UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS

JOHN W. MILES, individually and on behalf of all others similarly situated, Plaintiff, v. ANDY FRAIN SERVICES, INC., Defendant.	Case No. 25-cv-05706 CLASS ACTION JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiff John W. Miles ("Plaintiff"), individually, and on behalf of all others similarly situated (collectively, "Class members"), by and through his attorneys, brings this Class Action Complaint against Defendant Andy Frain Services, Inc. ("Andy Frain" or "Defendant"), and complains and alleges upon personal knowledge as to himself and information and belief as to all other matters.

INTRODUCTION

1. Plaintiff brings this class action against Andy Frain for its failure to secure and safeguard approximately 100,964 individuals' (including Plaintiff's) personally identifying information ("PII"), including names and Social Security numbers.

2. Andy Frain is a security company based in Aurora, Illinois, with offices across the country.

3. On or about October 23, 2024, Andy Frain detected that an unauthorized third party had gained access to Andy Frain's network systems and obtained files containing the PII of Andy Frain's current and former employees, including Plaintiff (the "Data Breach").

4. Andy Frain owed a duty to Plaintiff and Class members to implement and maintain reasonable and adequate security measures to secure, protect, and safeguard their PII against unauthorized access and disclosure. Andy Frain breached that duty by, among other things, failing to implement and maintain reasonable security procedures and practices to protect its current and former employees' PII from unauthorized access and disclosure.

5. As a result of Andy Frain's inadequate security and breach of its duties and obligations, the Data Breach occurred, and Plaintiff's and Class members' PII was accessed and disclosed. This action seeks to remedy these failings and their consequences. Plaintiff brings this action on behalf of himself and all persons whose PII was exposed as a result of the Data Breach, which Andy Frain detected on or about October 23, 2024.

6. Plaintiff, on behalf of himself and all other Class members, asserts claims for negligence, negligence per se, breach of implied contract, 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 John W. Miles

7. Plaintiff John W. Miles is a citizen of Alabama.

8. Plaintiff is a former employee of Andy Frain. As a condition of providing employment to Plaintiff, Andy Frain required Plaintiff to provide it with his PII.

9. Plaintiff believed Andy Frain had implemented and maintained reasonable security and practices to protect his PII. With this belief in mind, Plaintiff provided his PII to Andy Frain in connection with obtaining employment from Andy Frain.

10. At all relevant times, Andy Frain stored and maintained Plaintiff's PII on its network systems, including the systems accessed in the Data Breach.

11. Had Plaintiff known that Andy Frain does not adequately protect the PII in its possession, he would not have obtained employment from Andy Frain or agreed to entrust it with his PII.

12. 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; the wrongful disclosure and loss of confidentiality of his highly sensitive PII; and deprivation of the value of his PII.

Defendant Andy Frain Services, Inc.

13. Defendant Andy Frain Services, Inc. is an Illinois corporation with its principal place of business located at 761 Shoreline Drive, Aurora, IL 60504. It may be served through its registered agent: Mark A. Costa, 225 W. Washington St., Suite 1300, Chicago, IL 60606.

JURISDICTION AND VENUE

14. 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 amount in controversy exceeds $5,000,000, exclusive of interest and costs.

15. This Court has general personal jurisdiction over Andy Frain because it maintains its principal place of business in this District.

16. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because Andy Frain'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 Andy Frain and the Data Breach

17. Andy Frain is a security company that was founded in 1924.[1] The company provides security guards for several sectors, including retail, sporting events, and transportation.[2]

18. In the regular course of its business, Andy Frain collects and maintains the PII of its employees, including Plaintiff and Class members.

19. Andy Frain's website contains a Privacy Notice that applies to people who use the website, use Andy Frain's services, and use its employment application system.[3] Andy Frain's website claims that it will not share sensitive information, including Social Security numbers, "with third parties except as necessary for human resources administration."[4]

20. On or about October 23, 2024, Andy Frain detected an unauthorized third party in its computer network. Thereafter, the company determined that human resources files were affected in the Data Breach, including files containing the PII of Plaintiff and Class members. Andy Frain determined that at least names and Social Security numbers were affected in the Data Breach.

