IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF NEW YORK

JUSTIN STAIR, individually and on behalf of all others similarly situated, Plaintiff, v. FIELDTEX PRODUCTS, INC., Defendant.	Case No. 6:26-cv-6024 **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Justin Stair ("Plaintiff"), individually and on behalf of all other similarly situated individuals (the "Class Members," as defined below), by and through his counsel, files this Class Action Complaint against Fieldtex Products, Inc. ("Fieldtex" or "Defendant") and alleges the following based on personal knowledge of facts pertaining to himself and on information and belief based on the investigation of counsel as to all other matters.

I. INTRODUCTION

1. Plaintiff brings this class action lawsuit against Defendant for its negligent failure to protect and safeguard Plaintiff's and Class Members' highly sensitive personally identifiable information ("PII") culminating in a massive and preventable data breach (the "Data Breach" or "Breach"). As a result of Defendant's negligence and deficient data security practices, cybercriminals easily infiltrated Defendant's inadequately protected computer systems and stole the Private Information of Plaintiff and Class Members.

2. Defendant is a medical supply fulfillment organization providing sewing machine operators, first aid and EMS products, and OTC Benefit Packages delivered to Medicare Advantage Members.[1]

3. Defendant obtains, collects, uses, and derives a benefit from the Personal Identifying Information ("PII") of Plaintiff and Class Members. As such, Defendant assumed the legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion.

4. This class action seeks to redress Defendant's unlawful, willful and wanton failure to reasonably protect the sensitive PII of the Plaintiff and Class Members, in violation of Defendant's legal obligations. Defendant failed to properly safeguard and protect the PII in its possession, thereby allowing cybercriminals the opportunity to steal Plaintiff's and Class Members' valuable PII from Defendant's inadequately protected computer and network systems.

5. On or about August 19, 2025, Fieldtex became aware of unauthorized access to its network that resulted in the exposure of data maintained on its network (the "Data Breach").[2]

6. Plaintiff's and Class Members' PII was compromised due to Defendant's negligent and/or careless acts and omissions and their failure to protect the PII of Plaintiff and Class Members. The type of information contained within the affected data included patient names, addresses, dates of birth, insurance member identification number, plan names, effective terms, and gender.[3]

7. Plaintiff and Class Members are at significant risk of identity theft and various other forms of personal, social, and financial harm.

[1] https://fieldtex.com/ (last visited Jan. 1, 2026)
[2] Fieldtex Products, Inc., Notification of Data Security Incident: https://fieldtex.com/notification-of-data-security-incident/ (last visited Jan. 1, 2026).
[3] *Id.*

8. Plaintiff brings this action, individually, and on behalf of all others whose PII was compromised as a result of Defendant's failure to adequately protect PII, timely discover the breach, and warn its applicants, students, and employees of its inadequate information security practices, and effectively monitor its platforms for security vulnerabilities and incidents.

9. Plaintiff and Class Members have all suffered injury as a result of the Defendant's negligent conduct, including: (i) the potential for Plaintiff's and Class Members' exposed PII to be sold and distributed on the dark web, (ii) a lifetime risk of identity theft, sharing, and detrimental use of their sensitive information, (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII, (iv) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time, and (v) the continued and increased risk to their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to take appropriate and adequate measures to protect its applicants', students', and employees' PII.

10. Plaintiff brings this action individually and on behalf of the Class, seeking remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, disgorgement, injunctive relief, reasonable attorney fees and costs, and all other remedies this Court deems proper.

II. THE PARTIES

11. Plaintiff Justin Stair is an individual domiciled in and is a citizen of Hyndman, Pennsylvania. On or about November 20, 2025, Defendant sent Plaintiff Stair a letter informing him he had been impacted by the Data Breach.[4]

[4] Ex. 1 (Plaintiff's Notice Letter)

12. Defendant Fieldtex Products, Inc, is a New York corporation with its principal place of business at 2921 Brighton-Henrietta, Townline Road, Rochester, NY 14623.

III. JURISDICTION AND VENUE

13. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act (CAFA) and 28 U.S.C. § 1332(d) because this is a class action involving more than 100 class members, the amount in controversy exceeds $5,000,000, exclusive of interest and costs, and many members of the class are citizens of states different from Defendant.

14. This Court has personal jurisdiction over Defendant because its principal place of business is in this District, and it regularly transacts business in this District.

15. Venue is proper in this district pursuant to 28 U.S.C. §1391(b)(1) because the Western District of New York is the judicial district in which the Defendant resides and the location where the actions and/or omissions giving rise to Plaintiff's claims occurred.

IV. FACTUAL ALLEGATIONS

A. Background and the Data Breach

16. Defendant is a medical supply fulfillment organization providing sewing machine operators, first aid and EMS products, and OTC Benefit Packages delivered to Medicare Advantage Members.

17. In order to obtain Medicaid services and products, Plaintiff and Class Members were required to indirectly provide Defendant with their sensitive and confidential Private Information.

18. On or around August 19, 2025, Fieldtex discovered certain unauthorized activity within its computer systems.[5] Upon discovery, Fieldtex immediately secured its network. Following an investigation, Fieldtex confirmed that a limited amount of protected information may have been impacted in connection with the incident. On September 30, 2025, Fieldtex finalized its analysis of the impacted data and began notifying the corresponding health plans.[6]

19. Based on Defendant's Notification of Data Security Incident posted on its website, the personal information accessed in the Data Breach includes PII, such as: names, addresses, dates of birth, insurance member identification numbers, plan names, effective terms, and gender.[7]

20. In response to the Data Breach, Fieldtex implemented additional security measures within its network and is reviewing its current policies and procedures related to data security.[8] These additional measures show that Fieldtex did not have the adequate security safeguards in place to protect Plaintiff's and Class Members PII.

