UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF TEXAS
DALLAS DIVISION

AMANDA FITTON, on behalf of herself and all others similarly situated, Plaintiff, v. PINNACLE PROPANE, LLC, Defendant.	Case No.: 3:23-cv- 01559 **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Amanda Fitton ("Plaintiff"), through her attorneys, individually and on behalf of all others similarly situated, brings this Class Action Complaint against Defendant Pinnacle Propane, LLC ("Defendant"), and its present, former, or future direct and indirect parent companies, subsidiaries, affiliates, agents, and/or other related entities. Plaintiff alleges the following on information and belief—except as to her own actions, counsel's investigations, and facts of public record.

NATURE OF ACTION

1. This class action arises from Defendant's failure to protect highly sensitive data.

2. Defendant, Pinnacle Propane, LLC, is a propane supplier based in Irving, Texas, and is a Texas limited liability company.

3. As such, Defendant stores a litany of highly sensitive personal identifiable information ("PII") about its current and former employees. But Defendant lost control over that data when cybercriminals infiltrated its insufficiently protected computer systems in a data breach (the "Data Breach").

4. Thus, Defendant had no effective means to prevent, detect, stop, or mitigate breaches of its systems—thereby allowing cybercriminals unrestricted access to employee PII.

5. On information and belief, cybercriminals were able to breach Defendant's systems because Defendant failed to adequately train its employees on cybersecurity and failed to maintain reasonable security safeguards or protocols to protect the Class's PII. In short, Defendant's failures placed the Class's PII in a vulnerable position—rendering them easy targets for cybercriminals.

6. Plaintiff is a Data Breach victim, receiving breach notice in June 2023. She brings this class action on behalf of herself and all others harmed by Defendant's misconduct.

7. Plaintiff brings this class action against Defendant for its failure to secure and safeguard the confidential, personally identifiable information of its employees. The categories of stolen information about Defendant's current and former employees include, at a minimum, names, addresses, and Social Security numbers (the "PII").

8. Due to Defendant's negligence, Plaintiff and the Class have suffered harm and are subject to a present and continuing risk of identity theft. Plaintiff's and the Class's PII has been compromised and they must now undertake additional security measures to mitigate the damage caused by Defendant.

9. Plaintiff is a former employee of Defendant and Data Breach victim. Ms. Fitton worked for Defendant in 2021 and 2022, and, as a condition of that employment, was required to provide her PII to Defendant. Plaintiff reasonably believed that Defendant would take adequate steps to safeguard the PII she entrusted to it. Defendant did not, resulting in the Data Breach.

10. The Data Breach impacted many of Defendant's current and former employees. The full scope of the Data Breach, however, is either not known or has not been publicly disclosed.

11. Plaintiff brings this Complaint on behalf of persons whose PII was stolen during the Data Breach.

PARTIES

12. Plaintiff, Amanda Fitton, is a natural person and resident and citizen of Arkansas, where she intends to remain.

13. Defendant, Pinnacle Propane, LLC, is a Texas limited liability company with its headquarters and principal place of business located at 600 Las Colinas Blvd E, Ste. 2000, Irving, Texas 75039. The registered agent for service of process is Corporation Service Company d/b/a CSC – Lawyers Incorporating Service Company, 211 E. 7th Street, Suite 620, Austin, Texas 78701-3218.

JURISDICTION AND VENUE

14. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. Plaintiff and Defendant are citizens of different states. On information and belief there are over 100 putative Class Members.

15. This Court has personal jurisdiction over Defendant is headquartered in Texas, regularly conducts business in Texas, and has sufficient minimum contacts in Texas.

16. Venue is proper in the Dallas Division of the Northern District of Texas because Defendant's principal place of business is in Irving Texas which is in the Dallas Division of the Northern District of Texas, and because a substantial part of the events, acts, and omissions giving rise to Plaintiff's claims occurred in the Northern District of Texas.

BACKGROUND

Pinnacle Propane, LLC

17. Pinnacle Propane, LLC ("Pinnacle") is a propane supplier based in Irving, Texas, who claims to be "Providing the best propane services to residential and commercial customers."[1]

18. Pinnacle employs more than 17,000 employees worldwide, operates in 28 countries, on 4 continents, has 30 million customers worldwide, and claims to be the largest global liquefied petroleum gas distributor.[2]

19. As detailed more fully below, Pinnacle failed to safely and securely store the PII entrusted to it by its current and former employees and failed to prevent it from being compromised during the Data Breach.