21. The Black Basta Ransomware group claimed responsibility for the Data Breach.[5] Black Basta claimed to have stolen 750 GB of data from Andy Frain, "including ones related to

---

[1] *About Us*, ANDY FRAIN SERVICES, INC., http://www.andyfrain.com/about.cfm (last accessed May 21, 2025).
[2] *Services*, ANDY FRAIN SERVICES, INC., http://www.andyfrain.com/services.cfm (last accessed May 21, 2025).
[3] *Privacy Notice*, ANDY FRAIN SERVICES, INC., http://www.andyfrain.com/privacy-policy.cfm (last accessed May 21, 2025).
[4] *Id.*
[5] Eduard Kovacs, *Security Firm Andy Frain Says 100,000 People Impacted by Ransomware Attack*, SECURITYWEEK (May 12, 2025, 10:11 AM ET), https://www.securityweek.com/security-firm-andy-frain-says-100000-people-impacted-by-ransomware-attack/.

accounting, HR, and legal departments."[6] The Black Basta Ransomware group is a known threat actor that has been recognized by the U.S. Cybersecurity & Infrastructure Security Agency.[7] As of May 2024, the group had "impacted over 500 organizations globally."[8] Plaintiff's and Class members' PII is in the hands of notorious cybercriminals and Plaintiff and Class members are at imminent risk of harm, in addition to the harm they have already experienced.

22. While Andy Frain learned of the Data Breach on or about October 23, 2024, it waited until approximately April 30, 2025, approximately six months later, to begin notifying its current and former employees that the Data Breach occurred and that their PII was in the hands of cybercriminals.

23. Andy Frain's failure to promptly notify Plaintiff and Class members that their PII was accessed and stolen virtually ensured that the unauthorized third parties who exploited those security lapses could monetize, misuse, or disseminate that PII 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.

Andy Frain Knew that Criminals Target PII

24. At all relevant times, Andy Frain knew, or should have known, that the PII that it collected and stored was a target for malicious actors. Despite such knowledge, Andy Frain failed to implement and maintain reasonable and appropriate data privacy and security measures to

[6] *Id.*
[7] *#StopRansomware: Black Basta*, CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY (Nov. 8, 2024), https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-131a.
[8] *Id.*

protect Plaintiff's and Class members' PII from 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 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."[9]

26. PII is a valuable property right.[10] The value of PII as a commodity is measurable.[11] "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."[12] American companies are estimated to have spent over $19 billion on acquiring personal data of consumers in 2018.[13] 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.

---

[9] 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, 8:05 AM), https://www.businessinsider.com/data-breaches-retailers-consumer-companies-2019-1.

[10] *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.

[11] *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.

[12] 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.

[13] 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/.

27. 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, 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.

28. 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."[14]

Theft of PII Has Grave and Lasting Consequences for Victims

29. Theft of PII can have serious consequences for the victim. The FTC warns consumers that identity thieves use PII to receive medical treatment, start new utility accounts, and incur charges and credit in a person's name.[15] [16]

[14] 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.

[15] *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 May 21, 2025).

[16] 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).

30. 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.[17]

31. Identity theft is not an easy problem to solve. In a survey, the Identity Theft Resource Center found that almost 20% of victims of identity misuse needed more than a month to resolve issues stemming from identity theft.[18]

32. 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.[19]

33. It is within this context that Plaintiff and all other Class members must now live with the knowledge that their PII 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.

---

[17] *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/.

[18] Identity Theft Resource Center, *2023 Consumer Aftermath Report*, IDENTITY THEFT RES. CTR. (2023), https://www.idtheftcenter.org/publication/2023-consumer-impact-report/ (last accessed May 21, 2025).

