Information would not be exposed to data breaches.

6. On or between August 10, 2025, and August 17, 2025, an unauthorized third party accessed CSC's network systems and accessed protected Private Information.[3]

7. On or around August 17, 2025, CSC identified that unauthorized third parties infiltrated CSC's network systems which resulted in the access of protected Private Information.

8. Upon information and belief, the stolen Private Information included names and one or more of the following: address, phone number, email address, payment card information, date of birth, medical diagnosis/treatment information, date of service, patient ID number, medical

[1] https://clinicservice.com/about-clinic-service/ (last visited Feb. 5, 2026).
[2] https://cepcolorado.com/childrens-eye-physicians/ (last visited Feb. 5, 2026).
[3] https://www.mass.gov/doc/2026-128-clinic-service-corporation/download (last visited Feb. 5, 2026).

record number, Medicare/Medicaid number, health insurance information, health insurance claim number, health insurance policy number, and/or treatment cost information.

9. On or about December 8, 2025, CSC completed its investigation and began informing its clients. On or about January 27, 2026, CSC began sending individualized notice letters to impacted patients of CEP at CEP's request, more than 5 months after the breach was discovered.[4]

10. Due to CSC's and CEP's negligent and/or careless acts and omissions, and due to its utter failure to protect Class Members' sensitive data, Plaintiff's and Class Members' unencrypted, unredacted Private Information was compromised. Hackers obtained Plaintiff's and the Class's Private Information because of its value in exploiting and stealing their identities. The risks to Plaintiff and the Class will remain for their respective lifetimes.

11. The sensitive nature of the data exposed through the Data Breach signifies that Plaintiff and Class Members have suffered irreparable harm. Plaintiff and Class Members have lost the ability to control their private information and are subject to an increased risk of identity theft.

12. Now, and for the rest of their lives, Plaintiff and the Class Members will have to deal with the danger of identity thieves possessing and misusing their Private Information. Even those Class Members who have yet to experience identity theft will have to spend time responding to the Data Breach and are at an immediate and heightened risk of all manners of identity theft as a direct and proximate result of the Data Breach.

13. Plaintiff and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

[4] *Id.*

14. Plaintiff brings this action individually and on behalf of all persons whose Private Information was compromised due to CEP's failure to: (i) ensure CSC adequately protected Plaintiff's and Class Members' Private Information; (ii) select a management service provider with adequate data security, procedures, practices, infrastructure, and protocols; (iii) investigate CSC's data security measures prior to hiring CSC to ensure they were adequate; (v) advise CSC of its duties under FTC and HIPAA (described below); (vi) warn Plaintiff and Class Members of CSC's inadequate information security practices; and (viii) give timely notice of the Data Breach to Plaintiff and the Class.

15. The negligence of CSC and CEP violates federal and state statutes, regulations, and security procedures and guidelines.

16. As a result of Defendants' actions and/or inactions described herein, Plaintiff and Class Members have suffered injuries. The injuries they have suffered include: (i) diminished or lost value of their Private Information; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use, of their Private Information; (iii) lost opportunity costs associated with attempting to mitigate the actual, consequences of the Data Breach, including but not limited to lost time; (iv) the loss of time needed to take appropriate measures to avoid unauthorized and fraudulent charges, including but not limited to change their usernames and passwords on their accounts, investigate, correct and resolve unauthorized transactions; and (v) the continued and certainly an increased risk to their Private Information, which remains in CSC's and CEP's possession and is subject to further unauthorized disclosures so long as CEP and CSC fail to undertake appropriate and adequate measures to protect their Private Information. These risks will remain for the lifetimes of Plaintiff and Class Members.

II. THE PARTIES

17. Plaintiff **Yanna Merei and S.M.** are individuals domiciled in Aurora, Colorado. Plaintiff received a data breach notification letter informing Merei that S.M. was a victim of the Data Breach. **Exhibit 1.**

18. Defendant **Clinic Service Co.** is a corporation in Colorado with its principal place of business and headquarters located at 3464 South Willow Street, Denver, Colorado 80231.

19. Defendant **Children's Eye Physicians, P.C.** is a corporation in Colorado with its principal place of business and headquarters located at 4875 Ward Road Suite 600, Wheat Ridge, Colorado 80033. CEP's registered agent for service is Lynette Bridges who may be served at 4875 Ward Road Suite 600, Wheat Ridge, Colorado 80033. Upon information and belief, CEP provided its patients Private Information to CSC.

III. JURISDICTION AND VENUE

20. This Court has subject-matter jurisdiction pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d) because (1) the matter in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, (2) the action is a class action, (3) numerous Class Members are citizens of a different state that is diverse from at least one Defendant[5], and (4) there are more than 100 Class Members.

21. The Court has general personal jurisdiction over Defendants because Defendants are citizens of Colorado, are registered to do business in Colorado, and have their principal place of business in this District.

22. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b)(1) because

[5] In Defendant's notice letter submitted to the Massachusetts Attorney General, it lists the contact information for the attorney's general of 5 states and Washington D.C., indicating that residents of these jurisdictions were affected by the Data Breach. *See* https://www.mass.gov/doc/2026-128-clinic-service-corporation/download (last visited Feb. 5, 2026).

Defendants' principal place of business is in this District, and a substantial part of the events, acts, and omissions giving rise to Plaintiff's clams occurred in this District.

IV. FACTUAL ALLEGATIONS

A. Defendants' Collected Plaintiff's and Class Members' Private Information.

23. CEP acquired, collected, and stored Plaintiff's and Class Members' PII and PHI. By virtue of CEP's relationship with CSC, CSC also acquired, collected, and stored Plaintiff's and Class Members' PII and PHI through the billing services it provided to CEP.

24. Plaintiff provided his Private Information to CEP in connection with healthcare services.

25. CEP hired CSC as a third-party vendor to handle medical billing.

26. As a condition of doing business, Defendant CEP requires that its patients entrust it with highly sensitive personal and health information. In the ordinary course of receiving management service from CSC, CEP provided Plaintiff's and Class Members' Private Information to CSC.

27. The information held by Defendants at the time of the Data Breach included the unencrypted Private Information of Plaintiff and Class Members.

28. Upon information and belief, CEP made promises and representations to individuals that the Private Information collected from them would be kept safe and confidential, and that the privacy of that information would be maintained, and that CEP would delete any sensitive information after it was no longer required to maintain it, including through its privacy policies.

29. Plaintiff and Class Members provided their Private Information to CEP, with the reasonable expectation and on the mutual understanding that CEP would comply with its

obligations to keep such information confidential and secure from unauthorized access.

30. CSC could have prevented this Data Breach by properly securing and encrypting Plaintiff's and Class Members' Private Information. Similarly, CEP could have prevented the Data Breach by ensuring CSC properly secured and encrypted Plaintiff's and Class Members' Private Information.

31. As a result of collecting and storing the Private Information of Plaintiff and Class Members for its own financial benefit, Defendants had a continuous duty to adopt and employ reasonable measures to protect Plaintiff's and the Class Members' Private Information from disclosure to third parties. Moreover, CEP had a duty to ensure that its third-party vendor, CSC, implemented adequate cyber security safeguards to protect Plaintiff's and Class Members' Private Information from involuntary disclosure to unauthorized parties. Defendants had a legal duty to keep Plaintiff's and Class Members' Private Information safe and confidential.

32. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Private Information, Defendants assumed legal and equitable duties and knew or should have known it was responsible for protecting Plaintiff's and Class Members' Private Information from unauthorized disclosure.

33. Defendants had obligations under the FTC Act and HIPAA, contract, industry standards, and representations made to Plaintiff and Class Members, to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

34. CSC had a duty to design, maintain, and test its computer systems and networks to ensure that the Private Information in its possession was adequately secured and protected. Moreover, CEP owed a duty to Plaintiff and the Class to ensure CSC designed, maintained, and

tested its computer systems and networks to ensure that the Private Information in CSC's possession would be adequately secured and protected.

35. CEP owed a duty to Plaintiff and the Class to ensure CSC created and implemented reasonable data security practices and procedures to protect the Private Information in its possession.

36. CEP owed a duty to Plaintiff and the Class to ensure CSC implemented processes that would detect a breach on its data security systems in a timely manner.

37. CEP owed a duty to Plaintiff and the Class to ensure CSC acted upon data security warnings and alerts in a timely fashion.

