

**UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF NEW YORK**

ALEGRIA CLARK, individually and on
behalf of all others similarly situated,

Plaintiff,

v.

FIELDTEX PRODUCTS, INC.,

Defendant.

Case No. _____

CLASS ACTION

JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiff Alegria Clark (“Plaintiff”), individually, and on behalf of all others similarly situated (collectively, “Class members”), by and through her attorneys, brings this Class Action Complaint against Defendant Fieldtex Products, Inc. (“Fieldtex” or “Defendant”), and complains and alleges upon personal knowledge as to herself and information and belief as to all other matters.

INTRODUCTION

1. Plaintiff brings this class action against Defendant for its failure to secure and safeguard approximately 274,363 individuals’ (including Plaintiff’s) personally identifying information (“PII”) and personal health information (“PHI”), including names, addresses, dates of birth, insurance member identification numbers, plan names, effective terms, and gender.

2. Fieldtex is a contract manufacturing, medical supplies fulfillment, and supplemental benefits administration company based in Rochester, New York.

3. On or about August 19, 2025, Fieldtex discovered an unauthorized third party gained access to its network systems and accessed and acquired files containing

the PII/PHI of customers of Fieldtex's health plan clients, including Plaintiff and Class members (the "Data Breach").

4. Defendant owed a duty to Plaintiff and Class members to implement and maintain reasonable and adequate security measures to secure, protect, and safeguard their PII/PHI against unauthorized access and disclosure. Defendant breached that duty by, among other things, failing to implement and maintain reasonable security procedures and practices to protect Plaintiff's and Class members' PII/PHI from unauthorized access and disclosure.

5. As a result of Defendant's inadequate security and breach of its duties and obligations, the Data Breach occurred, and Plaintiff's and Class members' PII/PHI was accessed and disclosed. This action seeks to remedy these failings and their consequences. Plaintiff brings this action on behalf of herself and all persons whose PII/PHI was exposed as a result of the Data Breach, which Defendant discovered on or about August 19, 2025.

6. Plaintiff, on behalf of herself and all other Class members, asserts claims for negligence, negligence per se, and unjust enrichment, and seeks declaratory relief, injunctive relief, monetary damages, statutory damages, punitive damages, equitable relief, and all other relief authorized by law.

PARTIES

Plaintiff Alegria Clark

7. Plaintiff is a citizen and resident of Illinois.

8. Plaintiff's health plan contracts with Fieldtex for supplemental benefits administration services. In connection with obtaining such services from Fieldtex, Plaintiff's insurance provided Plaintiff's PII/PHI to Fieldtex.

9. At all relevant times, Fieldtex stored and maintained Plaintiff's PII/PHI on its network systems, including the systems impacted in the Data Breach.

10. Plaintiff received a notice letter from Fieldtex notifying her that her PII/PHI was in the files accessed and acquired by an unauthorized third party in the Data Breach.

11. As a direct result of the Data Breach, Plaintiff has suffered injury and damages including, *inter alia*, a substantial and imminent risk of identity theft and medical identity theft; the wrongful disclosure and loss of confidentiality of her highly sensitive PII/PHI; time and effort lost attempting to mitigate the harm caused by the Data Breach; and deprivation of the value of her PII/PHI.

Defendant Fieldtex Products, Inc.

12. Defendant Fieldtex Products, Inc. is a New York corporation with its principal place of business located at 2921 Brighton Henrietta Town Line Rd, Rochester, NY 14623.

JURISDICTION AND VENUE

13. The Court has subject matter jurisdiction over Plaintiff's claims under 28 U.S.C. § 1332(d)(2), because (a) there are 100 or more Class members, (b) at least one Class member is a citizen of a state that is diverse from Defendant's citizenship, and (c) the matter in controversy exceeds \$5,000,000, exclusive of interest and costs.

14. This Court has general personal jurisdiction over Defendant because it is organized under the laws of this State and maintains its principal place of business in this District.

15. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because Defendant's principal place of business is in this District and a substantial part of the events, acts, and omissions giving rise to Plaintiff's claims occurred in this District.

FACTUAL ALLEGATIONS

Overview of Fieldtex

16. Fieldtex offers contract sewing and manufacturing services, medical supplies fulfillment services, and over the counter supplemental benefits administration services on behalf of various health plans.¹

17. In the regular course of its business, Fieldtex collects and maintains the PII/PHI of the customers of its health plan clients, including Plaintiff and Class members. Fieldtex requires its health plan clients to provide it with their customers' PII/PHI, including the information stolen in the Data Breach, before it provides them benefit administration services.

18. On its website, Fieldtex promises, "[p]rotecting patient privacy is a cornerstone of our operations. Every step of our process is fully HIPAA-compliant, ensuring that sensitive information is handled securely and professionally, giving you peace of mind that your patients' data is safeguarded."²

¹ *Divisions*, FIELDTEX, <https://fieldtex.com/#divisions> (last accessed Dec. 22, 2025).

² *Why Fieldtex is Your Ideal Fulfillment Partner*, FIELDTEX (June 9, 2025), <https://fieldtex.com/why-fieldtex-is-your-ideal-fulfillment-partner/> (last accessed Dec. 22, 2025).