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

Damages Sustained by Plaintiff and Class Members

34. 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 compromise, publication, and theft of their PII; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII; (iv) lost opportunity costs associated with efforts attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII 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 compromised as a result of the Data Breach.

CLASS ALLEGATIONS

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

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

> All persons whose personally identifiable information was accessed in the Data Breach by an unauthorized third party, including all who were sent a notice of the Data Breach.

37. Excluded from the Class are Andy Frain Services, Inc., and its affiliates, parents, subsidiaries, officers, agents, and directors, as well as the judge(s) presiding over this matter and the clerks of said judge.

38. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of his 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.

39. The members in the Class are so numerous that joinder of each of the Class members in a single proceeding would be impracticable. Andy Frain has reported to the Office of the Maine Attorney General that the Data Breach affected approximately 100,964 persons.[20]

40. 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*:

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 from unauthorized access and disclosure;

b. Whether Defendant had a duty not to disclose the PII 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;

d. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII of Plaintiff and Class members;

e. Whether Defendant breached its duties to protect Plaintiff's and Class members' PII; and

f. Whether Plaintiff and Class members are entitled to damages and the measure of such damages and relief.

41. Defendant engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiff, on behalf of himself 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.

[20] *Data Breach Notifications*, OFFICE OF THE MAINE ATTORNEY GENERAL, https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/a767f210-0989-43f8-9ceb-8bc018ce2b8c.html (last accessed May 21, 2025).

42. Plaintiff's claims are typical of the claims of the Class. Plaintiff, like all proposed members of the Class, had his PII compromised in the Data Breach. Plaintiff and Class members were injured by the same wrongful acts, practices, and omissions committed by Defendant, 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.

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

44. 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 Defendant, so it would be impracticable for Class members to individually seek redress from Defendant'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

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

46. Andy Frain owed a duty to Plaintiff and Class members to exercise reasonable care in safeguarding and protecting the PII in its possession, custody, or control.

47. Andy Frain knew or should have known the risks of collecting, storing, and maintaining Plaintiff's and all other Class members' PII and the importance of maintaining secure systems and procedures. Andy Frain knew or should have known of the many data breaches that targeted companies that collect and store PII in recent years.

48. Given the nature of Andy Frain's business, the sensitivity and value of the PII it collects and maintains, and the resources at its disposal, Andy Frain should have identified the vulnerabilities to its systems and prevented the Data Breach from occurring.

49. Andy Frain breached these duties by failing to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII 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 entrusted to it—including Plaintiff's and Class members' PII.

50. It was reasonably foreseeable to Andy Frain that its failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII 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 to unauthorized individuals.

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

52. As a result of Andy Frain'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; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII; (iv) lost opportunity costs associated with effort attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII which remains in Andy Frain'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 compromised as a result of the Data Breach.

COUNT II
NEGLIGENCE PER SE

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

54. Andy Frain'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 Andy Frain, of failing to employ reasonable measures to protect and secure PII.

55. Andy Frain violated Section 5 of the FTCA by failing to use reasonable measures to protect Plaintiff's and other Class members' PII, by failing to provide timely

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

56. Andy Frain's violation of Section 5 of the FTCA constitutes negligence per se.

57. Plaintiff and Class members are within the class of persons that Section 5 of the FTCA were intended to protect.

58. The harm occurring as a result of the Data Breach is the type of harm that 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.

59. It was, or should have been, reasonably foreseeable to Andy Frain that its failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII 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 to unauthorized individuals.

60. The injury and harm that Plaintiff and the other Class members suffered was the direct and proximate result of Andy Frain's violations of Section 5 of the FTCA.

61. Plaintiff and Class members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, *inter alia*: (i) a substantially increased and imminent risk of identity theft—risks justifying expenditures for

protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII; (iii) breach of the confidentiality of their PII; (iv) deprivation of the value of their PII, for which there is a well-established national and international market; and (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of identity theft they face and will continue to face.