Defendant Collected and Stored the PII of Plaintiff and the Class

20. As part of its business, Defendant receives and maintains the PII of thousands of current and former employees. In doing so, Defendant implicitly promises to safeguard their PII.

21. In collecting and maintaining the PII, Defendant agreed it would safeguard the data in accordance with its internal policies, state law, and federal law. After all, Plaintiff and Class Members themselves took reasonable steps to secure their PII.

22. Under state and federal law, businesses like Defendant have duties to protect employees' PII and to notify them about breaches.

The Data Breach

23. On December 4, 2022, Defendant learned an unauthorized third party accessed its internal IT computer network from November 28, 2022 until December 6, 2022 in a Data Breach.

[1] PINNACLE PROPANE, https://www.pinnaclepropane.com/ last accessed (July 10, 2023).
[2] About Us, PINNACLE PROPANE, https://www.pinnaclepropane.com/about-pinnacle-propanelast accessed (July 10, 2023).

That Data Breach then lasted for nine days or more—giving criminals plenty of time to seize Plaintiff's and the Class's exposed PII.[3] Moreover, Defendant did not even provide victims with notice of the Data Breach until at least June 2023—more than six months after the start of the breach.

24. Simply put, Defendant failed in its duties when its inadequate security practices caused the Data Breach.

25. Then, Defendant kept the Class in the dark—thereby depriving the Class of the opportunity to try and mitigate their injuries in a timely manner.

26. When it did notify Plaintiff and the Class of the Data Breach, Defendant acknowledged that the Data Breach puts them at a present, continuing, and significant risk of suffering identity theft, warning them to "remain vigilant and take steps to protect against identity theft or fraud, including monitoring your accounts and free credit reports for suspicious activity."[4]

27. Since the breach, Defendant has stated it is "continuing to review and enhance our security measures and protocols in light of this incident to help reduce the risk of a similar event occurring in the future."[5]

28. On information and belief, Defendant failed to adequately train its employees on reasonable cybersecurity protocols or implement reasonable security measures.

29. Defendant's negligence is further evidenced by its failure to prevent the Data Breach and stop cybercriminals from accessing the PII.

30. Defendant has done little to remedy its Data Breach. True, Defendant has offered concessions of credit monitoring and identity services to Plaintiff and the Class.[6] However, upon

[3] Data Breach Notice, attached as **Exhibit A.**
[4] *Id.*
[5] *Id.*
[6] *Id.*

information and belief, such services do not properly compensate Plaintiff and Class Members for the injuries that Defendant inflicted upon them.

31. Because of Defendant's Data Breach, the sensitive PII of the Plaintiff and Class Members were placed into the hands of cybercriminals—inflicting numerous injuries and significant damages upon Plaintiff and Class Members.

Data Breaches Lead to Identity Theft and Cognizable Injuries.

32. The personal information of Plaintiff and the Class is valuable and has been commoditized in recent years.

33. It can take victims years to discover such identity theft and fraud. This gives criminals plenty of time to sell the PII far and wide.

34. The ramifications of Defendant's failure to keep Plaintiff's and the Class's PII secure are severe. Identity theft occurs when someone uses another's personal and financial information such as that person's name, account number, Social Security number, driver's license number, date of birth, and/or other information, without permission, to commit fraud or other crimes.

35. According to experts, one out of four data breach notification recipients become a victim of identity fraud.[7]

36. Stolen PII is often trafficked on the "dark web," a heavily encrypted part of the Internet that is not accessible via traditional search engines. Law enforcement has difficulty policing the "dark web" due to this encryption, which allows users and criminals to conceal identities and online activity.

[7] Study Shows One in Four Who Receive Data Breach Letter Become Fraud Victims, ThreatPost.com (last visited, Feb. 21, 2013), https://threatpost.com/study-shows-one-four-who-receive-data-breach-letter-become-fraud-victims-022013/77549/

37. Once PII is sold, it is often used to gain access to various areas of the victim's digital life, including bank accounts, social media, credit card, and tax details. This can lead to additional PII being harvested from the victim, as well as PII from family, friends, and colleagues of the original victim.

38. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses that year, resulting in more than $3.5 billion in losses to individuals and business victims.

39. Further, according to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good." Defendant did not rapidly report to Plaintiff and the Class that their PII had been stolen.