19. Plaintiff and Class members are, or were, customers of Fieldtex's clients, and Fieldtex stored Plaintiff's and Class members' PII/PHI on its network systems.

The Data Breach

20. On or about August 19, 2025, Fieldtex discovered that an unauthorized third party gained access to its network systems and acquired files containing the PII/PHI of Plaintiff and Class members, including their names, addresses, dates of birth, insurance member identification numbers, plan names, effective terms, and gender.³

21. Despite discovering the Data Breach on or about August 19, 2025, Fieldtex waited until approximately November 20, 2025—over three months after the Data Breach—to announce the Data Breach and begin notifying Plaintiff and Class members that their PII/PHI was accessed and acquired by unauthorized persons.⁴

22. The Akira ransomware group claimed responsibility for the Data Breach and added Fieldtex to its dark web data breach site.⁵

23. Defendant's failure to promptly notify Plaintiff and Class members that their PII/PHI was disclosed, accessed, and stolen virtually ensured that the unauthorized third parties who exploited those security lapses could monetize, misuse, or disseminate that PII/PHI before Plaintiff and Class members could take affirmative steps to protect their sensitive information. As a result, Plaintiff and Class members will suffer indefinitely from the substantial and concrete risk that their identities will be (or already have been) stolen and misappropriated.

³ *Notification of Data Security Incident*, FIELDTEX (Nov. 20, 2025), <https://fieldtex.com/notification-of-data-security-incident/>.

⁴ *See id.*

⁵ Eduard Kovacs, *Fieldtex Data Breach Impacts 238,000*, SC. WEEK (Dec. 12, 2025 8:12 AM), <https://www.securityweek.com/fieldtex-data-breach-impacts-238000/>.

Defendant Knew that Criminals Target PII/PHI

24. At all relevant times, Defendant knew, or should have known, that the PII/PHI that it collects and stores was a target for malicious actors. Despite such knowledge, Defendant failed to implement and maintain reasonable and appropriate data privacy and security measures to protect Plaintiffs and Class members' PII/PHI from unauthorized disclosures and cyberattacks that it should have anticipated and guarded against.

25. It is well known among companies that store sensitive personally identifying information that such information—such as the PII/PHI stolen in the Data Breach—is valuable and frequently targeted by criminals. In a recent article, *Business Insider* noted that “[d]ata breaches are on the rise for all kinds of businesses, including retailers Many of them were caused by flaws in . . . systems either online or in stores.”⁶

26. Cyber criminals seek out PHI at a greater rate than other sources of personal information. In a 2025 report, Kroll found that “the healthcare industry was the most breached” in 2024.⁷ The company found that 23% of the breaches that it handled responses for were from the healthcare industry, up from 18% in 2023.⁸

⁶ Dennis Green, Mary Hanbury & Aine Cain, *If you bought anything from these 19 companies recently, your data may have been stolen*, BUS. INSIDER (Nov. 19, 2019), <https://www.businessinsider.com/data-breaches-retailers-consumer-companies-2019-1>.

⁷ *Data Breach Outlook*, KROLL, <https://www.kroll.com/en/insights/publications/cyber/data-breach-outlook-2025> (last accessed Dec. 22, 2025).

⁸ *See id.*

27. PII/PHI is a valuable property right.⁹ The value of PII/PHI as a commodity is measurable.¹⁰ “Firms are now able to attain significant market valuations by employing business models predicated on the successful use of personal data within the existing legal and regulatory frameworks.”¹¹ American companies are estimated to have spent over \$19 billion on acquiring consumers’ personal data in 2018.¹² It is so valuable to identity thieves that once PII has been disclosed, criminals often trade it on the “cyber black-market,” or the “dark web,” for many years.

28. As a result of the real and significant value of these data, identity thieves and other cyber criminals have openly posted credit card numbers, Social Security numbers, PII/PHI, and other sensitive information directly on various internet websites making the information publicly available. This information from various breaches, including the information exposed in the Data Breach, can be readily aggregated with other such data and become more valuable to thieves and more damaging to victims.

⁹ See Marc van Lieshout, *The Value of Personal Data*, 457 Int’l Fed’n for Info. Processing 26 (May 2015) (“The value of [personal] information is well understood by marketers who try to collect as much data about personal conducts and preferences as possible . . .”), https://www.researchgate.net/publication/283668023_The_Value_of_Personal_Data.

¹⁰ See Robert Lowes, *Stolen EHR [Electronic Health Record] Charts Sell for \$50 Each on Black Market*, MEDSCAPE (April 28, 2014), <http://www.medscape.com/viewarticle/824192>.

¹¹ Organization for Economic Co-operation and Development, *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD iLIBRARY (Apr. 2, 2013), https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en.

¹² IAB Data Center of Excellence, *U.S. Firms to Spend Nearly \$19.2 Billion on Third-Party Audience Data and Data-Use Solutions in 2018, Up 17.5% from 2017*, INTERACTIVE ADVERT. BUREAU (Dec. 5, 2018), <https://www.iab.com/news/2018-state-of-data-report/>.