38. CEP owed a duty to Plaintiff and the Class to disclose if CSC's computer systems and data security practices were inadequate to safeguard individuals' Private Information from theft because such an inadequacy would be a material fact in the decision to entrust Private Information with CEP and/or CSC.

39. CEP owed a duty of care to Plaintiff and the Class because they were foreseeable and probable victims of any inadequate data security practices.

40. CEP owed a duty to Plaintiff and the Class to ensure CSC encrypted Plaintiff's and Class Members' PII and PHI and to ensure CSC monitored user behavior and activity in order to identify possible threats.

41. As a direct and/or proximate result of Defendants wrongful actions and/or inaction and the resulting Data Breach, the criminal(s) and/or the criminal's customers now have Plaintiff's and the other Class Members' Private Information.

42. Defendants derived a substantial economic benefit from collecting Plaintiff's and Class Members' Private Information. Without the required submission of Private Information, Defendants could not provide its services.

43. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their Private Information. Plaintiff and Class Members value the confidentiality of their Private Information and demand security to safeguard their Private Information.

B. The Data Breach

44. On or between August 10, 2025, and August 17, 2025, an unauthorized third party accessed CSC's network systems and accessed protected Private Information.[6]

45. On or around August 17, 2025, CSC identified that unauthorized third parties infiltrated CSC's network systems which resulted in the access of protected Private Information.

46. Upon information and belief, the stolen Private Information included names and one or more of the following: address, phone number, email address, payment card information, date of birth, medical diagnosis/treatment information, date of service, patient ID number, medical record number, Medicare/Medicaid number, health insurance information, health insurance claim number, health insurance policy number, and/or treatment cost information.

47. On or about December 8, 2025, CSC completed its investigation and began informing its clients. On or about January 27, 2026, CSC began sending individualized notice letters to impacted patients of CEP at CEP's request, more than 5 months after the breach was discovered.[7]

48. CEP failed to use reasonable security procedures and practices appropriate to the

[6] https://www.mass.gov/doc/2026-128-clinic-service-corporation/download (last visited Feb. 5, 2026).
[7] *Id.*

nature of the sensitive Private Information CSC was maintaining for Plaintiff and Class Members, causing the devastating exposure of their Private Information.

49. The cybercriminals accessed and acquired files containing unencrypted Private Information of Plaintiff and Class Members. Plaintiff's and Class Members' Private Information was accessed and stolen in the Breach.

50. Losing these types of Private Information poses a significant risk to the individuals involved. Most obviously, attackers can attempt to use names, addresses, and other data points for identity theft by setting up fraudulent accounts.

51. Plaintiff further believes her Private Information, and that of Class Members, was subsequently sold on the dark web following the Data Breach, as that is the *modus operandi* of cybercriminals that commit cyber-attacks of this type.

52. Defendants' actions represent a flagrant disregard of the rights of Plaintiff and the Class, both as to privacy and property.

53. As such, Plaintiff and the Class continue to be at an imminent and impending risk of identity theft and fraud.

C. Cyber Criminals Will Use Plaintiff's and Class Members' Private Information to Defraud them.

54. The type of data that was accessed and compromised here (including full names, Social Security numbers, and medical information) can easily be used to perpetrate fraud and identity theft. Social Security numbers are widely regarded as the most sensitive information hackers can access due to their durability.

55. Social Security numbers are the "gold standard" for identity theft.

56. Private Information is of great value to hackers and cybercriminals, and the data stolen in the Data Breach can and will be used in a variety of ways by criminals to exploit Plaintiff and Class Members and to profit off their misfortune.

57. Each year, identity theft causes tens of billions of dollars of losses to victims in the United States.[8]

58. For example, with the Private Information stolen in the Data Breach, including Social Security numbers, identity thieves can open financial accounts, apply for credit, obtain medical services, file fraudulent tax returns, commit crimes, create false driver's licenses and other forms of identification and sell them to other criminals or undocumented immigrants, steal government benefits, give breach victims' names to police during arrests, and many other harmful forms of identity theft.[9]

59. These criminal activities have and will result in devastating financial and personal losses to Plaintiff and Class Members.

60. Medical-related identity theft is one of the most common, most expensive, and most difficult to prevent forms of identity theft. According to Kaiser Health News, "medical-related identity theft accounted for 43 percent of all identity thefts reported in the United States in 2013[,]" which is more than identity thefts involving banking and finance, the government and the military, or education.[10]

---

[8] *Facts + Statistics: Identity Theft and Cybercrime*, INSURANCE INFO. INST., https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime (last visited Feb. 5, 2026).

[9] *See, e.g.*, Nikkita Walker, *What Can You Do With Your Social Security Number*, CREDIT.COM (Oct. 19, 2023), https://blog.credit.com/2017/11/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/.

[10] Michael Ollove, *The Rise of Medical Identity Theft in Healthcare*, KAISER HEALTH NEWS (Feb. 7, 2014), https://khn.org/news/rise-of-indentity-theft/.

61. "Medical records are a gold mine for criminals—they can access a customer's name, DOB, Social Security and insurance numbers, and even financial information all in one place."[11] A complete identity theft kit that includes health insurance credentials may be worth up to $1,000 on the black market.[12]

62. When cybercriminals manage to steal health insurance information and other personally sensitive data—as they did here—there is no limit to the amount of fraud to which Plaintiff and Class Members are exposed.

63. Social Security numbers are particularly sensitive pieces of personal information. As the Consumer Federation of America explains:

> **Social Security number.** *This is the most dangerous type of personal information in the hands of identity thieves* because it can open the gate to serious fraud, from obtaining credit in your name to impersonating you to get medical services, government benefits, your tax refunds, employment – even using your identity in bankruptcy and other legal matters. It's hard to change your Social Security number and it's not a good idea because it is connected to your life in so many ways.[13]
>
> (Emphasis added).

[11] *You Got It, They Want It: Criminals Targeting Your Private Healthcare Data, New Ponemon Study Shows*, IDX (May 14, 2015) https://www.idx.us/knowledge-center/you-got-it-they-want-it-criminals-are-targeting-your-private-healthcare-dat..

[12] *Managing cyber risks in an interconnected world: Key findings from The Global State of Information Security Survey 2015*, PRICEWATERHOUSECOOPERS (Sept. 30, 2014), https://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf.

[13] *Dark Web Monitoring: What You Should Know*, CONSUMER FEDERATION OF AMERICA (Mar. 19, 2019), https://consumerfed.org/consumer_info/dark-web-monitoring-what-you-should-know/.

64. PII is such a valuable commodity to identity thieves that once it has been compromised, criminals will use it for years.[14]

65. The Data Breach at issue here was targeted and financially motivated, as the only reason cybercriminals go through the trouble of hacking entities like CEP's vendor, CSC, is to steal the highly sensitive information they maintain, which can be exploited and sold for use in the kinds of criminal activity described herein.

66. A Social Security number, date of birth, and full name can sell for $60 to $80 on the digital black market.[15]

67. PHI is even more valuable on the black market than PII.[16]

68. According to the Center for Internet Security, "[t]he average cost of a data breach incurred by a non-healthcare related agency, per stolen record, is $158. For healthcare agencies the cost is an average of $355. Credit card information and PII sell for $1-$2 on the black market, but PHI can sell for as much as $363 according to the Infosec Institute. This is because one's personal health history, including ailments, illnesses, surgeries, etc., can't be changed, unlike credit card information or Social Security Numbers."[17]

69. "PHI is valuable 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

---

[14] *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO (July 5, 2007), https://www.gao.gov/products/gao-07-737.

[15] Michael Kan, *Here's How Much Your Identity Goes for on the Dark Web*, PGMAG (Nov. 15, 2017), https://www.pcmag.com/news/heres-how-much-your-identity-goes-for-on-the-dark-web.

[16] *Data Breaches: In the Healthcare Sector*, CENTER FOR INTERNET SECURITY, https://www.cisecurity.org/insights/blog/data-breaches-in-the-healthcare-sector (last visited Feb. 6, 2026).