40. Victims of identity theft also often suffer embarrassment, blackmail, or harassment in person or online, and/or experience financial losses resulting from fraudulently opened accounts or misuse of existing accounts.

41. Data breaches facilitate identity theft as hackers obtain victim's PII and use it to siphon money from existing accounts, open new accounts in the names of their victims, or sell victims' PII to others who do the same.

42. Victims of identity theft often suffer indirect financial costs as well, including the costs incurred due to litigation initiated by creditors and in overcoming the many obstacles they face in obtaining or retaining credit.

43. In addition to out-of-pocket expenses that can exceed thousands of dollars for the victim of new account identity theft, and the emotional toll identity theft can take, some victims have to spend a considerable time repairing the damage caused by the theft of their PII. Victims of new account identity theft will likely have to spend time correcting fraudulent information in their

credit reports and continuously monitor their reports for future inaccuracies, close existing bank/credit accounts, open new ones, and dispute charges with creditors.

44. Further complicating the issues faced by victims of identity theft, data thieves may wait years before attempting to use the stolen PII. To protect themselves, Plaintiff and the Class will need to remain vigilant against unauthorized data use for years or even decades to come.

45. The Federal Trade Commission ("FTC") has also recognized that consumer data is a new (and valuable) form of currency. In a FTC roundtable presentation, former Commissioner, Pamela Jones Harbour, underscored this point by reiterating that "most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency."[8]

46. Stolen PII is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen PII can be worth up to $1,000.00 depending on the type of information obtained.[9]

47. The FTC has also issued numerous guidelines for businesses that highlight the importance of reasonable data security practices. The FTC has noted the need to factor data security into all business decision-making.[10] According to the FTC, data security requires: (1) encrypting information stored on computer networks; (2) retaining payment card information only as long as necessary; (3) properly disposing of personal information that is no longer needed; (4) limiting administrative access to business systems; (5) using industry unapproved activity; (6)

[8] Statement of FTC Commissioner Pamela Jones Harbour—Remarks Before FTC Exploring Privacy Roundtable, (Dec. 7, 2009), http://www.ftc.gov/speeches/harbour/091207privacyroundtable.pdf (last visited September 22, 2021).
[9] *See* Here's How Much Your Personal Information Is Selling for on the Dark Web, Experian, https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited February 12, 2023).

[10] Start With Security, A Guide for Business, FTC, https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf

monitoring activity on networks to uncover unapproved activity; (7) verifying that privacy and security features function properly; (8) testing for common vulnerabilities; and (9) updating and patching third-party software.[11]

48. According to the FTC, unauthorized PII disclosures wreak havoc on consumers' finances, credit history and reputation, and can take time, money and patience to resolve the fallout.[12] The FTC, as such, treats the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5(a) of the FTC Act.

49. To that end, the FTC has issued orders against businesses that failed to employ reasonable measures to secure sensitive payment card data. *See In the matter of Lookout Services, Inc.*, No. C-4326, ¶ 7 (June 15, 2011) ("[Defendant] allowed users to bypass authentication procedures" and "failed to employ sufficient measures to detect and prevent unauthorized access to computer networks, such as employing an intrusion detection system and monitoring system logs."); *In the matter of DSW, Inc.*, No. C-4157, ¶ 7 (Mar. 7, 2006) ("[Defendant] failed to employ sufficient measures to detect unauthorized access."); *In the matter of The TJX Cos., Inc.*, No. C-4227 (Jul. 29, 2008) ("[R]espondent stored . . . personal information obtained to verify checks and process unreceipted returns in clear text on its in-store and corporate networks[,]" "did not require network administrators . . . to use different passwords to access different programs, computers, and networks[,]" and "failed to employ sufficient measures to detect and prevent unauthorized access to computer networks . . ."); *In the matter of Dave & Buster's Inc.*, No. C-4291 (May 20, 2010) ("[Defendant] failed to monitor and filter outbound traffic from its networks to identify and

[11] *Id.*
[12] See Taking Charge, What to Do If Your Identity is Stolen, FTC, at 3 (2012), www.consumer.ftc.gov/articles/pdf-0009-taking-charge.pdf.

block export of sensitive personal information without authorization" and "failed to use readily available security measures to limit access between instore networks . . ."). These orders, which all preceded Defendant's Data Breach, further clarify the measures businesses must take to meet their data security obligations.