21. Defendant knew of its duties to Plaintiff and the Class Members, and the risks associated with failing to protect the PII entrusted to it. On its website, Defendant states, "The privacy and protection of information is a top priority for Fieldtex."[9] Defendant knew or should have known that if it did not use adequate data security capabilities that Plaintiff's and the Class's PII would be unlawfully exposed.

22. Further, Defendant had notice of the Data Breach as early as August 19, 2025. Yet, Defendant negligently delayed in responding to the breach and informing Plaintiff and the Class of the breach.

---

[5] Fieldtex Products, Inc., Notification of Data Security Incident: https://fieldtex.com/notification-of-data-security-incident/ (last visited Jan. 1, 2026).
[6] *Id.*
[7] *Id.*
[8] *Id.*
[9] *Id.*

23. On or around November 20, 2025, Defendant began sending Plaintiff and Class Members a notice of the Data Breach ("Notice of the Data Breach").[10]

24. The details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure a breach does not occur again have not been shared with regulators or Plaintiff and Class Members, who retain a vested interest in ensuring that their information remains protected.

25. The unencrypted PII of Plaintiff and Class Members may end up for sale on the dark web, or simply fall into the hands of companies that will use the detailed PII for targeted marketing without the approval of Plaintiff and Class Members. Unauthorized individuals can easily access the PII of Plaintiff and Class Members.

26. Defendant was negligent and did not use or implement reasonable security procedures, oversight and practices appropriate to the nature of the sensitive, unencrypted information it was maintaining for Plaintiff and Class Members, causing the exposure and theft of PII for Plaintiff and Class Members.

27. Because Defendant had a duty to protect Plaintiff's and Class Members' PII, Defendant should have known through readily available and accessible information about potential threats for the unauthorized exfiltration and misuse of such information.

28. In April 2020, ZDNet reported, in an article titled "Ransomware mentioned in 1,000+ SEC filings over the past year," that "[r]ansomware gangs are now ferociously aggressive in their pursuit of big companies. They breach networks, use specialized tools to maximize

[10] Ex. 1

damage, leak corporate information on dark web portals, and even tip journalists to generate negative news for companies as revenge against those who refuse to pay."[11]

29. In September 2020, the United States Cybersecurity and Infrastructure Security Agency published online a "Ransomware Guide" advising that "[m]alicious actors have adjusted their ransomware tactics over time to include pressuring victims for payment by threatening to release stolen data if they refuse to pay and publicly naming and shaming victims as secondary forms of extortion."[12]

30. This readily available and accessible information confirms that, prior to the Data Breach, Defendant knew or should have known that: (i) cybercriminals were targeting the education sector, such as Defendant, (ii) cybercriminals were ferociously aggressive in their pursuit of organizations and universities in possession of significant sensitive information such as Defendant, (iii) cybercriminals were leaking sensitive information on dark web portals, and (iv) cybercriminals' tactics included threatening to release stolen data.

31. Considering the information readily available and accessible on the internet before the Data Breach and Defendant's involvement in data breach litigation, Defendant, having elected to store the unencrypted PII of Plaintiff and Class Members, had reason to know that Plaintiff's and the Class Members' PII was at risk for being shared with unknown and unauthorized persons.

32. Prior to the Data Breach, Defendant knew or should have known that there was a foreseeable risk that Plaintiff's and Class Members' PII could be accessed, exfiltrated, and published as the result of a cyberattack.

---

[11] 5 ZDNet, Ransomware mentioned in 1,000+ SEC filings over the past year (Apr. 30, 2020) (emphasis added), available at https://www.zdnet.com/article/ransomware-mentioned-in-1000-sec-filings-over-the-past-year/ (last visited December 29, 2025).

[12] U.S. CISA, Ransomware Guide – September 2020, available at https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C.pdf (last visited December 29, 2025).

33. Prior to the Data Breach, Defendant knew or should have known that it should have confirmed the information it obtained was encrypted within the PII to protect against their publication and misuse in the event of a cyberattack.

34. Since the breach, Defendant continues to store applicant, student, and employee information, including Plaintiff's and Class Members' PII, and has failed to give adequate assurances that it has enhanced its security practices sufficiently to avoid another breach.

B. Plaintiff's Experience

35. Plaintiff Stair was a patient of the Defendant's clients.

36. Upon information and belief, as a condition of receiving Medicaid products services from Defendant, Plaintiff was required to indirectly provide his Private Information to Defendant.

37. Defendant was obligated by law, regulations, and guidelines to protect Plaintiff's and the Class's PII and to ensure it maintained adequate data security for Plaintiff's and the Class's PII.

38. Upon information and belief, Defendant was in possession of Plaintiff's PII before, during, and after the Data Breach.

39. Plaintiff received Defendant's Notice of Data Breach on November 20, 2025.[13] The Notice stated that the PII accessed and acquired in the Data Breach included Plaintiff's name, address, date of birth, insurance member identification number, plan name, effective term, and gender.

40. As a result of the Data Breach, Plaintiff's sensitive information was accessed and stolen by an unauthorized actor, including his name, address, date of birth, insurance member

[13] Ex. 1 (Plaintiff's Notice Letter)

identification number, plan name, effective term, and gender. Defendant has not yet provided definitive findings for Plaintiff to know. The confidentiality of Plaintiff's sensitive information has been irreparably harmed. For the rest of his life, Plaintiff will have to worry about when and how his sensitive information may be shared or used to his detriment.