[17] *Id.*

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."[18]

70. Identity theft experts advise victims of data breaches: "[I]f there is reason to believe that your personal information has been stolen, you should assume that it can end up for sale on the dark web."[19]

71. These risks are both certainly impending and substantial. As the Federal Trade Commission ("FTC") has reported, if hackers get access to PII, **they will use it**.[20]

72. Hackers may not use the information right away, but this does not mean it will not be used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [I]n 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.[21]

73. For instance, with a stolen Social Security number, which is part of the Private Information compromised in the Data Breach, criminals can open financial accounts, get medical care, file fraudulent tax returns, commit crimes, and steal benefits.[22]

---

[18] *Id.*
[19] *Dark Web Monitoring: What You Should Know*, CONSUMER FEDERATION OF AMERICA (Mar. 19, 2019), https://consumerfed.org/consumer_info/dark-web-monitoring-what-you-should-know/.
[20] Ari Lazarus, *How fast will identity thieves use stolen info?*, MILITARY CONSUMER (May 24, 2017), https://www.militaryconsumer.gov/blog/how-fast-will-identity-thieves-use-stolen-info.
[21] *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO (July 5, 2007), https://www.gao.gov/products/gao-07-737 (emphasis added).
[22] *See* Nikkita Walker, *What Can Someone Do with Your Social Security Number?*, CREDIT.COM (Oct. 19, 2023), https://blog.credit.com/2017/11/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/.

74. Identity theft victims must spend countless hours and large amounts of money repairing the impact to their credit as well as protecting themselves in the future.[23]

75. The unfortunate truth is the full scope of the harm has yet to be realized. There may be a time lag between when harm occurs and when it is discovered, and also between when Private Information is stolen and when it is used.

76. Plaintiff and Class Members will need to pay for their own identity theft protection and credit monitoring for the rest of their lives due to Defendants' negligence.

77. Furthermore, identity monitoring services only alert someone to the fact that they have already been the victim of identity theft—it does not prevent identity theft.[24]

78. Nor can an identity monitoring service remove personal information from the dark web.[25]

79. "The people who trade in stolen personal information [on the dark web] won't cooperate with an identity theft service or anyone else, so it's impossible to get the information removed, stop its sale, or prevent someone who buys it from using it."[26]

80. As a direct and proximate result of the Data Breach, Plaintiff and the Class have been damaged and placed at an imminent and continuing increased risk of harm from fraud and identity theft. Plaintiff and the Class must now take the time and effort to mitigate the actual and potential impact of the Data Breach on their everyday lives, including placing "freezes" and

---

[23] *Guide for Assisting Identity Theft Victims*, FEDERAL TRADE COMMISSION (Sept. 2013), https://www.global-screeningsolutions.com/Guide-for-Assisting-ID-Theft-Victims.pdf.
[24] *See* Kayleigh Kulp, *Credit monitoring services may not be worth the cost*, CNBC (Nov. 30, 2017, 9:00 AM), https://www.cnbc.com/2017/11/29/credit-monitoring-services-may-not-be-worth-the-cost.html.
[25] *Dark Web Monitoring: What You Should Know*, CONSUMER FEDERATION OF AMERICA (Mar. 19, 2019), https://consumerfed.org/consumer_info/dark-web-monitoring-what-you-should-know/.
[26] *Id.*

"alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts, credit reports, and medical records for unauthorized activity for years to come.

81. Even more serious is the identity restoration that Plaintiff and other Class Members must go through, which can require spending countless hours filing police reports, filling out IRS forms, completing Federal Trade Commission checklists and Department of Motor Vehicle driver's license replacement applications, and calling financial institutions to cancel fraudulent credit applications, to name just a few of the steps Plaintiff and the Class must take.

82. Plaintiff and the Class have or will experience the following concrete and particularized harms for which they are entitled to compensation, including:

a. Actual identity theft;

b. Trespass, damage to, and theft of their personal property, including their Private Information;

c. Improper disclosure and theft of their Private Information;

d. The imminent and certainly impending injury flowing from potential fraud and identity theft posed by their Private Information being placed in the hands of criminals;

e. Loss of privacy suffered as a result of the Data Breach, including the harm of knowing cybercriminals have their Private Information;

f. Ascertainable losses in the form of time taken to respond to identity theft, including lost opportunities and lost wages from uncompensated time off from work;

g. Ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably expended to remedy or mitigate the effects of the Data Breach;

h. Ascertainable losses in the form of diminution of the value of Plaintiff's and Class Members' Private Information, for which there is a well-established and quantifiable national and international market;

i. The loss of use of and access to their credit, accounts, and/or funds;

j. Damage to their credit due to fraudulent use of their Private Information; and/or

k. Increased cost of borrowing, insurance, deposits, and the inability to secure more favorable interest rates because of a reduced credit score.

83. Moreover, Plaintiff and Class Members have an interest in ensuring that their Private Information, which remains in the possession of CEP and CSC, is protected from further breaches through the implementation of industry standard security measures and safeguards. Defendants have shown themselves wholly incapable of protecting Plaintiff's and Class Members' Private Information.

84. Plaintiff and Class Members also have an interest in ensuring that their Private Information is removed from all of CEP's and CSC's servers, systems, and files.

85. Plaintiff and Class Members are desperately trying to mitigate the damages Defendants caused them.

86. Given the kind of Private Information that was made accessible to hackers, however, Plaintiff is certain to incur additional damages. Because identity thieves have their Private Information, Plaintiff and Class Members will need to have identity theft monitoring protection for the rest of their lives. Some may even need to go through the long and arduous

process of getting a new Social Security number, with all the loss of credit and employment difficulties that come with a new number.[27]

87. None of this should have happened because the Data Breach was entirely preventable.

D. Defendants were Aware of the Risk of Cyberattacks.

88. According to the Center for Internet Security, "the health industry experiences more data breaches than any other sector."[28] This is because "Personal Health Information (PHI) is more valuable on the black market than credit card credentials or regular Personally Identifiable Information (PII). Therefore, there is a higher incentive for cyber criminals to target medical databases. They can sell the PHI and/or use it for their own personal gain."[29]

89. "In 2023, more than 540 organizations and 112 million individuals were implicated in healthcare data breaches reported to the HHS Office for Civil Rights (OCR), compared to 590 organizations and 48.6 million impacted individuals in 2022."[30]

90. "The number of cybersecurity attacks disrupting the healthcare sector has continued to be a growing concern. In the last three years, more than 90% of all healthcare organizations have reported at least one security breach which can manifest in denial of service, malicious code, ransomed data, and more."[31]

---

[27] *What happens if I change my Social Security number?*, LEXINGTON LAW (Aug. 10, 2022), https://www.lexingtonlaw.com/blog/credit-101/will-a-new-social-security-number-affect-your-credit.html.

[28] *Data Breaches: In the Healthcare Sector*, CENTER FOR INTERNET SECURITY, https://www.cisecurity.org/insights/blog/data-breaches-in-the-healthcare-sector (last visited April 11, 2024).

[29] *Id.*

[30] *This Year's Largest Healthcare Data Breaches*, HEALTH IT SECURITY (Dec. 26, 2023), https://healthitsecurity.com/features/this-years-largest-healthcare-data-breaches.

[31] *6 Industries Most Vulnerable to Cyber Attacks*, WGU (Aug. 3, 2021), https://www.wgu.edu/blog/6-industries-most-vulnerable-cyber-attacks2108.html.

91. "Healthcare organi[z]ations are rich targets for cybercriminals because they hold a large amount of sensitive patient data. This data can be used to commit identity theft or fraud or sold on the black market. Hackers can access this data in many ways, including phishing emails, malware, and unsecured networks."[32]

92. It is no secret that "[h]ealthcare data breaches are reaching record highs. Indeed, healthcare now sees more cyberattacks than any other industry. Fully one-third of all cyberattacks are aimed at healthcare institutions. Why? Because healthcare is a valuable and vulnerable target. Hospitals and healthcare institutions are a prime target for cybercrime due to the vast amount of sensitive data they hold."[33]

93. The health industry is frequently recognized as one of the most vulnerable industries for a cyberattack.[34]

94. CEP should have been aware, and indeed was aware, that CSC was at risk of a data breach that could expose the Private Information that CEP provided to CSC, especially given the rise of healthcare data breaches. However, CEP failed to inquire into CSC's cybersecurity safeguards to ensure that CSC implemented and complied with FTC and HIPAA regulations and guidelines.

---

[32] Troy Beamer, *What Industries Are Most Vulnerable to Cyber Attacks In 2024?*, TECHNEWS (Feb. 27, 2024), https://www.techbusinessnews.com.au/what-industries-are-most-vulnerable-to-cyberattacks-in-2022/.