COUNT III
BREACH OF IMPLIED CONTRACT

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

63. In connection with receiving employment, Plaintiff and all other Class members entered into implied contracts with Andy Frain.

64. Pursuant to these implied contracts, Plaintiff and Class members provided the labor and service to Andy Frain, and provided Andy Frain with their PII. In exchange, Andy Frain agreed to, among other things, and Plaintiff and Class members understood that Andy Frain would: (1) pay and provide benefits to Plaintiff and Class members for their labor and services; (2) use the PII provided to it to facilitate Plaintiff and Class members' employment and payment; (3) take reasonable measures to protect the security and confidentiality of Plaintiff's and Class members' PII; and (4) protect Plaintiff's and Class members' PII in compliance with federal and state laws and regulations and industry standards.

65. The protection of PII was a material term of the implied contracts between Plaintiff and Class members, on the one hand, and Andy Frain, on the other hand. Indeed, as set forth above, Andy Frain recognized the importance of data security and the privacy of its employees' PII in its Privacy Notice. Had Plaintiff and Class members known that Andy Frain

would not adequately protect their PII, they would not have sought employment from Andy Frain or agreed to provide it with their PII.

66. Plaintiff and Class members performed their obligations under the implied contract when they provided Andy Frain with their PII and labor.

67. Andy Frain breached its obligations under its implied contracts with Plaintiff and Class members by failing to implement and maintain reasonable security measures to protect and secure their PII and failing to implement and maintain security protocols and procedures to protect Plaintiff's and Class members' PII in a manner that complies with applicable laws, regulations, and industry standards.

68. Andy Frain's breach of its obligations of its implied contracts with Plaintiff and Class members directly resulted in the Data Breach and the injuries that Plaintiff and all other Class members have suffered from the Data Breach.

69. Plaintiff and all other Class members were damaged by Andy Frain's breach of implied contracts because: (i) they provided their labor and PII in exchange for payment and benefits including data security protection they did not receive; (ii) they face a substantially increased risk of identity theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (iii) their PII was improperly disclosed to unauthorized individuals; (iv) the confidentiality of their PII has been breached; (v) they were deprived of the value of their PII, for which there is a well-established national and international market; and (vi) they lost time and incurred money to mitigate and remediate the effects of the Data Breach, including the increased risks of identity theft they face and will continue to face.

COUNT IV
UNJUST ENRICHMENT

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

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

72. Plaintiff and Class members conferred a monetary benefit upon Andy Frain in the form of labor which enabled Andy Frain to run its business and through the provision of their PII.

73. Andy Frain accepted or had knowledge of the benefits conferred upon it by Plaintiff and Class members. Andy Frain benefitted from the receipt of Plaintiff's and Class members' PII, as this was necessary to facilitate Andy Frain's business and provision of services.

74. As a result of Andy Frain's conduct, Andy Frain's current and former employees suffered actual damages in an amount equal to the difference in value between labor provided with reasonable data privacy and security practices and procedures, and the value of payments for labor provided Andy Frain's current and former employees actually received without reasonable data privacy and security practices and procedures.

75. Andy Frain should not be permitted to retain the money belonging to Plaintiff and Class members because Andy Frain 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.

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

77. Andy Frain 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 his 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 himself and the Class, seek appropriate injunctive relief designed to prevent Defendant from experiencing another data breach by adopting and implementing best data security practices to safeguard PII 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: May 21, 2025 Respectfully submitted,

/s/ Ben Barnow
Ben Barnow (IL Bar No. 0118265)
Anthony L. Parkhill (IL Bar No. 6317680)
Riley W. Prince (IL Bar No. 6339536)
Nicholas W. Blue (IL Bar No. 6343317)
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
rprince@barnowlaw.com
nblue@barnowlaw.com

Attorneys for Plaintiff