41. Since the Breach, Plaintiff has experienced misuse of his personal information. Specifically, Plaintiff's bank checking account was shut down due to suspicious unauthorized charges originating from foreign countries that resulted in overdraft fees.

42. Plaintiff has also noticed an uptick in spam calls and emails. Specifically, Plaintiff has received unsolicited calls from Medicare and Medicaid stating that there were requests made to his accounts that required Plaintiff's verification. These unsolicited calls began after the Breach.

43. As a result of the Data Breach, upon information and belief, Plaintiff spent time dealing with the consequences of the Data Breach, which includes hours spent verifying the legitimacy of the Notice of Data Breach, researching credit monitoring and/or identity theft protection services, reviewing credit reports, reviewing account statements, and mitigating fraud/identity theft. This time has been lost forever and cannot be recaptured.

44. Additionally, Plaintiff is very careful about sharing his sensitive PII. Upon information and belief, Plaintiff has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

45. As a result of the Data Breach, Plaintiff Stair has experienced a noticeable increase in anxiety due to the loss of his privacy and anxiety over the impact of cybercriminals accessing, using, and selling his PII.

46. Plaintiff Stair anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the present and impending injuries caused by the Data Breach.

47. Plaintiff Stair has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches

48. Plaintiff Stair has suffered injury directly and proximately caused by the Data Breach, including: (a) theft of Plaintiff Stair's valuable PII; (b) the imminent and certain impending injury flowing from fraud and identity theft posed by Plaintiff Stair's PII being placed in the hands of cyber criminals; (c) damages to and diminution in value of Plaintiff Stair's PII that was entrusted to Defendant with the understanding that Defendant would safeguard this information against disclosure; (d) loss of the benefit of the bargain with Defendant to provide adequate and reasonable data security—i.e., the difference in value between what Plaintiff should have received from Defendant and Defendant's defective and deficient performance of that obligation by failing to provide reasonable and adequate data security and failing to protect Plaintiff's PII; and (e) continued risk to Plaintiff's PII, which remains in the possession of Defendant and which is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the PII that was entrusted to Defendant.

49. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from the Data Breach.

50. Plaintiff has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Cyber Criminals Will Use Plaintiff's and Class Members' PII to Further Defraud Them

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

52. Each year, identity theft causes tens of billions of dollars of losses to victims in the United States.[14] For example, with the PII stolen in the Data Breach, including dates of birth, gender, and names, identity thieves can open financial accounts, apply for credit, 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.[15] These criminal activities have and will result in devastating financial and personal losses to Plaintiff and the Class Members.

53. This was a financially motivated and targeted Data Breach, as the only reason the cyber criminals go through the trouble of running a targeted cyberattack is to get information that they can monetize by selling it on the black market for use in the kinds of criminal activity described herein. Indeed, a social security number, date of birth, and full name can sell for $60 to

[14] "Facts + Statistics: Identity Theft and Cybercrime," Insurance Info. Inst., https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime (discussing Javelin Strategy & Research's report "2018 Identity Fraud: Fraud Enters a New Era of Complexity") (last visited Dec. 29, 2025).

[15] *See, e.g.*, Christine DiGangi, *5 Ways an Identity Thief Can Use Your Social Security Number*, Nov. 15, 2017, https://www.usatoday.com/story/money/personalfinance/2017/11/15/5-ways-identity-thief-can-use-your-social-security-number/860643001/

$80 on the digital black market.[16] "[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."[17]

54. 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.[18]

55. The unencrypted Private Information of Plaintiff and Class Members will end up for sale on the dark web as that is the modus operandi of hackers.

56. Unencrypted Private Information may also fall into the hands of companies that will use the detailed Private Information for targeted marketing without the approval of Plaintiff and Class Members. Simply put, unauthorized individuals can easily access the Private Information of Plaintiff and Class Members.

57. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal Private Information to monetize the information. Criminals monetize the data by selling the stolen information on the black market to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

---

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

[17] *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/.

[18] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown,* GAO, June 4, 2007, https://www.gao.gov/assets/gao-07-737.pdf

58. Plaintiff's and Class Members' Private Information is of great value to hackers and cyber criminals, and the data stolen in the Data Breach has been used and will continue to be used in a variety of sordid ways for criminals to exploit Plaintiff and Class Members and to profit off their misfortune.

59. One such example of criminals piecing together bits and pieces of compromised Private Information for profit is the development of "Fullz" packages.[19]

60. With "Fullz" packages, cyber-criminals can cross-reference two sources of Private Information to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals.

61. The development of "Fullz" packages means here that the stolen Private Information from the Data Breach can easily be used to link and identify it to Plaintiff's and Class Members' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the Private Information that was exfiltrated in the Data Breach, criminals may still easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over.

[19] Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off of those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. See, e.g., Brian Krebs, Medical Records for Sale in Underground Stolen From Texas Life Insurance Firm, Krebs on Security (Sep. 18, 2014), https://krebsonsecuritv.eom/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-](https://krebsonsecuritv.eom/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-finn/ (last visited Jan. 5, 2026).