[33] *What Industries Are Most Vulnerable to Cyberattacks?*, PSM, https://www.psmpartners.com/blog/most-targeted-industries-for-cyber-attacks/

[34] *See, e.g.*, *id.*; Liudmyla Pryimenko, *The 7 Industries Most Vulnerable to Cyberattacks*, EKRAN (Mar. 25, 2024), https://www.ekransystem.com/en/blog/5-industries-most-risk-of-data-breaches; Ani Petrosyan, *Distribution of cyberattacks across worldwide industries in 2023*, STATISTA (Mar. 22, 2024), https://www.statista.com/statistics/1315805/cyber-attacks-top-industries-worldwide/; *6 Industries Most Vulnerable to Cyber Attacks*, WGU (Aug. 3, 2021), https://www.wgu.edu/blog/6-industries-most-vulnerable-cyber-attacks2108.html.

95. CEP's assurances to its patients that it maintains high standards of cybersecurity are further evidence that CEP recognized it had a duty to use reasonable measures to protect the Private Information that it solicited, collected, and maintained.

96. CEP was aware of the risks and harm that could result from CSC's inadequate data security.

E. Defendants Failed to Comply with Federal Trade Commission Requirements.

97. Federal and State governments have established security standards and issued recommendations to minimize data breaches and the resulting harm to individuals and financial institutions. The Federal Trade Commission ("FTC") has issued numerous guides for businesses that highlight the importance of reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[35]

98. Data breaches are preventable.[36] "In almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate security solutions."[37] "Organizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised[.]"[38]

99. Most reported data breaches "are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures. . . . Appropriate information security

---

[35] *See Start with Security: A Guide for Business*, FEDERAL TRADE COMMISSION, (June 2015), available at https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.
[36] Lucy L. Thomson, *Despite the Alarming Trends, Data Breaches Are Preventable*, DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson, ed., 2012), available at https://lawcat.berkeley.edu/record/394088.
[37] *Id.* at 17.
[38] *Id.* at 28.

controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a *data breach never occurs*."[39]

100. Here, many failures laid the groundwork for the Data Breach.

101. The FTC has published guidelines that establish reasonable data security practices for businesses.[40]

102. The FTC guidelines emphasize the importance of having a data security plan, regularly assessing risks to computer systems, and implementing safeguards to control such risks.[41]

103. The FTC guidelines establish that businesses should protect the confidential 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 for installing vendor-approved patches to correct security problems.[42]

104. The FTC guidelines also recommend that businesses utilize an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating hacking attempts; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[43]

105. CEP failed to ensure that CSC followed reasonable and necessary industry standards to prevent the Data Breach, including the FTC's guidelines.

---

[39] *Id.*
[40] *Protecting Personal Information: A Guide for Business*, FTC (Oct. 2016), available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.
[41] *Id.*
[42] *Id.*
[43] *Id.*

106. CEP also failed to ensure that CSC met the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework, NIST Special Publications 800-53, 53A, or 800-171; the Federal Risk and Authorization Management Program (FEDRAMP); or the Center for Internet Security's Critical Security Controls (CIS CSC), which are well respected authorities in cybersecurity readiness.

107. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[44]

108. To prevent and detect the attack here, CEP should have ensured that CSC complied with the following measures as recommended by the Federal Bureau of Investigation:

- Implemented an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Enabled strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scanned all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configured firewalls to block access to known malicious IP addresses.

[44] *See How to Protect Your Networks from RANSOMWARE*, at 3, available at https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view.

- Patched operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Managed the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configured access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.
- Disabled macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.
- Implemented Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.
- Considered disabling Remote Desktop protocol (RDP) if it is not being used.
- Used application whitelisting, which only allows systems to execute programs known and permitted by security policy.

- Executed operating system environments or specific programs in a virtualized environment.
- Categorized data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[45]

109. According to information and belief, Defendant CSC failed to do any of the above and CEP failed to ensure that CSC complied with cybersecurity industry standards.

110. To prevent and detect ransomware attacks, upon information and belief, CEP failed to ensure CSC recommended its employees, as recommended by the United States Cybersecurity & Infrastructure Security Agency, take the following measures:

- **Updated and patched your computer**. Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks.
- **Used caution with links and when entering website addresses**. Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net).

[45] *Id.* at 3–4.

- **Opened email attachments with caution**. Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.
- **Kept your personal information safe**. Check a website's security to ensure the information you submit is encrypted before you provide it.
- **Verified email senders**. If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.
- **Inform yourself**. Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.
- **Used and maintain preventative software programs**. Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic.[46]

[46] *See Protecting Against Ransomware*, CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY (revised Sept. 2, 2021), https://www.cisa.gov/news-events/news/protecting-against-ransomware (internal citations omitted).

111. In addition, to prevent and detect the Data Breach, CEP should have ensured that CSC implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

- **Harden internet-facing assets**
  - Apply latest security updates
  - Use threat and vulnerability management
  - Perform regular audits
- **Thoroughly investigate and remediate alerts.**
  - Prioritize and treat commodity malware infections as potential full compromise of the system
- **Include IT professionals in security discussions.**
  - Ensure collaboration among security operations, security administrators, and information technology administrators to configure servers and other endpoints securely
- **Build and maintain credential hygiene**
  - Use multifactor authentication or network level authentication and enforce strong, randomized, just-in-time local administrator passwords
- **Apply principle of least-privilege**
  - Monitor for adversarial activities
  - Hunt for brute force attempts
  - Monitor for cleanup of Event Logs
  - Analyze logon events

- **Harden infrastructure**
    - Utilize Windows Defender Firewall
    - Enable tamper protection
    - Enable cloud-delivered protection
    - Turn on attack surface reduction rules and Antimalware Scan Interface for Office Visual Basic for Applications[47]

112. Given that CSC was storing the Private Information of CEP's patients, including Plaintiff and Class Members, CSC could and should have implemented all of the above measures to prevent and detect cyberattacks and CEP owed a duty to Plaintiff and Class Members to ensure that CSC did so.

113. Specifically, among other failures, Defendants had far too much confidential unencrypted information held on their systems. Such Private Information should have been segregated into an encrypted system.[48]

114. Moreover, it is well-established industry standard practice for a business to dispose of confidential Private Information once it is no longer needed.[49]

115. The FTC has repeatedly emphasized the importance of disposing of unnecessary Private Information: "Keep sensitive data in your system only as long as you have a business reason to have it. Once that business need is over, properly dispose of it. If it's not on your system,

---

[47] *See Human-operated ransomware attacks: A preventable disaster*, MICROSOFT THREAT INTELLIGENCE (Mar 5, 2020), https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/.

[48] *See* Adnan Raja, *How to Safeguard Your Business Data With Encryption*, DATAINSIDER (Aug. 14, 2018), https://digitalguardian.com/blog/how-safeguard-your-business-data-encryption.

[49] *See Protecting Personal Information: A Guide for Business*, FEDERAL TRADE COMMISSION (Oct. 2016), https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business.

it can't be stolen by hackers."[50] Rather than following this basic standard of care, CSC kept CEP's patients' unencrypted Private Information on its inadequately secured systems indefinitely.

116. In sum, the Data Breach could have been easily prevented through standard practices like the use of industry standard network segmentation and encryption of all Private Information—which CSC negligently failed to do and CEP failed to ensure that CSC did so.

117. Further, the scope of the Data Breach could have been dramatically reduced had Defendants utilized proper record retention and destruction practices—but CSC negligently did no such thing and CEP failed to ensure that CSC utilized proper record retention and security safeguards.

F. Defendants Failed to Comply with HIPAA Under the Law and the Applicable Standards of Care.

118. As the custodians of healthcare records handling medical patient data and providing services to hospitals and healthcare organizations, CEP is a covered entity under HIPAA (45 C.F.R. § 160.103). As such, CEP and CSC are required to comply with the HIPAA Privacy Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and the HIPAA Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and C ("Security Standards for the Protection of Electronic Protected Health Information").

119. HIPAA's Privacy Rule establishes national standards for protecting health information, including health information that is kept or transferred in electronic form.

[50] *Id.* at 6.

120. CEP and CSC are required to "comply with the applicable standards, implementation specifications, and requirements" of HIPAA "with respect to electronic protected health information." 45 C.F.R. § 164.302.

121. "Electronic protected health information" is "individually identifiable health information . . . that is: (i) transmitted by electronic media; [or] (ii) maintained in electronic media[.]" 45 C.F.R. § 160.103.