29. PHI is particularly valuable and has been referred to as a “treasure trove for criminals.”¹³ A cybercriminal who steals a person’s PHI can end up with as many as “seven to ten personal identifying characteristics of an individual.”¹⁴

30. All-inclusive health insurance dossiers containing sensitive health insurance information, names, addresses, telephone numbers, email addresses, Social Security numbers, and bank account information, complete with account and routing numbers, can fetch up to \$1,200 to \$1,300 each on the black market.¹⁵ According to a report released by the Federal Bureau of Investigation’s (“FBI”) Cyber Division, criminals can sell healthcare records for 50 times the price of a stolen Social Security or credit card number.¹⁶

31. Criminals can use stolen PII/PHI to extort a financial payment by “leveraging details specific to a disease or terminal illness.”¹⁷ Quoting Carbon Black’s Chief Cybersecurity Officer, one recent article explained: “Traditional criminals understand the power of coercion and extortion . . . By having healthcare information—

¹³ See Andrew Steager, *What Happens to Stolen Healthcare Data*, HEALTHTECH MAG. (Oct. 20, 2019), <https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon> (quoting Tom Kellermann, Chief Cybersecurity Officer, Carbon Black, stating “Health information is a treasure trove for criminals.”).

¹⁴ *Id.*

¹⁵ See SC Staff, *Health Insurance Credentials Fetch High Prices in the Online Black Market*, SC MAG. (July 16, 2013), <https://www.scmagazine.com/news/breach/health-insurance-credentials-fetch-high-prices-in-the-online-black-market>.

¹⁶ See Federal Bureau of Investigation, *Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain* (April 8, 2014), <https://www.illumweb.com/wp-content/uploads/ill-mo-uploads/103/2418/health-systems-cyber-intrusions.pdf>.

¹⁷ Steager, *supra* note 13.

specifically, regarding a sexually transmitted disease or terminal illness—that information can be used to extort or coerce someone to do what you want them to do.”¹⁸

32. Consumers place a high value on the privacy of their data, as they should. Researchers shed light on how much consumers value their data privacy—and the amount is considerable. Indeed, studies confirm that “when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites.”¹⁹

33. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers’ PII/PHI has thus deprived that consumer of the full monetary value of the consumer’s transaction with the company.

Theft of PII/PHI Has Grave and Lasting Consequences for Victims

34. Theft of PII/PHI can have serious consequences for the victim. The FTC warns consumers that identity thieves use PII/PHI to receive medical treatment, start new utility accounts, and incur charges and credit in a person’s name.^{20 21}

¹⁸ *Id.*

¹⁹ Janice Y. Tsai et al., *The Effect of Online Privacy Information on Purchasing Behavior, An Experimental Study*, 22(2) INFO. SYS. RSCH. 254 (June 2011) <https://www.jstor.org/stable/23015560?seq=1>.

²⁰ See Federal Trade Commission, *What to Know About Identity Theft*, FTC CONSUMER INFO., <https://www.consumer.ftc.gov/articles/what-know-about-identity-theft> (last accessed Dec. 22, 2025).

²¹ The FTC defines identity theft as “a fraud committed or attempted using the identifying information of another person without authority.” 12 C.F.R. § 1022.3(h). The FTC describes “identifying information” as “any name or number that may be used, alone or in conjunction with any other information, to identify a specific person,” including, among other things, “[n]ame, social security number, date of birth, official State or government issued driver’s license or identification number, alien registration number, government passport number, employer or taxpayer identification number.” 12 C.F.R. § 1022.3(g).

35. Experian, one of the largest credit reporting companies in the world, warns consumers that “[i]dentity thieves can profit off your personal information” by, among other things, selling the information, taking over accounts, using accounts without permission, applying for new accounts, obtaining medical procedures, filing a tax return, and applying for government benefits.²²

36. Identity theft is not an easy problem to solve. In a 2025 survey, the Identity Theft Resource Center found that 20% of victims of identity misuse needed more than 30 days to resolve issues stemming from identity theft and 13% required three months or more.²³

37. Theft of PII is even more serious when it includes theft of PHI. Data breaches involving medical information “typically leave[] a trail of falsified information in medical records that can plague victims’ medical and financial lives for years.”²⁴ It “is also more difficult to detect, taking almost twice as long as normal identity theft.”²⁵ In warning consumers on the dangers of medical identity theft, the FTC states that an identity thief may use PII/PHI “to see a doctor, get prescription drugs, buy medical

²² See Louis DeNicola, *What Can Identity Thieves Do with Your Personal Information and How Can You Protect Yourself*, EXPERIAN (May 21, 2023), <https://www.experian.com/blogs/ask-experian/what-can-identity-thieves-do-with-your-personal-information-and-how-can-you-protect-yourself/>.

²³ Identity Theft Resource Center, *2025 Consumer Impact Report*, IDENTITY THEFT RES. CTR. (2025), <https://www.idtheftcenter.org/publication/itrc-2025-consumer-impact-report/> (last accessed Dec. 22, 2025).

²⁴ Pam Dixon & John Emerson, *The Geography of Medical Identity Theft*, WORLD PRIV. F. (Dec. 12, 2017), http://www.worldprivacyforum.org/wp-content/uploads/2017/12/WPF_Geography_of_Medical_Identity_Theft_fs.pdf.