62. Thus, even if certain information (such as contact information or potentially social security numbers) was not stolen in the data breach, criminals can still easily create a comprehensive "Fullz" package

63. The existence and prevalence of "Fullz" packages means that the Private Information stolen from the data breach can easily be linked to the unregulated data (like contact information) of Plaintiff and the other Class Members. Then, this comprehensive dossier can be sold—and then resold in perpetuity—to crooked operators and other criminals (like illegal and scam telemarketers).

64. 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.

65. Defendant's offer of one year of credit monitoring through Cyberscout to Plaintiff and some members of the Class is woefully inadequate and will not fully protect them from the damages and harm caused by Defendant's data security failures. While some harm has begun already, the full scope of the harm has yet to be realized. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. Once the twelve-months have expired, 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 Defendant's gross negligence. Furthermore, identity monitoring only alerts someone to the fact that they have *already been the victim of identity theft* (*i.e.*, fraudulent acquisition and use of another person's PII)—it does not prevent identity theft.[20] Nor can an identity monitoring service remove personal information from the dark web.[21] "The people who trade in stolen personal information [on the

[20] *See, e.g.*, Kayleigh Kulp, *Credit Monitoring Services May Not Be Worth the Cost*, Nov. 30, 2017, https://www.cnbc.com/2017/11/29/credit-monitoring-services-may-not-be-worth-the-cost.html

[21] *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/.

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."[22]

66. As a direct and proximate result of the Data Breach, Plaintiff and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from continued fraud and identity theft. Plaintiff and Class Members must now take the time and effort to mitigate the actual and potential impact of the Data Breach in their everyday lives, including placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come. Even more seriously is the identity restoration that Plaintiff and other Class Members must go through, which can include spending countless hours filing police reports, filling out IRS forms, Federal Trade Commission checklists, 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 Class Members must take.

67. Plaintiff and Class Members have suffered, and continue to suffer, actual harms for which they are entitled to compensation, including:

a. Trespass, damage to, and theft of their personal property including PII;

b. Improper disclosure of their PII;

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

[22] *Id.*

d. Loss of privacy suffered as a result of the Data Breach, including the harm of knowing cyber criminals have their PII and that identity thieves may use that information to defraud other victims of the Data Breach;

e. 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; and

f. Ascertainable losses in the form of deprivation of the value of Plaintiff's and Class Members' personal information for which there is a well-established and quantifiable national and international market.

68. Moreover, Plaintiff and Class Members have an interest in ensuring that their information, which remains in the possession of Defendant, is protected from further breaches by the implementation of industry standard security measures and safeguards. Defendant has shown themselves wholly incapable of protecting Plaintiff's and Class Members' PII.

69. Defendant themselves acknowledged the harm caused by the Data Breach because it offered Plaintiff and some Class Members the woefully inadequate twelve months of credit monitoring through Cyberscout. Twelve months of credit monitoring is, however, inadequate to protect Plaintiff and Class Members from a lifetime of identity theft risk.

70. Defendant further acknowledged, in its letter to Plaintiff and other Class Members, that Fieldtex needed to improve its security protocols, stating: "We are making our computer system stronger, so this doesn't happen again."

71. The Breach Notice further acknowledged that the Data Breach would cause inconvenience to affected individuals and that financial harm would likely occur, stating: "[Check your bank and credit reports often. Look for anything that seems strange or that you didn't do. If

you see something weird, change your passwords right away and tell your bank or credit card company..”

72. At Defendant’s suggestion, Plaintiff and Class Members are desperately trying to mitigate the damage that Defendant’s Data Breach has caused them. Given the kind of PII Defendant allowed to be stolen, Plaintiff and Class Members are certain to incur additional damages. Because identity thieves have their PII and are already using it, Plaintiff and Class Members will need to have identity theft monitoring protection for the rest of their lives.

C. Defendant Was Aware of the Risk of Cyber Attacks

73. Data security breaches have dominated the headlines for the last two decades. And it doesn’t take an IT industry expert to know it. The general public can tell you the names of some of the biggest cybersecurity breaches: Target,[23] Yahoo,[24] Marriott International,[25] Chipotle, Chili’s, Arby’s,[26] and others.[27]

74. Defendant, who requires the collection and maintenance of highly sensitive and valuable PII, should certainly have been aware, and indeed was aware, that not encrypting PII created a substantial risk for a data breach that could expose the PII it collected and maintained.

75. With the increasing prevalence of data breach announcements, Defendant certainly recognized it had a duty to use reasonable measures to protect the wealth of PII that it collected

[23] Michael Kassner, *Anatomy of the Target Data Breach: Missed Opportunities and Lessons Learned*, ZDNET (Feb. 2, 2015), https://www.zdnet.com/article/anatomy-of-the-target-data-breach-missed-opportunities-and-lessons-learned/.
[24] Martyn Williams, *Inside the Russian Hack of Yahoo: How They Did It*, CSOONLINE.COM (Oct. 4, 2017), https://www.csoonline.com/article/3180762/inside-the-russian-hack-of-yahoo-how-they-did-it.html.
[25] Patrick Nohe, *The Marriot Data Breach: Full Autopsy*, THE SSL STORE: HASHEDOUT (Mar. 22, 2019), https://www.thesslstore.com/blog/autopsying-the-marriott-data-breach-this-is-why-insurance-matters/.

[26] Alfred Ng, *FBI Nabs Alleged Hackers in Theft of 15M Credit Cards from Chipotle, Others*, CNET (Aug. 1, 2018), https://www.cnet.com/news/fbi-nabs-alleged-hackers-in-theft-of-15m-credit-cards-from-chipotle-others/?ftag=CMG-01-10aaa1b.
[27] *See, e.g.*, Taylor Armerding, *The 18 Biggest Data Breaches of the 21st Century*, CSO ONLINE (Dec. 20, 2018), https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html.

and maintained.