122. The HIPAA Security Rule, 45 C.F.R. Part 164, Subpart C, requires CEP and CSC to:

a. Ensure the confidentiality, integrity, and availability of all electronic protected health information it or any business associate creates, receives, maintains, or transmits;

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

c. Protect against any reasonably anticipated uses or disclosures of such information; and

d. Ensure compliance by its workforce.

123. HIPAA also requires CEP to ensure that CSC "review and modify the security measures implemented . . . as needed to continue provision of reasonable and appropriate protection of electronic protected health information[.]" 45 C.F.R. § 164.306(e).

124. Additionally, HIPAA requires CEP to ensure that CSC "[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights[.]" 45 C.F.R. § 164.312(a)(1).

125. The HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, further requires CEP and CSC to provide notice of the Data Breach to each affected individual "without unreasonable delay and in no case later than 60 days following discovery of [the] breach[.]" Upon information and belief, Defendants did not provide notice within this framework to affected individuals including Plaintiff and Class Members.

126. Defendants were also prohibited by the Federal Trade Commission Act, 15 U.S.C. § 45 (the "FTC Act"), from engaging in "unfair or deceptive acts or practices in or affecting commerce[.]" The FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act. *See, e.g.*, *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

127. Defendants were further required by various states' laws and regulations to protect Plaintiff's and Class Members' Private Information.

128. CEP owed a duty to Plaintiff and the Class to ensure that CSC design, maintain, and test its computer and email systems to ensure that the Private Information in its possession and control was adequately secured and protected.

129. CEP owed a duty to Plaintiff and the Class to ensure that CSC create and implement reasonable data security practices and procedures to protect the Private Information in its possession, including adequately training their employees (and any others who accessed Private Information within its computer systems) on how to adequately protect Private Information.

130. CEP owed a duty to Plaintiff and the Class to ensure that CSC act upon data security warnings and alerts in a timely fashion.

131. CEP owed a duty to Plaintiff and the Class to ensure CSC adequately train and supervise its employees to identify and avoid any phishing emails that make it past its email filtering service.

132. CEP owed a duty to Plaintiff and the Class to ensure CSC disclose if their computer systems and data security practices were inadequate to safeguard individuals' Private Information from theft because such an inadequacy would be a material fact in individuals' decisions to entrust CEP with their Private Information.

133. Defendants owed a duty to Plaintiff and the Class to disclose in a timely and accurate manner when data breaches occurred.

134. CEP is a sophisticated organization with the resources to ensure the entities it hired deployed robust cybersecurity protocols. CEP knew, or should have known, that hiring an entity that used such protocols was necessary to fulfill their statutory, regulatory, and common law duties to Plaintiff and Class Members. CEP's failure to ensure CSC did so is, therefore, intentional, willful, reckless and/or grossly negligent.

135. CEP was on notice that failing to take the necessary steps to ensure CSC secured Plaintiff's and Class Members' Private Information left that information in a dangerous condition.

136. CEP disregarded the rights of Plaintiff and Class Members by, *inter alia*, (i) intentionally, willfully, recklessly, or negligently failing to ensure CSC had adequate data security; (ii) failing to investigate and confirm CSC's network servers were protected against unauthorized intrusions; (iii) failing to disclose that CSC did not have adequately robust security protocols and training practices in place to adequately safeguard Plaintiff's and Class Members' Private Information; (iv) failing to ensure CSC took standard and reasonably available steps to prevent the Data Breach; (v) concealing the existence and extent of the Data Breach for an unreasonable

duration of time; and (vi) failing to provide Plaintiff and Class Members prompt and accurate notice of the Data Breach.

137. Defendants beached the duties owed to Plaintiff and the Class and the Breach is the proximate cause of Plaintiff's and Class Members' injuries.

138. The actual and adverse effects to Plaintiff and Class Members, including the imminent, immediate, and continuing increased risk of harm for identity theft, identity fraud and/or medical fraud directly and/or proximately caused by Defendants wrongful actions and/or inaction, *infra*, and the resulting Data Breach require Plaintiff and Class Members to take affirmative acts to recover their peace of mind and personal security including, without limitation, purchasing credit reporting services, purchasing credit monitoring and/or internet monitoring services, frequently obtaining, purchasing and reviewing credit reports, bank statements, and other similar information, instituting and/or removing credit freezes and/or closing or modifying financial accounts, for which there is a financial and temporal cost. Plaintiff and Class Members have suffered, and will continue to suffer, such damages for the foreseeable future.

G. Plaintiff's Individual Experience

139. CEP required Plaintiff to provide her Private Information to CEP in order to provide medical services. CSC also acquired, collected, and stored Plaintiff's and Class Members' Private Information through the billing services it provided to CEP. CEP is obligated by law, regulations, and guidelines to ensure CSC maintained adequate data security for Plaintiff and the Class.

140. Plaintiff is a patient of CEP. Upon information and belief, CEP provided Plaintiff's Private Information to CSC as a third-party vendor for management services.

141. Plaintiff entrusted her Private Information to CEP, as the record custodian of her Private Information, with the reasonable expectation and mutual understanding that CEP would

keep her Private Information secure from unauthorized access.

142. By soliciting and accepting Plaintiff's Private Information, CEP agreed to safeguard and protect it from unauthorized access and delete it after a reasonable time.

143. Upon information and belief, CEP and CSC were in possession of Plaintiff's Private Information before, during, and after the Data Breach.

144. Upon information and belief, Plaintiff is a victim of the Data Breach.

145. Following the Data Breach, Plaintiff made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to researching the Data Breach, reviewing and monitoring her accounts for fraudulent activity, and reviewing her credit reports. Plaintiff has spent **hours** responding to the Data Breach.

146. Plaintiff will be forced to spend additional time reviewing her credit reports and monitoring her accounts for the rest of her life. This is time which has been lost forever and cannot be recaptured.

147. Plaintiff places significant value in the security of her Private Information and does not readily disclose it. Plaintiff entrusted CEP with her Private Information with the understanding that CEP would keep her information secure and would employ reasonable and adequate data security measures to ensure that her Private Information would not be compromised.

148. Plaintiff has never knowingly transmitted unencrypted Private Information over the internet or any other unsecured source.

149. As a direct and traceable result of the Data Breach, Plaintiff suffered actual injury and damages after her Private Information was compromised and stolen in the Data Breach, including, but not limited to: (a) lost time and money related to monitoring her accounts and credit reports for fraudulent activity; (b) loss of privacy due to her Private Information being accessed

and stolen by cybercriminals; (c) loss of the benefit of her bargain because CEP and CSC did not adequately protect her Private Information; (d) emotional distress because identity thieves now possess her first and last name paired with her Social Security number and other sensitive information; (e) imminent and impending injury arising from the increased risk of fraud and identity theft now that her Private Information has been stolen and published on the dark web; (f) diminution in the value of her Private Information, a form of intangible property that CEP and CSC obtained from Plaintiff; and (g) other economic and non-economic harm.

150. Plaintiff has been and will continue to be at a heightened and substantial risk of future identity theft and its attendant damages for ***years*** to come. This risk is certainly real and impending, and is not speculative, given the highly sensitive nature of the Private Information stolen in the Data Breach.

151. CEP breached its duties to Plaintiff by failing to ensure that CSC had adequate security measures to protect Plaintiff's Private Information from unauthorized disclosures

152. Plaintiff has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains in the possession of CEP and CSC is protected, and safeguarded from future data breaches. Absent Court intervention, Plaintiff's Private Information will be wholly unprotected and at-risk of future data breaches.

V. CLASS ACTION ALLEGATIONS

153. Plaintiff incorporates by reference all preceding paragraphs as if fully restated here.

154. Pursuant to Federal Rule of Civil Procedure 23, Plaintiff seeks certification of the following class:

> **All individuals whose Private Information was accessed and/or acquired in the Data Breach, including those who received a notice letter.**

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

156. Plaintiff reserves the right to amend or modify the above Class definition or to propose subclasses in subsequent pleadings and motions for class certification.

157. Plaintiff anticipates the issuance of notice setting forth the subject and nature of the instant action to the proposed Class. Upon information and belief, Defendants own business records or electronic media can be utilized for the notice process.

158. **Numerosity:** The proposed Class is so numerous that joinder of all members is impracticable. While the exact number is unknown to Plaintiff, it is believed that the Breach affected thousands of individuals whose Private Information was stored and maintained within CSC's network and systems, including CEP's patients. The number of affected individuals may be obtained by Defendants' records.