²⁵ See Federal Bureau of Investigation, *Health Care Systems and Medical Devices at Risk . . .*, *supra* note 16.

devices, submit claims with your insurance provider, or get other medical care.”²⁶ The FTC also warns, “If the thief’s health information is mixed with yours it could affect the medical care you’re able to get or the health insurance benefits you’re able to use.”²⁷

38. A report published by the World Privacy Forum and presented at the US FTC Workshop on Informational Injury describes what medical identity theft victims may experience:

- a. Changes to their health care records, most often the addition of falsified information, through improper billing activity or activity by imposters. These changes can affect the healthcare a person receives if the errors are not caught and corrected.
- b. Significant bills for medical goods and services neither sought nor received.
- c. Issues with insurance, co-pays, and insurance caps.
- d. Long-term credit problems based on problems with debt collectors reporting debt due to identity theft.
- e. Serious life consequences resulting from the crime; for example, victims have been falsely accused of being drug users based on falsified entries to their medical files; victims have had their children removed from them due to medical activities of the imposter; victims have been denied jobs due to incorrect information placed in their health files due to the crime.
- f. As a result of improper and/or fraudulent medical debt reporting, victims may not qualify for mortgage or other loans and may experience other financial impacts.
- g. Phantom medical debt collection based on medical billing or other identity information.

²⁶ See Federal Trade Commission, *What to Know About Medical Identity Theft*, FTC CONSUMER INFO., <https://www.consumer.ftc.gov/articles/what-know-about-medical-identity-theft> (last accessed Dec. 22, 2025).

²⁷ *Id.*

h. Sales of medical debt arising from identity theft can perpetuate a victim's debt collection and credit problems, through no fault of their own.²⁸

39. There may also be time lags between when sensitive personal information is stolen, when it is used, and when a person discovers it has been used. On average it takes approximately three months for consumers to discover their identity has been stolen and used, but it takes some individuals up to three years to learn that information.²⁹

40. It is within this context that Plaintiff and all other Class members must now live with the knowledge that their PII/PHI is forever in cyberspace and was taken by someone intending to use that information for any number of improper purposes and scams, including making the information available for sale on the black-market.

Damages Sustained by Plaintiff and Class Members

41. Plaintiff and Class members have suffered and will suffer injury, including, but not limited to: (i) a substantially increased and imminent risk of identity theft; (ii) the disclosure, compromise, and theft of their PII/PHI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII/PHI; (iv) lost opportunity costs associated with efforts to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII/PHI which remains in Defendant's possession; and (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII/PHI compromised as a result of the Data Breach.

²⁸ See Dixon & Emerson, *supra* note 24.

²⁹ John W. Coffey, *Difficulties in Determining Data Breach Impacts*, 17 J. OF SYSTEMICS, CYBERNETICS AND INFORMATICS 9 (2019), <http://www.iiiisci.org/journal/pdv/sci/pdfs/IP069LL19.pdf>.

CLASS ALLEGATIONS

42. This action is brought and may be properly maintained as a class action pursuant to Fed. R. Civ. P. 23.

43. Plaintiff brings this action on behalf of herself and all members of the following Class of similarly situated persons:

All persons whose PII/PHI was accessed in the Data Breach by unauthorized persons, including all who were sent a notice of the Data Breach.

44. Excluded from the Class are Fieldtex Products, Inc. and its affiliates, parents, subsidiaries, employees, officers, agents, board members, and directors, as well as the judge(s) presiding over this matter and the clerks of said judge.

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

46. The members in the Class are so numerous that joinder of each of the Class members in a single proceeding would be impracticable. Fieldtex has reported to the U.S. Department of Health and Human Services that approximately 274,363 individuals were affected by the Data Breach.³⁰

47. Common questions of law and fact exist as to all Class members and predominate over any potential questions affecting only individual Class members. Such common questions of law or fact include, *inter alia*:

³⁰ See *Cases Currently Under Investigation*, HHS, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last accessed Dec. 22, 2025).

- a. whether Defendant had a duty to implement and maintain reasonable security procedures and practices to protect and secure Plaintiff's and Class members' PII/PHI from unauthorized access and disclosure;
- b. whether Defendant had duties not to disclose the PII/PHI of Plaintiff and Class members to unauthorized third parties;
- c. whether Defendant failed to exercise reasonable care to secure and safeguard Plaintiff's and Class members' PII/PHI;
- d. whether Defendant breached its duties to protect Plaintiff's and Class members' PII/PHI; and
- e. whether Plaintiff and Class members are entitled to damages and the measure of such damages and relief.

48. Fieldtex engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiff, on behalf of herself and all other Class members. Individual questions, if any, pale in comparison, in both quantity and quality, to the numerous common questions that dominate this action.

49. Plaintiff's claims are typical of the claims of the Class. Plaintiff, like all proposed members of the Class, had her PII/PHI compromised in the Data Breach. Plaintiff and Class members were injured by the same wrongful acts, practices, and omissions committed by Fieldtex, as described herein. Plaintiff's claims therefore arise from the same practices or course of conduct that give rise to the claims of all Class members.

50. Plaintiff will fairly and adequately protect the interests of the Class members. Plaintiff is an adequate representative of the Class in that she has no interests adverse to, or that conflict with, the Class she seeks to represent. Plaintiff has retained counsel with substantial experience and success in the prosecution of complex consumer protection class actions of this nature.