76. In 2022, a total of 1,802 data breaches occurred, which represents the second highest number of data events in a single year and just 60 events short of the all-time record of 1,862 in 2021. The education sector had 65 compromises affecting 888,905 individuals.[28]

77. In light of the significant number of data breaches that occurred in the education this decade, Defendant knew or should have known that Plaintiffs' and Class Members' PII would be targeted by cybercriminals.

78. Defendant was clearly aware of the risks it was taking when failing to ensure it had adequate data security.

D. Defendant Could Have Prevented the Breach

79. Data breaches are preventable.[29] As Lucy Thompson wrote in the DATA BREACH AND ENCRYPTION HANDBOOK, "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."[30] She added that "[o]rganizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised . . . ."[31]

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

[28] ITRC_2022-Data-Breach-Report_Final-1.pdf (idtheftcenter.org) (last visited Dec. 29, 2025)

[29] Lucy L. Thomson, "Despite the Alarming Trends, Data Breaches Are Preventable," *in* DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson, ed., 2012).

[30] *Id.* at 17.

[31] *Id.* at 28.

security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that *a data breach never occurs*." [32]

81. In a Data Breach like this, many failures laid the groundwork for the Breach. The FTC has published guidelines that establish reasonable data security practices for businesses. 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.[33] The 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. The guidelines also recommended 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.

82. Upon information and belief, Defendant failed to comply with the reasonable and necessary industry standards necessary to prevent a data breach, including the FTC's guidelines. Upon information and belief, Defendant also failed to ensure that the Defendant 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 reasonable cybersecurity preparation.

---

[32] *Id.*

[33] FTC, *Protecting Personal Information: A Guide for Business*, https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

83. 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."[34]

84. To prevent and detect cyber-attacks, including the attack that resulted in the Data Breach, Defendant could and should have ensured it implemented, as recommended by the Federal Bureau of Investigation, the following measures:

- Implement 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.
- Enable 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.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch 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.
- Manage 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.
- Configure 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.
- Disable 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.

[34] *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

- Implement 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.

- Consider disabling Remote Desktop protocol (RDP) if it is not being used.

- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.

- Execute operating system environments or specific programs in a virtualized environment.

- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[35]

85. Further, to prevent and detect cyber-attacks, including the cyber-attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

- **Update and patch 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….

- **Use 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)….

- **Open 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.

- **Keep your personal information safe**. Check a website's security to ensure the information you submit is encrypted before you provide it….

[35] *Id.* at 3-4.

- **Verify 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.

- **Use and maintain preventative software programs**. Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic….[36]

86. In addition, to prevent and detect cyber-attacks, including the cyber-attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures.

- **Secure internet-facing assets**

  - Apply latest security updates
  - Use threat and vulnerability management
  - Perform regular audit; remove privileged credentials

- **Thoroughly investigate and remediate alerts**

  - Prioritize and treat commodity malware infections as potential full compromise;

- **Include IT Pros in security discussions**

  - Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

- **Build credential hygiene**

[36] *See* Security Tip (ST19-001) Protecting Against Ransomware (original release date Apr. 11, 2019), *available at* https://www.cisa.gov/news-events/news/protecting-against-ransomware

- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin 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**

  - Use 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].[37]

87. Given that Defendant stored the PII of thousands of individuals, including the PII of Plaintiff and the Class Members, Defendant could and should have ensured the Fieldtex systems were capable of preventing and detecting cyber-security attacks.

88. Defendant acquired, collected, and stored the PII of Plaintiff and Class Members.

89. Plaintiff and other Members of the Class entrusted their PII to Defendant.

90. By obtaining, collecting, and storing the PII of Plaintiff and Class Members, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting the PII from disclosure.

91. Given that Defendant was storing the PII of other individuals, Defendant could and should have implemented all of the above measures to prevent and detect cyber-security attacks. However, Defendant failed to do so.

92. The occurrence of the Data Breach indicates that Defendant failed to adequately

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

implement one or more of the above measures to prevent ransomware attacks, resulting in the Data Breach and the exposure of the PII of Plaintiff and Class Members.

93. Defendant could have prevented this Data Breach by properly securing and encrypting the folders, files, and or data fields containing the PII of Plaintiff and Class Members and ensuring Defendant properly secured and encrypted the folders, files, and/or data fields containing the PII of Plaintiff and Class Members. Alternatively, Defendant could have destroyed the data it no longer had a reasonable need to maintain or only stored data in an Internet accessible environment when there was a reasonable need to do so.

94. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the PII of Plaintiff and Class Members from being compromised.

95. The ramifications of Defendant's failure to keep secure the PII of Plaintiff and Class Members are long lasting and severe. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.

E. Defendant's Response to the Data Breach is Inadequate to Protect Plaintiff and the Class

96. Defendant failed to inform Plaintiff and Class Members of the Data Breach in time for them to protect themselves from identity theft.

97. On or around November 20, 2025, Defendant publicly disclosed on its website that, "On or around August 19, 2025, Fieldtex discovered certain unaturhozed activity within its computer systems…Fieldtex confirmed that a limited amount of protected health information may have been impacted in connection with this incident."[38]

[38] https://fieldtex.com/notification-of-data-security-incident/ (last visited Jan. 1, 2026)

98. Despite learning of the Data Breach in August 2025, Defendant did not begin notifying the Plaintiff and Class Members until December 19, 2025—over four (4) months after knowledge of the breach.