159. **Typicality:** Plaintiff's claims are typical of the claims of the Class because Plaintiff's Private Information, like that of every other Class Member, was compromised in the Data Breach. Plaintiff and all members of the Class were injured by the same wrongful acts, practices, and omissions committed by Defendants, as described herein. Plaintiff's claims therefore arise from the same practices or course of conduct that gives rise to the claims of all Class Members.

160. **Adequacy:** Plaintiff is an adequate representative of the Class because Plaintiff's interests do not conflict with the interests of the Class. Plaintiff has retained counsel competent

and highly experienced in data breach class action litigation, and Plaintiff and Plaintiff's counsel intend to prosecute this action vigorously. The interests of the Class will be fairly and adequately protected by Plaintiff and his counsel.

161. **Superiority:** A class action is superior to other available means of fair and efficient adjudication of the claims of Plaintiff and the Class. The injury suffered by each individual Class Member is relatively small in comparison to the burden and expense of individual prosecution of complex and expensive litigation. It would be very difficult if not impossible for individual members of the Class to effectively redress Defendants' wrongdoing. Even if Class Members could afford such individual litigation, the court system could not. Individualized litigation presents potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties, and to the court system, presented by the complex legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties and provides benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

162. **Commonality and Predominance:** Defendants engaged in a common course of conduct toward Plaintiff and Class Members, in that Plaintiff's and Class Members' Private Information was stored on the same network and unlawfully accessed in the same way. There are many questions of law and fact common to the claims of Plaintiff and the other members of the Class, and those questions predominate over any questions that may affect individual members of the Class. Common questions for the Class include:

a. Whether Defendants engaged in the wrongful conduct alleged herein;

b. Whether Defendants owed a duty to Plaintiff and Class Members to adequately protect their Private Information;

c. Whether Defendants breached its duties to Plaintiff and Class Members to adequately protect their Private Information;

d. Whether CEP's failure to ensure CSC implemented adequate data security measures was a cause of the Data Breach;

e. Whether CEP failed to ensure that CSC's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

f. Whether CEP failed to ensure CSC's data security systems prior to and during the Data Breach were consistent with industry standards;

g. Whether CEP knew or should have known that CSC's computer and network security systems, or the computer and network security systems of its vendors, were vulnerable to cyberattacks;

h. Whether Defendants conduct, including its failure to act, resulted in or was the proximate cause of the Data Breach;

i. Whether CEP was negligent in permitting unencrypted Private Information belonging to its patients to be stored within CSC's network;

j. Whether CEP was negligent in failing to ensure that CSC adhere to reasonable data retention policies;

k. Whether Defendants breached implied contractual duties to Plaintiff and the Class to use reasonable care in protecting their Private Information;

l. Whether Defendants were unjustly enriched by unlawfully retaining a benefit conferred upon it by Plaintiff and Class Members;

m. Whether CEP and CSC should have discovered the Data Breach sooner;

n. Whether CEP and CSC failed to adequately respond to the Data Breach, including failing to investigate it diligently and notify affected individuals in the most expedient time possible and without unreasonable delay, and whether this caused damages to Plaintiff and the Class;

o. Whether Defendants continues to breach duties owed to Plaintiff and the Class;

p. Whether Plaintiff and the Class suffered injuries as a proximate result of Defendants' negligent actions or failures to act;

q. Whether CEP was negligent in selecting, supervising, and/or monitoring vendors;

r. Whether Plaintiff and the Class are entitled to recover damages, equitable relief, and other relief; and

s. Whether Defendants' actions alleged herein constitute gross negligence, and whether Plaintiff and Class Members are entitled to punitive damages.

163. Defendants 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.

164. Finally, all members of the proposed Class are readily ascertainable. Defendants have access to Class Members' names and addresses.

VI. CAUSES OF ACTION

FIRST CAUSE OF ACTION
NEGLIGENCE
(On Behalf of Plaintiff and the Class)

165. Plaintiff re-alleges and incorporates by reference all preceding factual paragraphs as though fully set forth herein.

166. CEP gathered and stored the Private Information of Plaintiff and Class members as

part of its business practices, which was in turn provided to CSC so that CSC could billing services to CEP.

167. CEP had full knowledge of the sensitivity of the Private Information that CEP possessed and provided to CSC and the potential harm that Plaintiffs and Class Members could and would suffer if their Private Information were wrongfully disclosed by CEP or CSC.

168. Upon accepting and storing Plaintiff' and Class Members' Private Information on their computer systems and networks, Defendants undertook and owed a duty to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting their Private Information from unauthorized access and disclosure.

169. CEP had a duty to Plaintiff and Class Members to exercise reasonable care in selecting, monitoring, and ensuring any management service providers it hired used adequate data security, procedures, and protocols to prevent foreseeable harm to Plaintiff and the Class pursuant to the provisions of the FTC and HIPAA.

170. CEP had a common law duty to exercise reasonable care to avoid causing foreseeable risk of harm to Plaintiff and the Class when selecting a billing provider, such as CSC, to provide technology and management services that included CSC storing, safeguarding, handling, collecting, and protecting the Private Information provided by Plaintiffs and the Class. This duty included taking action to ensure CSC adequately safeguarded such data, that CSC was aware of its security requirements under the FTC and HIPAA, and that CSC implemented the security requirements required by the FTC and HIPAA. CEP utterly failed to do any of the above.

171. Defendants were also responsible for providing timely notification of the Data Breach to Plaintiff and Class Members but failed to do so.

172. CEP was in a superior position to ensure CSC's data security practices were sufficient to protect against the foreseeable risk of harm to Plaintiff and Class Members from a data breach.

173. Defendants knew Plaintiff and Class Members relied on it to protect their Private Information. Plaintiff and Class Members were not in a position to assess the data security practices used by CSC. Because they had no means to identify CSC's security deficiencies, Plaintiff and Class Members had no opportunity to safeguard their Private Information from cybercriminals. Defendants exercised control over the Private Information stored in CSC's systems and networks; accordingly, Defendants were best positioned and most capable of preventing the harms caused by the Data Breach.

174. Defendants were aware, or should have been aware, of the fact that cybercriminals routinely target healthcare entities through cyberattacks in an attempt to steal valuable Private Information. In other words, Defendants knew of a foreseeable risk to CSC's data security systems but failed to ensure that CSC implemented reasonable security measures.

175. Defendants' duties extended to protecting Plaintiff and the Class from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to such risk, or defeats protections put in place to guard against that risk, or where the parties are in a special relationship. *See* Restatement (Second) of Torts § 302B.

176. Defendants had a duty to protect and safeguard the Private Information of Plaintiff and the Class from unauthorized access and disclosure. Additionally, Defendants owed Plaintiff and the Class a duty to ensure that CSC:

a. exercised reasonable care in designing, implementing, maintaining, monitoring, and testing its networks, systems, protocols, policies, procedures and practices to ensure that Plaintiff's and Class Members' Private Information was adequately secured from impermissible release, disclosure, and publication;

b. protected Plaintiff's and Class Members' Private Information by using reasonable and adequate data security practices and procedures;

c. implemented processes to quickly detect a data breach, security incident, or intrusion involving its networks and servers; and

d. promptly notified Plaintiff and Class Members of any data breach, security incident, or intrusion that affected or may have affected their Private Information.

177. Defendants breached its duties, and thus was negligent, by failing to ensure that CSC use reasonable measures to protect Plaintiff's and Class Members' Private Information.

178. Defendants' willful failure to abide by its duties to Plaintiff and Class Members was wrongful, reckless, and grossly negligent considering the foreseeable risks and known threats.

179. It was foreseeable that Defendants' failure to use reasonable measures to protect Plaintiff's and Class Members' Private Information would result in injury to Plaintiff and Class Members.

180. Furthermore, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the healthcare industry.

181. As a direct and proximate result of Defendants negligent conduct, including, but not limited to, CEP's failure to ensure CSC implement and maintain reasonable data security

practices and procedures as described above, Plaintiff and the Class have suffered damages and are at imminent risk of additional harms and damages (as alleged above).

182. Further, through their failure to provide timely and clear notification of the Data Breach to Plaintiff and Class Members, Defendants prevented Plaintiff and Class Members from taking meaningful, proactive steps to secure their Private Information and mitigate the impact of the Data Breach.