50. Consumers place a high value on their PII and a greater value on their PHI, in addition to the privacy of their PII. Research shows how much consumers value their data privacy, and the amount is considerable. Indeed, studies confirm that "[a]mong U.S. subjects, protection against errors, improper access, and secondary use of personal information is worth US $30.49–44.62."[13]

51. By virtue of the Data Breach here and unauthorized release and disclosure of the PII of Plaintiff and the Class, Defendant deprived Plaintiff and the Class of the substantial value of their PII, to which they are entitled. As previously alleged, Defendant failed to provide reasonable and adequate data security, pursuant to and in compliance with industry standards and applicable law.

52. Identity theft associated with data breaches is particularly pernicious due to the fact that the information is made available, and has usefulness to identity thieves, for an extended period of time after it is stolen.

53. As a result, victims suffer immediate and long-lasting exposure and are susceptible to further injury over the passage of time.

54. Even absent any adverse use, consumers suffer injury from the simple fact that information associated with their financial accounts and identity has been stolen. When PII is

[13] See Il-Horn Hann et al., The Value of Online Information Privacy (Oct. 2002) available at http://www.comp.nus.edu.sg/~ipng/research/privacy.pdf (last visited September 22, 2021); see also Tsai, Cranor, Acquisti, and Egelman, The Effect of Online Privacy Information on Purchasing Behavior, 22 (2) Information Systems Research 254, 254 (June 2011).

stolen, accounts become less secure, and the information once used to sign up for bank accounts and other financial services is no longer as reliable as it had been before the theft. Thus, consumers must spend time and money to re-secure their financial position and rebuild the good standing they once had in the financial community.

55. As a direct and proximate result of Defendant's wrongful actions and omissions here, Plaintiff and the Class have suffered, and will continue to suffer, ascertainable losses, economic damages, and other actual injury and harm, including, *inter alia*: (i) from the untimely and inadequate notification of the Data Breach, (ii) the resulting immediate and continuing risk of future ascertainable losses, economic damages and other actual injury and harm, (iii) the opportunity cost and value of lost time they must spend to monitor their financial accounts and other accounts—for which they are entitled to compensation; (iv) out-of-pocket expenses for securing identity theft protection and other similar necessary services; (v) the diminution in value of their PII; (vi) the compromise and continuing publication of their PII; (vii) unauthorized use of stolen PII; and (viii) the continued risk to their PII, which remains in the possession of Defendant and is subject to further breaches so long as Defendant fails to undertake the appropriate measures to protect the PII in their possession.

Defendant Failed to Adhere to FTC Guidelines

56. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making. To that end, the FTC has issued numerous guidelines identifying best data security practices that businesses, such as Defendant, should employ to protect against the unlawful exposure of PII.

57. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established guidelines for fundamental data security principles and practices for business. The guidelines explain that businesses should:

a. protect the personal customer information that they keep;

b. properly dispose of personal information that is no longer needed;

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems.

58. The guidelines also recommend that businesses watch for large amounts of data being transmitted from the system and have a response plan ready in the event of a breach.

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

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

61. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to employees' PII constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

Plaintiff's Experiences and Injuries

62. Plaintiff was injured by Defendant's Data Breach.

63. Plaintiff was employed by Defendant, but her employment ended in October 2022.

64. As a condition of her employment with Defendant, Plaintiff provided Defendant with her PII. Defendant used that PII to facilitate its employment of Plaintiff, including payroll, and required Plaintiff to provide that PII to obtain employment and payment for that employment.

65. Plaintiff provided her PII to Defendant and trusted the company would use reasonable measures to protect it according to Defendant's internal policies, as well as state and federal law. Defendant obtained and continues to maintain Plaintiff's PII and has a continuing legal duty and obligation to protect that PII from unauthorized access and disclosure.

66. Through its Data Breach, Defendant compromised Plaintiff's PII. To which, Plaintiff received a Notice of Data Breach in June 2023.

67. Since the Data Breach, Plaintiff has been the victim of identity theft. Someone attempted several fraudulent charges to her checking account between January and March 2023.

68. Plaintiff has also suffered from an increasing flood of spam texts and phone calls.

69. Plaintiff has spent—and will continue to spend—significant time and effort monitoring her accounts to protect herself from identity theft, and, in fact, Defendant directed her to take those steps in its breach notice. Plaintiff fears for her personal financial security and worries about what information was exposed in the Data Breach, specifically her Social Security number.