51. A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages and other financial detriment suffered by Plaintiff and Class members are relatively small compared to the burden and expense that would be required to individually litigate their claims against Fieldtex, so it would be impracticable for Class members to individually seek redress from Fieldtex's wrongful conduct. Even if Class members could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

CAUSES OF ACTION

COUNT I **NEGLIGENCE**

52. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

53. Fieldtex owed a duty to Plaintiff and Class members to exercise reasonable care in safeguarding and protecting the PII/PHI in its possession, custody, or control.

54. Fieldtex knew or should have known the risks of collecting and storing Plaintiff's and all other Class members' PII/PHI and the importance of maintaining secure systems. Fieldtex knew or should have known of the many data breaches that targeted entities that collect and store PII/PHI in recent years.

55. Given the nature of Fieldtex's business, the sensitivity and value of the PII/PHI it collects, stores, and maintains, and the resources at its disposal, Fieldtex should have identified the vulnerabilities to its systems and prevented the Data Breach from occurring.

56. Fieldtex breached these duties by failing to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII/PHI by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect PII/PHI entrusted to it—including Plaintiff's and Class members' PII/PHI.

57. It was reasonably foreseeable to Fieldtex that its failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII/PHI by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems would result in the unauthorized release, disclosure, and dissemination of Plaintiff's and Class members' PII/PHI to unauthorized individuals.

58. But for Fieldtex's negligent conduct or breach of the above-described duties owed to Plaintiff and Class members, their PII/PHI would not have been compromised.

59. As a result of Fieldtex's above-described wrongful actions, inaction, and want of ordinary care that directly and proximately caused the Data Breach, Plaintiff and Class members have suffered and will suffer injury, including, but not limited

to: (i) a substantial increase in the likelihood of identity theft; (ii) the compromise, publication, and theft of their PII/PHI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII/PHI; (iv) lost opportunity costs associated with efforts to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII/PHI which remains in Fieldtex's possession; and (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII/PHI compromised as a result of the Data Breach.

COUNT II
NEGLIGENCE PER SE

60. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

61. Fieldtex's duties arise from, *inter alia*, the HIPAA Privacy Rule ("Standards for Privacy of Individually Identifiable Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and E, and the HIPAA Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C (collectively, "HIPAA Privacy and Security Rules").

62. Fieldtex's duties also arise from Section 5 of the FTC Act ("FTCA"), 15 U.S.C. § 45(a)(1), which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted by the FTC, the unfair act or practice by a business, such as Fieldtex, of failing to employ reasonable measures to protect and secure PII/PHI.

63. Fieldtex violated HIPAA Privacy and Security Rules and Section 5 of the FTCA by failing to use reasonable measures to protect Plaintiff's and other Class

members' PII/PHI, by failing to provide timely notice, and by not complying with applicable industry standards. Fieldtex's conduct was particularly unreasonable given the nature and amount of PII/PHI it obtains and stores, and the foreseeable consequences of a data breach involving PII/PHI including, specifically, the substantial damages that would result to Plaintiff and the other Class members.

64. Fieldtex's violation of the HIPAA Privacy and Security Rules and Section 5 of the FTCA constitutes negligence per se.

65. Plaintiff and Class members are within the class of persons that the HIPAA Privacy and Security Rules and Section 5 of the FTCA were intended to protect.

66. The harm occurring as a result of the Data Breach is the type of harm that the HIPAA Privacy and Security Rules and Section 5 of the FTCA were intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair practices or deceptive practices, caused the same type of harm that has been suffered by Plaintiff and Class members as a result of the Data Breach.

67. It was reasonably foreseeable to Fieldtex that its failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII/PHI by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems, would result in the release, disclosure, and dissemination of Plaintiff's and Class members' PII/PHI to unauthorized individuals.

68. The injury and harm that Plaintiff and the other Class members suffered was the direct and proximate result of Fieldtex's violations of the HIPAA Privacy and Security Rules and Section 5 of the FTCA. Plaintiff and Class members have suffered and will suffer injury, including, but not limited to: (i) a substantial increase in the likelihood of identity theft; (ii) the compromise, publication, and theft of their PII/PHI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII/PHI; (iv) lost opportunity costs associated with efforts to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII/PHI which remains in Fieldtex's possession; and (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII/PHI compromised as a result of the Data Breach.

COUNT III
UNJUST ENRICHMENT

69. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

70. Plaintiff and Class members conferred a monetary benefit upon Fieldtex in the form of money paid to their health plans, which the health plans in turn used to pay for services from Fieldtex, and through the provision of their PII/PHI, which was also necessary for Fieldtex to provide its services. Plaintiff did so with an implicit understanding that some of these payments would go towards protecting Plaintiff's PII/PHI.

71. Fieldtex accepted or had knowledge of the benefits conferred upon it by Plaintiff and Class members. Fieldtex benefitted from the receipt of Plaintiff's and Class

members' PII/PHI, as this was used to provide supplemental benefits administration services and billing services.

72. As a result of Fieldtex's conduct, Plaintiff and Class members suffered actual damages in an amount equal to the difference in value between their payments made with reasonable data privacy and security practices and procedures that they paid for and expected, and those payments without reasonable data privacy and security practices and procedures that they received.