183. Plaintiff and Class Members could have taken actions earlier had they been timely notified of the Data Breach.

184. Plaintiff and Class Members could have enrolled in credit monitoring, instituted credit freezes, and changed their passwords, among other things, had they been alerted to the Data Breach more quickly.

185. Plaintiff and Class Members suffered harm from Defendants' delay in notifying them of the Data Breach.

186. As a direct and proximate result of Defendants' conduct, including, but not limited to, CEP's failure to ensure CSC implemented and maintained reasonable data security practices and procedures, Plaintiff and Class Members have suffered or will suffer injury and damages, including, but not limited to: (i) the loss of the opportunity to determine for themselves how their Private Information is used; (ii) the publication and theft of their Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, fraud, and/or unauthorized use of their Private Information, including the need for substantial credit monitoring and identity protection services for an extended period of time; (iv) lost time and opportunity costs associated with efforts expended to address and 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 fraud and identity theft; (v) costs associated with placing freezes on credit reports and password protections; (vi) anxiety, emotional distress, loss of privacy, and other economic and non-economic losses; (vii) the continued risk to their Private Information, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the Private Information in their continued possession; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the inevitable and continuing consequences of compromised Private Information for the rest of their lives. Thus, Plaintiff and the Class are entitled to damages in an amount to be proven at trial.

187. The damages Plaintiff and the Class have suffered and will suffer (as alleged above) were and are the direct and proximate result of Defendants' negligent conduct.

188. Plaintiff and the Class have suffered cognizable injuries and are entitled to actual and punitive damages in an amount to be proven at trial.

SECOND CAUSE OF ACTION
NEGLIGENCE *PER SE*
(On Behalf of Plaintiff and the Class)

189. Plaintiff re-alleges and incorporates all preceding factual paragraphs as though fully set forth herein.

190. Defendants had a duty to ensure that CSC implemented and maintained reasonable data security practices pursuant to Section 5 of the FTC Act, 15 U.S.C. § 45(a), which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect sensitive and confidential data.

191. The FTC Act prohibits "unfair practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendants,

of failing to use reasonable measures to protect PII/PHI. The FTC publications and orders described above also formed part of the basis of Defendants' duty in this regard.

192. CEP solicited, collected, stored, and maintained Plaintiff's and Class Members' Private Information as part of its regular business, which affects commerce.

193. Defendant violated the FTC Act by failing to ensure that CSC used reasonable measures to protect Plaintiff' and Class Members' Private Information and by failing to comply with applicable industry standards, as described herein.

194. Defendants breached their duties to Plaintiff and the Class under the FTC Act by failing to ensure that CSC implemented and maintained fair, reasonable, and adequate data security practices to safeguard Plaintiff' and Class Members' Private Information, and by failing to provide prompt notice of the Data Breach without unreasonable delay.

195. Defendants' multiple failures to comply with applicable laws and regulations constitute negligence *per se*.

196. Plaintiff and the Class are within the class of persons that the FTC Act was intended to protect.

197. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, like Defendants, that fail to employ reasonable data security measures and avoid unfair and deceptive practices, causing the same harm as that suffered by Plaintiff and the Class.

198. Defendants breached their duties to Plaintiff and the Class by unreasonably delaying and failing to provide notice of the Data Breach expeditiously and/or as soon as practicable to Plaintiff and the Class.

199. Defendants' violations of the FTC Act constitute negligence *per se*.

200. As a direct and proximate result of Defendants' negligence *per se*, Plaintiff and the Class have suffered, and continue to suffer, damages arising from the Data Breach, as alleged above.

201. Defendants also had a duty to ensure that CSC used reasonable security measures under HIPAA, which requires covered entities that handle and/or store medical records of patients/customers, like Defendants, to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1). Some or all of the medical information at issue in this action constitutes "protected health information" within the meaning of HIPAA.

202. 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 Private Information. HHS subsequently promulgated multiple regulations under the authority of the Administrative Simplification provisions of HIPAA. These rules include 45 C.F.R. § 164.304, 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).

203. CEP failed to ensure that CSC complied with HIPAA regulations.

204. Defendants' violations of HIPAA constitute negligence *per se*.

205. Plaintiff and the Class are within the class of persons HIPAA was intended to protect.

206. The harm that occurred as a result of the Data Breach is the type of harm HIPAA was intended to guard against.

207. CEP's duty to ensure its vendor CSC used reasonable care in protecting Plaintiff' and Class Members' Private Information arose not only as a result of the statutes and regulations described above, but also because CEP is bound by industry standards to protect and secure Private Information in its possession and control.

208. Defendants reasonably knew, or should have known, of the risk of harms to Plaintiff and Class Members in an event of a breach and exfiltration of Private Information.

209. Additionally, as a direct and proximate result of Defendants negligence *per se*, Plaintiff and the Class have suffered and will suffer imminent and impending injuries arising from the increased risk of future fraud and identity theft.

210. As a direct and proximate result of Defendants negligence *per se*, Plaintiff and the Class are entitled to recover actual, consequential, and nominal damages.

211. Plaintiff and the Class have suffered injury and are entitled to damages in amounts to be proven at trial.

THIRD CAUSE OF ACTION
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and the Class)

212. Plaintiff re-alleges and incorporates all preceding factual paragraphs as though fully set forth herein.

213. Plaintiff alleges this claim against Defendant CEP only.

214. Plaintiff and Class Members were required to provide their Private Information to CEP in connection with the services CEP provided.

215. CEP solicited and accepted possession of Plaintiff's and Class Members' Private Information, and in turn, provided the Private Information to CSC for billing services.

216. CEP impliedly promised and represented to protect Plaintiff's and Class members' Private Information and ensure that any vendor CEP hired had adequate data security measures to protect the Private Information.

217. In delivering, directly or indirectly, their Private Information to CEP and paying for healthcare services, Plaintiff and Class Members intended and understood that CEP would adequately safeguard their Private Information.

218. Plaintiff and Class Members reasonably expected that the Private Information they entrusted to CEP and to its vendor CSC, in order to receive medical services, would remain confidential and would not be shared or disclosed to criminal third parties.

219. Plaintiff and CEP had a mutual understanding that CEP's vendor would implement and maintain adequate and reasonable data security practices and procedures to protect Plaintiff's and Class Members' sensitive Private Information. Plaintiff and CEP also shared an expectation and understanding that CEP's vendor would not share or disclose, whether intentionally or unintentionally, the sensitive Private Information in its possession and control.

220. Based on CEP's representations, legal obligations, and acceptance of Plaintiff's and Class Members' Private Information, CEP had a duty to safeguard the Private Information in its possession and ensure that CSC used reasonable data security practices.

221. When Plaintiff and Class Members paid money and provided their Private Information to CEP, either directly or indirectly, in exchange for goods or services, they entered into implied contracts with CEP.

222. CEP entered into implied contracts with Plaintiff and the Class under which CEP agreed to comply with its statutory and common law duties to safeguard and protect Plaintiff's and

Class Members' Private Information and to timely notify Plaintiff and Class Members of a data breach.

223. The implied promise of confidentiality includes consideration beyond those pre-existing duties owed under Section 5 of the FTC Act, HIPAA, and other state and federal regulations. The additional consideration included implied promises to take adequate steps to ensure that CEP's vendor complied with specific industry data security standards and FTC guidelines on data security.

224. CEP's implied promises include, but are not limited to: (i) taking steps to ensure any agents or vendors who are granted access to Private Information protect the confidentiality of that information; (ii) taking steps to ensure that Private Information in the possession and control of Defendant, its agents, and/or vendors is restricted and limited to achieve an authorized medical purpose; (iii) restricting access to qualified and trained agents and/or vendors; (iv) designing and implementing appropriate retention policies to protect the Private Information from unauthorized access and disclosure; (v) applying or requiring proper encryption of the Private Information; (vi) requiring multifactor authentication for access to the Private Information; and (vii) other steps necessary to protect against foreseeable data breaches.

225. Plaintiff and Class Members (or their doctors and healthcare providers) would not have entrusted their Private Information to CEP in the absence of such implied contracts.

226. CEP recognized that Plaintiff's and Class Members' Private Information is highly sensitive and must be protected, and that this protection was of material importance to Plaintiff and Class Members.