70. Because of Defendant's Data Breach, Plaintiff has suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, Plaintiff's injuries are precisely the type of injuries that the law contemplates and addresses.

71. Plaintiff suffered actual injury from the exposure (and likely theft) of her PII—which violates her rights to privacy.

72. Plaintiff suffered actual injury in the form of damages to and diminution in the value of her PII. After all, PII is a form of intangible property—property that Defendant was required to adequately protect.

73. Plaintiff suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because Defendant's Data Breach placed Plaintiff's PII right in the hands of criminals.

74. Because of the Data Breach, Plaintiff anticipates spending considerable amounts of time and money to try and mitigate her injuries.

75. Today, Plaintiff has a continuing interest in ensuring that her PII—which, upon information and belief, remains backed up in Defendant's possession—is protected and safeguarded from additional breaches.

CLASS ACTION ALLEGATIONS

76. Plaintiff brings this class action under Fed. R. Civ. P. 23(a), 23(b)(2), and 23(b)(3), individually and on behalf of all members of the following class:

> All individuals residing in the United States whose PII was compromised in the Data Breach discovered by Pinnacle Propane, LLC in December 2022.

77. Excluded from the Class are Defendant, its agents, affiliates, parents, subsidiaries, any entity in which Defendant has a controlling interest, any Defendant officer or director, any successor or assign, and any Judge who adjudicates this case, including their staff and immediate family.

78. Plaintiff reserves the right to amend the class definition.

79. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of her claims on class-wide bases using the same evidence as would be used to prove those elements in individual actions asserting the same claims.

80. Ascertainability. All members of the proposed Class are readily ascertainable from information in Defendant's custody and control. After all, Defendant already identified some individuals and sent them data breach notices.

81. Numerosity. The Class Members are so numerous that joinder of all Class Members is impracticable. Upon information and belief, the proposed Class includes thousands of members.

82. Commonality and Predominance. Plaintiff and the Class's claims raise predominantly common fact and legal questions—which predominate over any questions affecting individual Class members—for which a class wide proceeding can answer for all Class members. In fact, a class wide proceeding is necessary to answer the following questions:

a. if Defendant had a duty to use reasonable care in safeguarding Plaintiff's and the Class's PII;

b. if Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. if Defendant were negligent in maintaining, protecting, and securing PII;

d. if Defendant breached contract promises to safeguard Plaintiff and the Class's PII;

e. if Defendant took reasonable measures to determine the extent of the Data Breach after discovering it;

f. if Defendant's Breach Notice was reasonable;

g. if the Data Breach caused Plaintiff and the Class injuries;

h. what the proper damages measure is; and

i. if Plaintiff and the Class are entitled to damages, treble damages, and or injunctive relief.

83. Typicality. Plaintiff's claims are typical of Class member's claims as each arises from the same Data Breach, the same alleged violations by Defendant, and the same unreasonable manner of notifying individuals about the Data Breach.

84. Adequacy. Plaintiff will fairly and adequately protect the proposed Class's common interests. Her interests do not conflict with Class members' interests. And Plaintiff has retained counsel—including lead counsel—that is experienced in complex class action litigation and data privacy to prosecute this action on the Class's behalf.

85. Superiority. A class action is superior to all other available means for the fair and efficient adjudication of this controversy. The damages or other financial detriment suffered by individual Class members are relatively small compared to the burden and expense that individual litigation against Defendant would require. Thus, it would be practically impossible for Class members, on an individual basis, to obtain effective redress for their injuries. Not only would individualized litigation increase the delay and expense to all parties and the courts, but individualized litigation would also create the danger of inconsistent or contradictory judgments

arising from the same set of facts. By contrast, the class action device provides the benefits of adjudication of these issues in a single proceeding, ensures economies of scale, provides comprehensive supervision by a single court, and presents no unusual management difficulties.

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

86. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

87. Plaintiff and the Class entrusted their PII to Defendant on the premise and with the understanding that Defendant would safeguard their PII, use their PII for business purposes only, and/or not disclose their PII to unauthorized third parties.

88. Defendant owed a duty of care to Plaintiff and Class Members because it was foreseeable that Defendant's failure—to use adequate data security in accordance with industry standards for data security—would compromise their PII in a data breach. And here, that foreseeable danger came to pass.