99. During these intervals, the cybercriminals had the opportunity to exploit the Plaintiff and Class Members' PII while Defendant was sitting idle and secretly still investigating the Data Breach.

100. By delaying notice of the Breach to Plaintiff and Class Members, Defendant prevented Plaintiff and Class Members from taking earlier actions to protect their PII and mitigate the harms of the Breach.

101. Although Defendant states that it has offered complimentary credit monitoring services to those whose information may have been involved in the Breach, this offer is wholly inadequate given that cybercriminals may wait to misuse the PII.[39] Indeed, some individuals may not experience misuse of their information until months or years later, requiring that Plaintiff and Class Members to pay for credit monitoring for the rest of their lives.

F. Defendant Failed to Comply with FTC Guidelines

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

103. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal information that they keep; properly dispose of personal

[39] *Id.*

information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[40] The guidelines also recommend businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

104. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect patient 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.

105. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiff's and Class Members' PII constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

106. Defendant was always fully aware of their obligations to protect the PII of Plaintiff and Class Members and the significant repercussions that would result from its failure to ensure it utilized adequate cybersecurity measures.

V. CLASS ACTION ALLEGATIONS

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

[40] https://www.bulkorder.ftc.gov/system/files/publications/2_9-00006_716a_protectingpersinfo-508.pdf (last visited Dec. 29, 2025)

108. Plaintiff brings this action against Defendant on behalf of himself and all other individuals similarly situated under Federal Rule of Civil Procedure 23. Plaintiff asserts all claims on behalf of a nationwide class (the "Class") defined as follows:

> All natural persons residing in the United States whose personal identifiable information (PII) was compromised as a result of the Data Breach, including all those who received a Notice Letter.

109. Excluded from the Class is the Defendant, any entity in which Defendant has a controlling interest, and Defendant's 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 judicial staff.

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

111. The proposed Class meets the requirements of Fed. R. Civ. P. 23(a), (b)(1), (b)(2), (b)(3), and (c)(4).

112. **Numerosity:** The proposed Class is so numerous that joinder of all members is impracticable. Although the precise number of individuals is currently unknown, on information and belief, the number of affected individuals is greater than 200,000. Further, The Class is identifiable within Defendant's records.

113. **Typicality:** Plaintiff's claims are typical of the claims of the Class. Plaintiff and all members of the Class were injured through Defendant's uniform misconduct. All had their PII compromised as a result of the Data Breach.

114. **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 their counsel.

115. **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 members of the Class individually to effectively redress Defendant's wrongdoing. Even if Class Members could afford such individual litigation, the court system could not. Individualized litigation presents a 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.

116. **Commonality and Predominance:** 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. When Defendant actually learned of the Data Breach and whether its response was adequate;

b. Whether Defendant failed to adequately safeguard Plaintiff's and Class Members' PII;

c. Whether Defendant owed a duty to Plaintiff and the Class to ensure its systems were capable of adequately protecting their PII, and whether it breached this duty;

d. Whether Defendant breached its duties to Plaintiff and the Class as a result of the Data Breach;

e. Whether Defendant failed to ensure its systems provided adequate cyber security;

f. Whether Defendant knew or should have known its systems and software were vulnerable to cyber-attacks;

g. Whether Defendant's conduct, including its failure to act, resulted in or was the proximate cause of the breach of its company network;

h. Whether Defendant was negligent in failing to ensure its systems and software adhered to reasonable retention policies, thereby greatly increasing the size of the Data Breach;

i. Whether Defendant breached implied contractual duties to Plaintiff and Class Members to use reasonable care in protecting their PII;

j. Whether Defendant 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 Class Members;

k. Whether Defendant continues to breach duties to Plaintiff and Class Members;

l. Whether Plaintiff and the Class suffered injury as a proximate result of Defendant's negligent actions or failures to act;

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

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

VI. CAUSES OF ACTION

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

117. Plaintiff incorporates by reference all preceding factual allegations as though fully alleged here.

118. Fieldtex gathered and stored the PII of Plaintiff and Class Members in exchange for services with the mutual understanding that Fieldtex would protect the PII from unauthorized disclosures to third parties.

119. Fieldtex solicited, collected, stored, and maintained the PII of Plaintiff and Class Members on inadequately secured computer systems and networks.

120. Upon accepting and storing Plaintiff's and Class Members' PII on its computer systems and networks, Defendant 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.

121. Defendant had full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and Class Members could and would suffer if the PII were wrongfully disclosed. Defendant had a duty to Plaintiff and each Class Member to exercise reasonable care in holding, safeguarding, and protecting that information. Plaintiff and Class Members were the foreseeable victims of any inadequate safety and security practices. Plaintiff and the Class Members had no ability to protect their PII that was in Defendant's possession. As such, a special relationship existed between the Defendant and the Plaintiff and Class Members.

122. Defendant owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure

that its computer systems and networks, and the personnel responsible for them, adequately protected the PII.

123. Defendant's duty included a responsibility to implement processes by which it could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

124. Defendant was well aware, or should have been aware, of the fact that cyber criminals routinely target higher education facilitators, including universities, through cyberattacks in an attempt to steal the PII of employees, applicants, students, and business associates.

125. Defendant owed Plaintiff and Class Members a common law duty to use reasonable care to avoid causing foreseeable risk of harm to Plaintiff and the Class when obtaining, storing, using, and managing personal information, including taking action to reasonably safeguard such data and provide notification to Plaintiff and Class Members of any breach in a timely manner so that appropriate action could be taken to minimize losses.