227. Had CEP disclosed to Plaintiff and Class Members (or their doctors and healthcare providers) that CSC did not have adequate data security practices to secure their Private

Information, Plaintiff and Class Members (or their doctors and healthcare providers) would not have provided their Private Information to CEP.

228. Plaintiff and Class Members (or their doctors and healthcare providers) fully performed their obligations under the implied contracts with CEP.

229. CEP breached the implied contracts with Plaintiff and Class Members by failing to safeguard Plaintiff's and Class Members' Private Information and by failing to provide them with timely and accurate notice of the Data Breach.

230. As a direct and proximate result of CEP's breach of the implied contracts, Plaintiff and Class Members have suffered damages, including foreseeable consequential damages that CEP knew about when it solicited and collected Plaintiff' and Class Members' Private Information.

231. Alternatively, Plaintiff and Class Members were the intended beneficiaries of data protection agreements entered into between CEP and CSC.

232. Plaintiff and the Class have suffered injuries as described herein, and are entitled to actual and punitive damages, statutory damages, and reasonable attorneys' fees and costs, in an amount to be proven at trial.

FOURTH CAUSE OF ACTION
UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Class)

233. Plaintiff re-alleges and incorporates all preceding factual paragraphs as though fully set forth herein.

234. Plaintiff alleges this claim in the alternative to her breach of implied contract claim.

235. Plaintiff alleges this claim against Defendant CEP only.

236. Plaintiff and Class Members conferred a benefit on CEP by way of providing their Private Information to CEP as part of CEP's business.

237. CEP required Plaintiff's and Class Members' Private Information to conduct their business and generate revenue, which it could not do without collecting and maintaining Plaintiff's and Class Members' Private Information.

238. By conferring their Private Information to CEP, directly or indirectly, Plaintiff and Class Members reasonably understood CEP would be responsible for securing their Private Information from unauthorized access and disclosure and ensure any vendor CEP used would comply with FTC and HIPAA cybersecurity regulations and guidelines.

239. Plaintiff and Class Members paid a certain sum of money to CEP, which was used to fund adequate data security.

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

241. There is a direct nexus between money paid to CEP and the requirement for CEP to use a vendor that would keep Plaintiff's and Class Members' Private Information confidential and protected from unauthorized access and disclosure.

242. Protecting the Private Information of Plaintiff and Class Members is integral to CEP's business. Without their Private Information, CEP would be unable to provide services comprising CEP's core business.

243. Plaintiff's and Class Members' Private Information have monetary value.

244. CEP solicited, collected, stored, and maintained Plaintiff' and Class Members' Private Information, and as such, Defendant had direct knowledge of the monetary benefits conferred upon it by Plaintiff and the Class. CEP profited from these transactions and used Plaintiff' and Class Members' Private Information for business purposes.

245. CEP appreciated that a monetary benefit was being conferred upon it by Plaintiff and Class Members and accepted that monetary benefit.

246. CEP enriched itself by saving the costs it reasonably should have expended on hiring a vendor that used adequate data security measures to secure Plaintiff's and Class Members' Private Information. CSC did not implement adequate security measures to protect Plaintiff's and Class Members' Private Information, and CEP failed to contract with a vendor with adequate security safeguards. Instead of providing a reasonable level of security that would have prevented the Data Breach, CEP instead calculated to increase its own profit at the expense of Plaintiff and Class Members by hiring a vendor that utilized cheaper, ineffective security measures that did not have adequate security safeguards and allowed the Breach to occur.

247. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of CEP's decision to prioritize its own profits over the requisite security and the safety of their Private Information.

248. CEP failed to ensure that CSC provided reasonable security safeguards and protect the Private Information of Plaintiff and Class Members, and as a result, CEP were overpaid.

249. Under the facts and circumstances outlined above, however, it is inequitable for CEP to retain that benefit without payment of the value thereof.

250. Under the principles of equity and good conscience, CEP should not be permitted to retain the monetary benefit belonging to Plaintiff and Class Members, because CEP failed to

ensure that its vendor implement appropriate data management and security measures sufficient to protect against unauthorized access.

251. CEP acquired Plaintiff's and Class Members' Private Information through inequitable means in that it failed to disclose CSC's inadequate data security practices, as previously alleged.

252. If Plaintiff and Class Members knew that CEP and CSC would not secure their Private Information, they would not have allowed CEP to collect their Private Information.

253. Plaintiff and Class Members have no adequate remedy at law.

254. As a direct and proximate result of CEP's conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm (as alleged above).

255. CEP should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, all gains that it unjustly received.

FIFTH CAUSE OF ACTION
NEGLIGENT TRAINING, HIRING, AND SUPERVISION
(On Behalf of Plaintiff and the Class)

256. Plaintiff re-alleges and incorporates all preceding factual paragraphs as though fully set forth herein.

257. Plaintiff brings this claim against Defendant CEP

258. At all relevant times, CSC was CEP's agent. CEP granted CSC access to the Private Information of Plaintiff and the Class without properly vetting CSC, inquiring about/ investigating CSC's data security, training CSC, advising CSC of its duties owed to Plaintiff and the Class under the FTC and HIPAA, and/or advising CSC of the confidential nature of Plaintiff's and the Class's Private Information.

259. CEP was negligent and failed to exercise the requisite standard of care in the hiring,

supervision, and retention of CSC – who disclosed Plaintiffs' and the Class's Private Information without authorization and caused the damages delineated herein by virtue of the Data Breach.

260. At all times relevant hereto, Defendant CEP owed a duty to Plaintiffs and the Class to train and supervise its agents and third parties handling sensitive Private Information in its possession to ensure they recognized the duties owed to Plaintiff and the Class to keep their Private Information safe from data breaches.

261. CEP owed a duty to Plaintiff and the Class to ensure CSC had adequate data security, procedures, and protocols sufficient to protect Plaintiff's and the Class's Private Information from data breaches prior to hiring CSC.

262. CEP also owed a continuing duty to Plaintiff and the Class to ensure CSC continued to employ adequate data security, procedures, and protocols sufficient to protect Plaintiff's and the Class's Private Information from data breaches after hiring CSC.

263. CEP breached this duty by failing to ensure CSC possessed the requisite data security, procedures, practices, infrastructure, and protocols to protect Plaintiff's and the Class's Private Information from data breaches prior to hiring CSC and while CSC worked for CEP.

264. CEP was on notice of the importance of data security because of well publicized data breaches occurring throughout the United States and because of the FTC publications on data breaches. Despite knowledge of prior data breaches, CEP failed to ensure CSC possessed the adequate security posture to protect Plaintiff's and the Class's Private Information from unauthorized disclosure.

265. CEP knew or should have known that the failure to ensure CSC employed adequate data security, procedures, and protocols would create an unreasonable risk of danger to persons and property.

266. As a direct and proximate result of CEP's breach of its duties, and its negligent hiring, training, selection, and supervision, of CSC, which resulted in the disclosure of Plaintiff's and Class members' confidential Private Information in the Data Breach, Plaintiff and the members of the Class suffered damages, including, without limitation, loss of the benefit of the bargain, exposure to heightened future risk of identity theft, loss of privacy, diminution in value of their Private Information, and actual misuse of their Private Information.

267. CEP was advised of the Data Breach by CSC, but continued to employ CSC, putting Plaintiff and the Class at risk of more data breaches in the future.

268. The acts and omissions of CEP in negligently hiring, retaining, training, and/or supervising CSC are such as to show gross negligence and reckless disregard for the safety of others and, therefore, punitive damages are appropriate.

VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiff and the Class pray for judgment against Defendant as follows:

a. For an order determining that this action is properly brought as a class action and certifying Plaintiff as the representative of the Class and her counsel as Class Counsel;

b. A judgment in favor of Plaintiff and the Class awarding them appropriate monetary relief, including compensatory damages, punitive damages, attorney fees, expenses, costs, and such other and further relief as is just and proper;

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

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

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

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

VIII. DEMAND FOR JURY TRIAL

Plaintiff hereby demands a trial by jury on any and all issues raised in this Class Action Complaint so triable as of right.

Dated: February 6, 2026

Respectfully submitted,

/s/ William B. Federman

William B. Federman
Jessica A. Wilkes
FEDERMAN & SHERWOOD
10205 North Pennsylvania Avenue
Oklahoma City, OK 73120
T: (405) 235-1560
E: wbf@federmanlaw.com
E: jaw@federmanlaw.com

Attorneys for Plaintiff and the Proposed Class