89. Defendant has full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and the Class could and would suffer if their PII was wrongfully disclosed.

90. Defendant owed these duties to Plaintiff and Class Members because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendant knew or should have known would suffer injury-in-fact from Defendant's inadequate security practices. After all, Defendant actively sought and obtained Plaintiff and Class Members' PII.

91. Defendant owed—to Plaintiff and Class Members—at least the following duties to:

a. exercise reasonable care in handling and using the PII in its care and custody;

b. implement industry-standard security procedures sufficient to reasonably protect the information from a data breach, theft, and unauthorized;

c. promptly detect attempts at unauthorized access;

d. notify Plaintiff and Class Members within a reasonable timeframe of any breach to the security of their PII.

92. Also, Defendant owed a duty to timely and accurately disclose to Plaintiff and Class Members the scope, nature, and occurrence of the Data Breach. After all, this duty is required and necessary for Plaintiff and Class Members to take appropriate measures to protect their PII, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the Data Breach.

93. Defendant also had a duty to exercise appropriate clearinghouse practices to remove PII it was no longer required to retain under applicable regulations.

94. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the PII of Plaintiff and the Class involved an unreasonable risk of harm to Plaintiff and the Class, even if the harm occurred through the criminal acts of a third party.

95. By being entrusted by Plaintiff and the Class to safeguard their personal data, Defendant had a special relationship with Plaintiff and the Class. Plaintiff and the Class agreed to provide their personal data with the understanding that Defendant would take appropriate measures to protect it and would inform Plaintiff and the Class of any security concerns that might call for action by Plaintiff and the Class.

96. Defendant breached its duty to Plaintiff and the Class by failing to implement and maintain reasonable security controls that were capable of adequately protecting the PII of Plaintiff and the Class.

97. Defendant also breached its duty to timely and accurately disclose to its current and former employees, Plaintiff and the Class, that their PII had been or was reasonably believed to have been improperly accessed or stolen.

98. Defendant's negligence in failing to maintain reasonable data security is further evinced by its failure to comply with legal obligations and industry standards, and the delay between the date of the Data Breach and the time when Defendant disclosed it.

99. The injuries to Plaintiff and the Class were reasonably foreseeable to Defendant because laws and statutes, and industry standards require it to safeguard and protect its computer systems and employ procedures and controls to ensure that unauthorized third parties did not gain access to Plaintiff's and the Class's PII.

100. The injuries to Plaintiff and the Class were reasonably foreseeable because Defendant knew or should have known that systems used for safeguarding PII were inadequately secured and exposed consumer PII to being breached, accessed, and stolen by hackers and unauthorized third parties. As such, Defendant's own misconduct created a foreseeable risk of harm to Plaintiff and the Class.

101. Defendant implemented knowingly deficient data security measures and failed to adopt reasonable measure that could protect the PII of Plaintiff and the Class, and those deficient security measures proximately caused Plaintiff's and the Class's injuries because they directly allowed hackers to easily access Plaintiff and the Class's PII. This ease of access allowed the hackers to steal PII of Plaintiff and the Class, which could lead to dissemination in black markets.

102. As a direct proximate result of Defendant's conduct, Plaintiff and the Class have suffered theft of their PII. Defendant allowed thieves access to Plaintiff's and the Class's PII, thereby decreasing the security of Plaintiff's and the Class's financial and health accounts, making Plaintiff's and the Class's identities less secure and reliable, and subjecting Plaintiff and the Class to the imminent threat of identity theft. Not only will Plaintiff and the Class have to incur time and money to re-secure their bank accounts and identities, but they will also have to protect against identity theft for years to come.

SECOND CAUSE OF ACTION
Negligence *per se*
(On Behalf of Plaintiff and the Class)

103. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

104. Under the FTC Act, 15 U.S.C. § 45, Defendant had a duty to use fair and adequate computer systems and data security practices to safeguard Plaintiff and Class Members' PII.

105. Section 5 of 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 Defendant, of failing to use reasonable measures to protect the PII entrusted to it. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendant's duty to protect Plaintiff and the Class Members' sensitive PII.

106. Defendant breached its respective duties to Plaintiff and Class Members under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard PII.

107. Defendant violated its duty under Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and

amount of PII Defendant had collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

108. The harm that has occurred is the type of harm the FTC Act is intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses that, because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and members of the Class.

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

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

111. Defendant's various violations and its failure to comply with applicable laws and regulations constitutes negligence *per se*.