126. Defendant's duty 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.

127. Defendant had duties to protect and safeguard the PII of Plaintiff and Class Members from potential cyberattacks, including by ensuring its systems and software: (i) encrypted any document or report containing PII, (ii) did not permit documents containing unencrypted PII to be maintained on its systems, and (iii) took other similarly common-sense

precautions when dealing with sensitive PII. Additional duties that Defendant owed Plaintiff and Class Members include:

a. Exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting the PII in its possession;

b. Protect the PII in its possession using reasonable and adequate security procedures and systems;

c. Ensure its systems and software were adequately and properly audited and tested;

d. Ensure its systems and software did not store PII for longer than absolutely necessary;

e. Implement processes to quickly detect a data breach, security incident, or intrusion; and

f. Promptly notify Plaintiff and Class Members of any data breach, security incident, or intrusion that affected or may have affected their PII.

128. Plaintiff and Class Members were the intended beneficiaries of Defendant's duties, creating a special relationship between them. Defendant was in a position to ensure that its systems and software were sufficient to protect the PII that Plaintiff and the Class had entrusted to it Defendant.

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

130. Defendant breached its duties of care by failing to adequately protect Plaintiff's and Class Members' PII. Defendant breached its duties by, among other things;

a. Failing to exercise reasonable care in obtaining, retaining securing, safeguarding, deleting, and protecting the PII in its possession;

b. Failing to ensure its systems and software were capable of protecting the PII in its possession using reasonable and adequate security procedures and systems;

c. Failing to ensure its systems and software were adequately and properly audited and tested to avoid cyberattacks;

d. Failing to train its employees regarding how to properly and securely transmit and store PII, including maintaining PII in an encrypted format;

e. Failing to consistently enforce security policies aimed at protecting Plaintiff and Class Members' PII;

f. Failing to implement processes to quickly detect data breaches, security incidents, or intrusions;

g. Failing to abide by reasonable retention and destruction policies for PII of former applicants, students, and employees; and

h. Failing to promptly and accurately notify Plaintiff and Class Members of the Data Breach that affected their PII.

131. Defendant's willful failure to abide by these duties was wrongful, reckless, and grossly negligent in light of the foreseeable risks and known threats.

132. Further, through its failure to provide timely and clear notification of the Data Breach to Plaintiff and Class Members, Defendant prevented Plaintiff and Class Members from taking meaningful, proactive steps to secure their PII and mitigate the impact of the Data Breach.

133. 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.

134. Plaintiff and Class Members suffered harm from Defendant's delay in notifying them of the Data Breach.

135. It was foreseeable that Defendant's failure to use reasonable measures to protect Plaintiff's and Class Members' PII would result in injury to Plaintiff and Class Members.

136. As a proximate and foreseeable result of Defendant's grossly negligent conduct, Plaintiff and Class Members have suffered damages and are at imminent risk of additional harm and damages (as alleged above).

137. The damages Plaintiff and Class Members have suffered (as alleged above) were and are reasonably foreseeable.

138. The damages Plaintiff and the Class have and will suffer were and are the direct and proximate result of Defendant's grossly negligent conduct.

139. 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)

140. Plaintiff incorporates by reference all preceding factual allegations as though fully alleged here.

141. Pursuant to the FTC Act, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and the Class's PII.

142. 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 PII. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendant's duty to protect Plaintiff's and the members of the Class's PII.

143. Defendant solicited, collected, stored, and maintained Plaintiff's and Class Members' PII as part of its regular business, which affects commerce.

144. Defendant violated the FTC Act by failing to use reasonable measures to protect Plaintiff's and Class Members' PII and by failing to comply with applicable industry standards, as described herein.

145. Defendant breached its respective duties to Plaintiff and Class Members under the FTC Act by inadequately protecting its systems and software and failing to ensure its systems and software provided fair, reasonable, or adequate data security to safeguard PII.

146. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential PII.

147. Defendant violated its duty under Section 5 of the FTC Act by failing to use reasonable measures to protect Plaintiff's and the Class's 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 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.

148. 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 organizations 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 the Class.

149. But for Defendant's wrongful and negligent breach of the duties owed to Plaintiff and members of the Class, Plaintiff and members of the Class would not have been injured.

150. The injuries and harm suffered by Plaintiff and members of the Class was the reasonably foreseeable result of Defendant's breach of duties. Defendant knew or should have known its systems and software were incapable of safeguarding Plaintiff's and Class Members' PII and that a breach would cause Plaintiff and members of the Class to suffer the foreseeable harms associated with the exposure of their PII.

151. Had Plaintiff and the Class known that Defendant did not adequately protect their PII, Plaintiff and members of the Class would not have entrusted Defendant with their PII.

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

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

154. 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 Defendant, 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.

155. Defendant's duty to use reasonable care in protecting Plaintiff's and Class Members' Private Information arose not only as a result of the statutes and regulations described

above, but also because Defendant is bound by industry standards to protect and secure Private Information in its possession and control.

156. As a direct and proximate result of Defendant's negligence per se, Plaintiff and the Class have suffered harm, including actual misuse of their PII; loss of time and money resolving fraudulent charges; loss of time and money obtaining protections against future identity theft; lost control over the value of PII; harm resulting from damaged credit scores and information; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen PII, entitling them to damages in an amount to be proven at trial.