73. Fieldtex should not be permitted to retain the money belonging to Plaintiff and Class members because Fieldtex failed to adequately implement the data privacy and security procedures for itself that Plaintiff and Class members expected and that were otherwise mandated by federal, state, and local laws and industry standards.

74. Plaintiff and Class members have no adequate remedy at law.

75. Fieldtex should be compelled to provide for the benefit of Plaintiff and Class members all unlawful proceeds received by it as a result of the conduct and Data Breach alleged herein.

PRAYER FOR RELIEF

Plaintiff, individually and on behalf of all other members of the Class, respectfully requests that the Court enter judgment in her favor and against Defendant as follows:

A. Certifying the Class as requested herein, designating Plaintiff as Class Representative, and appointing Plaintiff's counsel as Class Counsel;

B. Awarding Plaintiff and the Class appropriate monetary relief, including actual damages, statutory damages, punitive damages, restitution, and disgorgement;

C. Awarding Plaintiff and the Class equitable, injunctive, and declaratory relief, as may be appropriate. Plaintiff, on behalf of herself and the Class, seeks appropriate injunctive relief designed to prevent Defendant from experiencing another data breach by adopting and implementing best data security practices to safeguard PII/PHI and to provide or extend credit monitoring services and similar services to protect against all types of identity theft and medical identity theft;

D. Awarding Plaintiff and the Class pre-judgment and post-judgment interest to the maximum extent allowable;

E. Awarding Plaintiff and the Class reasonable attorneys' fees, costs, and expenses, as allowable; and

F. Awarding Plaintiff and the Class such other favorable relief as allowable under law.

JURY TRIAL DEMANDED

Plaintiff demands a trial by jury of all claims in this Class Action Complaint so triable.

Dated: December 22, 2025

Respectfully submitted,

/s/ Adam Pollock

Adam Pollock

POLLOCK COHEN LLP

111 Broadway, Suite 1804

New York, NY 10006

Tel: 212-337-5361

adam@pollockcohen.com

Ben Barnow*
Anthony L. Parkhill*
BARNOW AND ASSOCIATES, P.C.
205 West Randolph Street, Suite 1630
Chicago, IL 60606
Tel: 312.621.2000
Fax: 312.641.5504
b.barnow@barnowlaw.com
aparkhill@barnowlaw.com

Counsel for Plaintiff

**Pro hac vice forthcoming*

CIVIL COVER SHEET

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

I. (a) PLAINTIFFS

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

(c) Attorneys (Firm Name, Address, and Telephone Number)

DEFENDANTS

County of Residence of First Listed Defendant _____
(IN U.S. PLAINTIFF CASES ONLY)

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

Attorneys (If Known)

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

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

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

- | | PTF | DEF | | PTF | DEF |
|---|----------------------------|----------------------------|---|----------------------------|----------------------------|
| Citizen of This State | <input type="checkbox"/> 1 | <input type="checkbox"/> 1 | Incorporated or Principal Place of Business In This State | <input type="checkbox"/> 4 | <input type="checkbox"/> 4 |
| Citizen of Another State | <input type="checkbox"/> 2 | <input type="checkbox"/> 2 | Incorporated and Principal Place of Business In Another State | <input type="checkbox"/> 5 | <input type="checkbox"/> 5 |
| Citizen or Subject of a Foreign Country | <input type="checkbox"/> 3 | <input type="checkbox"/> 3 | Foreign Nation | <input type="checkbox"/> 6 | <input type="checkbox"/> 6 |

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

Click here for: [Nature of Suit Code Descriptions.](#)