112. As a direct and proximate result of Defendant's negligence *per se*, Plaintiff and Class Members have suffered and will continue to suffer numerous injuries (as detailed *supra*).

THIRD CAUSE OF ACTION
Breach of Implied Contract
(On Behalf of Plaintiff and the Class)

113. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

114. Plaintiff and Class Members were required to provide their PII to Defendant as a condition of employment with Defendant.

115. Plaintiff and the Class Members accepted Defendant's offers by disclosing their PII to Defendant or its third-party agents in exchange for employment.

116. In turn, and through internal policies, Defendant agreed to protect and not disclose the PII to unauthorized persons.

117. Implicit in the parties' agreement was that Defendant would provide Plaintiff and Class Members with prompt and adequate notice of all unauthorized access and/or theft of their PII.

118. After all, Plaintiff and Class Members would not have entrusted their PII to Defendant or its third-party agents in the absence of such an agreement with Defendant.

119. Plaintiff and the Class fully performed their obligations under the implied contracts with Defendant.

120. The covenant of good faith and fair dealing is an element of every contract. Thus, parties must act with honesty in fact in the conduct or transactions concerned. Good faith and fair dealing, in connection with executing contracts and discharging performance and other duties according to their terms, means preserving the spirit—and not merely the letter—of the bargain. In short, the parties to a contract are mutually obligated to comply with the substance of their contract in addition to its form.

121. Subterfuge and evasion violate the duty of good faith in performance even when an actor believes their conduct to be justified. Bad faith may be overt or consist of inaction. And fair dealing may require more than honesty.

122. Defendant materially breached the contracts it entered with Plaintiff and Class Members by:

a. failing to safeguard their information;

b. failing to notify them promptly of the intrusion into its computer systems that compromised such information.

c. failing to comply with industry standards;

d. failing to comply with the legal obligations necessarily incorporated into the agreements; and

e. failing to ensure the confidentiality and integrity of the electronic PII that Defendant created, received, maintained, and transmitted.

123. In these and other ways, Defendant violated its duty of good faith and fair dealing.

124. Defendant's material breaches were the direct and proximate cause of Plaintiff and Class Members' injuries (as detailed *supra*).

125. Plaintiff and Class Members performed as required under the relevant agreements, or such performance was waived by Defendant's conduct.

FOURTH CAUSE OF ACTION
Breach of Fiduciary Duty
(On Behalf of Plaintiff and the Class)

126. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

127. Given the relationship between Defendant and Plaintiff and Class Members, where Defendant became guardian of Plaintiff and Class Members' PII, Defendant became a fiduciary by its undertaking and guardianship of the PII, to act primarily for Plaintiff and Class Members, (1) for the safeguarding of Plaintiff and Class Members' PII; (2) to timely notify Plaintiff and Class Members of a Data Breach and disclosure; and (3) to maintain complete and accurate records of what information (and where) Defendant did and does store.

128. Defendant has a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of Defendant's relationship with them—especially to secure their PII.

129. Because of the highly sensitive nature of the PII, Plaintiff and Class Members would not have entrusted Defendant, or anyone in Defendant's position, to retain their PII had they known the reality of Defendant's inadequate data security practices.

130. Defendant breached its fiduciary duties to Plaintiff and Class Members by failing to sufficiently encrypt or otherwise protect Plaintiff and Class Members' PII.

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

132. As a direct and proximate result of Defendant's breach of its fiduciary duties, Plaintiff and Class Members have suffered and will continue to suffer numerous injuries (as detailed *supra*).

FIFTH CAUSE OF ACTION
Intrusion upon Seclusion
(On Behalf of Plaintiff and the Class)

133. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

134. Texas recognizes the tort of Intrusion upon Seclusion, and adopts the formulation of that tort found in the Restatement (Second) of Torts, which states:

> One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person.

Restatement (Second) of Torts§ 652B (1977).

135. Plaintiff and the Class had a legitimate expectation of privacy regarding their highly sensitive and confidential PII and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

136. Defendant owed a duty to its current and former patients, including Plaintiff and the Class, to keep this information confidential.

137. The unauthorized acquisition (i.e., theft) by a third party of Plaintiff and Class Members' PII is highly offensive to a reasonable person.