157. Additionally, as a direct and proximate result of Defendant's negligence per se, Plaintiff and Class members have suffered and will suffer the continued risks of exposure of their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant's fails to undertake appropriate and adequate measures to protect their PII in their continued possession.

THIRD CAUSE OF ACTION
BREACH OF THIRD-PARTY BENEFICIARY CONTRACT
(On Behalf of Plaintiff and the Class)

158. Plaintiff incorporates by reference all preceding factual allegations as though fully alleged here.

159. On information and belief, Defendant entered into contracts to provide organization machine operators, first aid and EMS products, and OTC Benefit Packages to its clients, to the benefit of Plaintiff and Class Members.

160. On information and belief, these contracts are virtually identical and were made expressly for the benefit of Plaintiff and Class Members, as it was their Private Information that Defendant agreed to receive and protect through its services. Thus, the benefit of collection and

protection of the Private Information belonging to Plaintiff and Class Members was the direct and primary objective of the contracting parties.

161. Defendant knew that if it were to breach these contracts with its clients, Plaintiff and Class Members would be harmed.

162. Defendant breached its contracts with its clients and as a result Plaintiff and Class Members were affected by this Data Breach when it failed to use reasonable data security measures that could have prevented the Data Breach, and when it failed to timely notify Plaintiff and Class Members regarding the breach.

163. As foreseen, Plaintiff and Class Members were harmed by Defendants' failure to use reasonable data security measures to store the Private Information that Plaintiff and Class Members provided to their patients who in turn provided that information to Defendants, and Defendants' failure to timely notify Plaintiff and Class Members, including but not limited to, the continuous and substantial risk of harm through the loss of their Private Information.

164. Accordingly, Plaintiff and Class Members are entitled to damages in an amount to be determined at trial, including actual, consequential, and nominal damages, along with costs and attorneys' fees incurred in this action.

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

165. Plaintiff incorporates by reference all preceding factual allegations as though fully alleged here. This Count is pled in the alternative to the Breach of Third-Party Beneficiary Contract Count above.

166. Plaintiff and Class Members conferred a monetary benefit on Defendant by providing Defendant with their valuable PII.

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

168. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to avoid their 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.

169. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiff and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

170. Defendant acquired the monetary benefit and PII through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

171. If Plaintiff and Class Members knew that Defendant had not secured their PII, they would not have agreed to provide their PII to Defendant.

172. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their PII, which

remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect PII in its continued possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

173. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

174. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly received from them.

FIFTH CAUSE OF ACTION
INJUNCTIVE AND DECLARATORY RELIEF
(On Behalf of Plaintiff and the Class)

175. Plaintiff incorporates by reference all preceding factual allegations as though fully alleged here.

176. This count is brought under the Federal Declaratory Judgment Act, 28 U.S.C. § 2201.

177. As previously alleged and pleaded, Defendant owes duties of care to Plaintiff and Class Members that require them to adequately secure their PII.

178. Defendant still possesses the PII of Plaintiff and the Class Members.

179. Defendant has not satisfied its contractual obligations and legal duties to Plaintiff and the Class Members.

180. Defendant has claimed that it will "continually evaluate and modify our practices and internal controls to enhance the security and privacy of [Plaintiff's and Class Members']

personal information." But there is nothing to prevent Defendant from reversing any changes made once it has weathered the increased public attention resulting from this Breach.

181. Plaintiff, therefore, seeks a declaration (1) that Defendant's existing security measures do not comply with its contractual obligations and duties of care to provide adequate security, and (2) that to comply with its contractual obligations and duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to:

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

b. Ordering Defendant to significantly increase its spending on cybersecurity including systems and personnel;

c. Ordering Defendant to engage third-party security auditors and internal personnel to run automated security monitoring;

d. Ordering that Defendant audit, test, and train their security personnel regarding any new or modified procedures;

e. Ordering that Defendant protect Plaintiff's and the Class's PII by, among other things, guaranteeing it has firewalls and access controls so that if one area of Defendant's systems are compromised, hackers cannot gain access to other portions of its systems;

f. Ordering that Defendant cease storing unencrypted PII on its systems;

g. Ordering that Defendant conduct regular database scanning and securing

checks;

h. Ordering Defendant to routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

i. Ordering Defendant to implement and enforce adequate retention policies for PII, including destroying, in a reasonably secure manner, PII once it is no longer necessary for it to be retained; and

j. Ordering Defendant to meaningfully educate its current, former, and prospective employees and subcontractors about the threats they face as a result of the loss of their financial and personal information to third parties, as well as the steps they must take to protect themselves.

VII. PRAYER FOR RELIEF

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

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

b. A judgment in favor of Plaintiff and the Class awarding them appropriate monetary relief, including compensatory damages, punitive damages, attorneys' 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 Defendant 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 all appropriate issues raised in this Class Action Complaint.

Dated: January 7, 2026

Respectfully submitted,

/s/Randi Kassan
Randi Kassan (NY Bar No 4375754)
MILBERG, PLLC
100 Garden City Plaza, Suite 408
Garden City, NY 11530
Telephone: (516) 741-5600
rkassan@milberg.com

William B. Federman, *pro hac vice forthcoming*
Jessica A. Wilkes, *pro hac vice forthcoming*
FEDERMAN & SHERWOOD
10205 North Pennsylvania Avenue
Oklahoma City, OK 73120
T: (405) 235-1560
E: WBF@federmanlaw.com
E: JAW@federmanlaw.com

Counsel for the Plaintiff and the Proposed Class