CONTRACT	TORTS	FORFEITURE/PENALTY	BANKRUPTCY	OTHER STATUTES	
<input type="checkbox"/> 110 Insurance <input type="checkbox"/> 120 Marine <input type="checkbox"/> 130 Miller Act <input type="checkbox"/> 140 Negotiable Instrument <input type="checkbox"/> 150 Recovery of Overpayment & Enforcement of Judgment <input type="checkbox"/> 151 Medicare Act <input type="checkbox"/> 152 Recovery of Defaulted Student Loans (Excludes Veterans) <input type="checkbox"/> 153 Recovery of Overpayment of Veteran's Benefits <input type="checkbox"/> 160 Stockholders' Suits <input type="checkbox"/> 190 Other Contract <input type="checkbox"/> 195 Contract Product Liability <input type="checkbox"/> 196 Franchise	PERSONAL INJURY <input type="checkbox"/> 310 Airplane <input type="checkbox"/> 315 Airplane Product Liability <input type="checkbox"/> 320 Assault, Libel & Slander <input type="checkbox"/> 330 Federal Employers' Liability <input type="checkbox"/> 340 Marine <input type="checkbox"/> 345 Marine Product Liability <input type="checkbox"/> 350 Motor Vehicle <input type="checkbox"/> 355 Motor Vehicle Product Liability <input type="checkbox"/> 360 Other Personal Injury <input type="checkbox"/> 362 Personal Injury - Medical Malpractice	PERSONAL INJURY <input type="checkbox"/> 365 Personal Injury - Product Liability <input type="checkbox"/> 367 Health Care/Pharmaceutical Personal Injury Product Liability <input type="checkbox"/> 368 Asbestos Personal Injury Product Liability PERSONAL PROPERTY <input type="checkbox"/> 370 Other Fraud <input type="checkbox"/> 371 Truth in Lending <input type="checkbox"/> 380 Other Personal Property Damage <input type="checkbox"/> 385 Property Damage Product Liability	<input type="checkbox"/> 625 Drug Related Seizure of Property 21 USC 881 <input type="checkbox"/> 690 Other LABOR <input type="checkbox"/> 710 Fair Labor Standards Act <input type="checkbox"/> 720 Labor/Management Relations <input type="checkbox"/> 740 Railway Labor Act <input type="checkbox"/> 751 Family and Medical Leave Act <input type="checkbox"/> 790 Other Labor Litigation <input type="checkbox"/> 791 Employee Retirement Income Security Act IMMIGRATION <input type="checkbox"/> 462 Naturalization Application <input type="checkbox"/> 465 Other Immigration Actions	<input type="checkbox"/> 422 Appeal 28 USC 158 <input type="checkbox"/> 423 Withdrawal 28 USC 157 INTELLECTUAL PROPERTY RIGHTS <input type="checkbox"/> 820 Copyrights <input type="checkbox"/> 830 Patent <input type="checkbox"/> 835 Patent - Abbreviated New Drug Application <input type="checkbox"/> 840 Trademark <input type="checkbox"/> 880 Defend Trade Secrets Act of 2016 SOCIAL SECURITY <input type="checkbox"/> 861 HIA (1395ff) <input type="checkbox"/> 862 Black Lung (923) <input type="checkbox"/> 863 DIWC/DIWW (405(g)) <input type="checkbox"/> 864 SSID Title XVI <input type="checkbox"/> 865 RSI (405(g)) FEDERAL TAX SUITS <input type="checkbox"/> 870 Taxes (U.S. Plaintiff or Defendant) <input type="checkbox"/> 871 IRS—Third Party 26 USC 7609	<input type="checkbox"/> 375 False Claims Act <input type="checkbox"/> 376 Qui Tam (31 USC 3729(a)) <input type="checkbox"/> 400 State Reapportionment <input type="checkbox"/> 410 Antitrust <input type="checkbox"/> 430 Banks and Banking <input type="checkbox"/> 450 Commerce <input type="checkbox"/> 460 Deportation <input type="checkbox"/> 470 Racketeer Influenced and Corrupt Organizations <input type="checkbox"/> 480 Consumer Credit (15 USC 1681 or 1692) <input type="checkbox"/> 485 Telephone Consumer Protection Act <input type="checkbox"/> 490 Cable/Sat TV <input type="checkbox"/> 850 Securities/Commodities/Exchange <input type="checkbox"/> 890 Other Statutory Actions <input type="checkbox"/> 891 Agricultural Acts <input type="checkbox"/> 893 Environmental Matters <input type="checkbox"/> 895 Freedom of Information Act <input type="checkbox"/> 896 Arbitration <input type="checkbox"/> 899 Administrative Procedure Act/Review or Appeal of Agency Decision <input type="checkbox"/> 950 Constitutionality of State Statutes
REAL PROPERTY <input type="checkbox"/> 210 Land Condemnation <input type="checkbox"/> 220 Foreclosure <input type="checkbox"/> 230 Rent Lease & Ejectment <input type="checkbox"/> 240 Torts to Land <input type="checkbox"/> 245 Tort Product Liability <input type="checkbox"/> 290 All Other Real Property	CIVIL RIGHTS <input type="checkbox"/> 440 Other Civil Rights <input type="checkbox"/> 441 Voting <input type="checkbox"/> 442 Employment <input type="checkbox"/> 443 Housing/Accommodations <input type="checkbox"/> 445 Amer. w/Disabilities - Employment <input type="checkbox"/> 446 Amer. w/Disabilities - Other <input type="checkbox"/> 448 Education	PRISONER PETITIONS Habeas Corpus: <input type="checkbox"/> 463 Alien Detainee <input type="checkbox"/> 510 Motions to Vacate Sentence <input type="checkbox"/> 530 General <input type="checkbox"/> 535 Death Penalty Other: <input type="checkbox"/> 540 Mandamus & Other <input type="checkbox"/> 550 Civil Rights <input type="checkbox"/> 555 Prison Condition <input type="checkbox"/> 560 Civil Detainee - Conditions of Confinement			

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

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

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing (Do not cite jurisdictional statutes unless diversity):

Brief description of cause:

VII. REQUESTED IN COMPLAINT:

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

DEMAND \$

CHECK YES only if demanded in complaint:

JURY DEMAND: ☐ Yes ☐ No

VIII. RELATED CASE(S) IF ANY

(See instructions):

JUDGE

DOCKET NUMBER

DATE

SIGNATURE OF ATTORNEY OF RECORD

FOR OFFICE USE ONLY

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

INSTRUCTIONS FOR ATTORNEYS COMPLETING CIVIL COVER SHEET FORM JS 44

Authority For Civil Cover Sheet

The JS 44 civil cover sheet and the information contained herein neither replaces nor supplements the filings and service of pleading or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. Consequently, a civil cover sheet is submitted to the Clerk of Court for each civil complaint filed. The attorney filing a case should complete the form as follows:

- I.(a) Plaintiffs-Defendants.** Enter names (last, first, middle initial) of plaintiff and defendant. If the plaintiff or defendant is a government agency, use only the full name or standard abbreviations. If the plaintiff or defendant is an official within a government agency, identify first the agency and then the official, giving both name and title.
 - (b) County of Residence.** For each civil case filed, except U.S. plaintiff cases, enter the name of the county where the first listed plaintiff resides at the time of filing. In U.S. plaintiff cases, enter the name of the county in which the first listed defendant resides at the time of filing. (NOTE: In land condemnation cases, the county of residence of the "defendant" is the location of the tract of land involved.)
 - (c) Attorneys.** Enter the firm name, address, telephone number, and attorney of record. If there are several attorneys, list them on an attachment, noting in this section "(see attachment)".
- II. Jurisdiction.** The basis of jurisdiction is set forth under Rule 8(a), F.R.Cv.P., which requires that jurisdictions be shown in pleadings. Place an "X" in one of the boxes. If there is more than one basis of jurisdiction, precedence is given in the order shown below.
- United States plaintiff. (1) Jurisdiction based on 28 U.S.C. 1345 and 1348. Suits by agencies and officers of the United States are included here. United States defendant. (2) When the plaintiff is suing the United States, its officers or agencies, place an "X" in this box.
- Federal question. (3) This refers to suits under 28 U.S.C. 1331, where jurisdiction arises under the Constitution of the United States, an amendment to the Constitution, an act of Congress or a treaty of the United States. In cases where the U.S. is a party, the U.S. plaintiff or defendant code takes precedence, and box 1 or 2 should be marked.
- Diversity of citizenship. (4) This refers to suits under 28 U.S.C. 1332, where parties are citizens of different states. When Box 4 is checked, the citizenship of the different parties must be checked. (See Section III below; **NOTE: federal question actions take precedence over diversity cases.**)
- III. Residence (citizenship) of Principal Parties.** This section of the JS 44 is to be completed if diversity of citizenship was indicated above. Mark this section for each principal party.
- IV. Nature of Suit.** Place an "X" in the appropriate box. If there are multiple nature of suit codes associated with the case, pick the nature of suit code that is most applicable. Click here for: [Nature of Suit Code Descriptions](#).
- V. Origin.** Place an "X" in one of the seven boxes.
- Original Proceedings. (1) Cases which originate in the United States district courts.
- Removed from State Court. (2) Proceedings initiated in state courts may be removed to the district courts under Title 28 U.S.C., Section 1441.
- Remanded from Appellate Court. (3) Check this box for cases remanded to the district court for further action. Use the date of remand as the filing date.
- Reinstated or Reopened. (4) Check this box for cases reinstated or reopened in the district court. Use the reopening date as the filing date.
- Transferred from Another District. (5) For cases transferred under Title 28 U.S.C. Section 1404(a). Do not use this for within district transfers or multidistrict litigation transfers.
- Multidistrict Litigation – Transfer. (6) Check this box when a multidistrict case is transferred into the district under authority of Title 28 U.S.C. Section 1407.
- Multidistrict Litigation – Direct File. (8) Check this box when a multidistrict case is filed in the same district as the Master MDL docket.
- PLEASE NOTE THAT THERE IS NOT AN ORIGIN CODE 7.** Origin Code 7 was used for historical records and is no longer relevant due to changes in statute.
- VI. Cause of Action.** Report the civil statute directly related to the cause of action and give a brief description of the cause. **Do not cite jurisdictional statutes unless diversity.** Example: U.S. Civil Statute: 47 USC 553 Brief Description: Unauthorized reception of cable service.
- VII. Requested in Complaint.** Class Action. Place an "X" in this box if you are filing a class action under Rule 23, F.R.Cv.P.
- Demand. In this space enter the actual dollar amount being demanded or indicate other demand, such as a preliminary injunction.
- Jury Demand. Check the appropriate box to indicate whether or not a jury is being demanded.
- VIII. Related Cases.** This section of the JS 44 is used to reference related pending cases, if any. If there are related pending cases, insert the docket numbers and the corresponding judge names for such cases.

Date and Attorney Signature. Date and sign the civil cover sheet.

AO 440 (Rev. 12/09) Summons in a Civil Action

UNITED STATES DISTRICT COURT

for the

_____ District of _____

Plaintiff

v.

Defendant

)
)
)
)
)
)
)

Civil Action No. _____

SUMMONS IN A CIVIL ACTION

To: *(Defendant's name and address)*

A lawsuit has been filed against you.

Within 21 days after service of this summons on you (not counting the day you received it) — or 60 days if you are the United States or a United States agency, or an officer or employee of the United States described in Fed. R. Civ. P. 12 (a)(2) or (3) — you must serve on the plaintiff an answer to the attached complaint or a motion under Rule 12 of the Federal Rules of Civil Procedure. The answer or motion must be served on the plaintiff or plaintiff's attorney, whose name and address are:

If you fail to respond, judgment by default will be entered against you for the relief demanded in the complaint. You also must file your answer or motion with the court.

CLERK OF COURT

Date: _____

Signature of Clerk or Deputy Clerk