138. The intrusion was into a place or thing which was private and entitled to be private. Plaintiff and the Class disclosed their sensitive and confidential information to Defendant, but did so privately, with the intention that their information would be kept confidential and protected from unauthorized disclosure. Plaintiff and the Class were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

139. The Data Breach constitutes an intentional interference with Plaintiff and the Class's interest in solitude or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

140. Defendant acted with a knowing state of mind when it permitted the Data Breach because it knew its information security practices were inadequate.

141. Defendant acted with a knowing state of mind when it failed to notify Plaintiff and the Class in a timely fashion about the Data Breach, thereby materially impairing their mitigation efforts.

142. Acting with knowledge, Defendant had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiff and the Class.

143. As a proximate result of Defendant's acts and omissions, the private and sensitive PII of Plaintiff and the Class were stolen by a third party and is now available for disclosure and redisclosure without authorization, causing Plaintiff and the Class to suffer damages (as detailed supra).

144. Unless and until enjoined and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and the Class since their PII are still maintained by Defendant with their inadequate cybersecurity system and policies.

145. Plaintiff and the Class have no adequate remedy at law for the injuries relating to Defendant's continued possession of their sensitive and confidential records. A judgment for monetary damages will not end Defendant's inability to safeguard the PII of Plaintiff and the Class.

146. In addition to injunctive relief, Plaintiff, on behalf of himself and the other Class Members, also seeks compensatory damages for Defendant's invasion of privacy, which includes the value of the privacy interest invaded by Defendant, the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest and costs.

SIXTH CAUSE OF ACTION
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

147. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

148. This claim is pleaded in the alternative to the breach of implied contract claim.

149. Plaintiff and Class Members conferred a benefit upon Defendant, by providing Defendant with their valuable PII. They also conferred a benefit on Defendant by providing their employment services.

150. Defendant appreciated or had knowledge of the benefits it received from Plaintiff and Class Members. And Defendant benefited from receiving Plaintiff and Class Members' PII, as this was used to provide its goods and services.

151. Defendant enriched itself by saving the costs they reasonably should have expended on data security measures to secure Plaintiff's and Class Members' PII.

152. Instead of providing a reasonable level of security, or retention policies, that would have prevented the Data Breach, Defendant instead calculated to avoid its data security obligations at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

153. Under principles of equity and good conscience, Defendant should not be permitted to retain the full value of Plaintiff and Class Members' payment because Defendant failed to adequately protect their PII.

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

155. Defendant should be compelled to disgorge into a common fund—for the benefit of Plaintiff and Class Members—all unlawful or inequitable proceeds that it received because of its misconduct.

PRAYER FOR RELIEF

Plaintiff and Class Members respectfully requests judgment against Defendant and that the Court enter an order:

A. Certifying this case as a class action on behalf of Plaintiff and the proposed Class, appointing Plaintiff as class representative, and appointing her counsel to represent the Class;

B. Awarding declaratory and other equitable relief as necessary to protect the interests of Plaintiff and the Class;

C. Awarding injunctive relief as necessary to protect the interests of Plaintiff and the Class;

D. Awarding Plaintiff and the Class damages including applicable compensatory, exemplary, punitive damages, and statutory damages, as allowed by law;

E. Awarding restitution and damages to Plaintiff and the Class in an amount to be determined at trial;

F. Awarding attorneys' fees and costs, as allowed by law;

G. Awarding prejudgment and post-judgment interest, as provided by law;

H. Granting Plaintiff and the Class leave to amend this complaint to conform to the evidence produced at trial; and

I. Granting other relief that this Court finds appropriate.

DEMAND FOR JURY TRIAL

Plaintiff demands a jury trial for all claims so triable.

DATED: July 13, 2023

Respectfully submitted,

/s/ Joe Kendall

JOE KENDALL
Texas Bar No. 11260700
KENDALL LAW GROUP, PLLC
3811 Turtle Creek Blvd., Suite 1450
Dallas, Texas 75219
Telephone: 214/744-3000 / 214/744-3015 (fax)
jkendall@kendalllawgroup.com

TURKE & STRAUSS LLP
Samuel J. Strauss*
Raina Borrelli*
613 Williamson Street, Suite 201
Madison, Wisconsin 53703
Telephone: (608) 237-1775
Facsimile: (608) 509-4423
sam@turkestrauss.com
raina@turkestrauss.com

Attorneys for Plaintiff and Proposed Class
**Pro Hac Vice Forthcoming*

ClassAction.org
