EXHIBIT A

SUPREME COURT OF THE STATE OF NEW YORK
COUNTY OF WESTCHESTER

SALVATORE J. CONTRISTANO, individually, and on behalf of all others similarly situated, Plaintiff, v. EMPRESS AMBULANCE SERVICE, LLC, Defendant.	Case No. CLASS ACTION JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiff Salvatore J. Contristano ("Plaintiff"), individually, and on behalf of all others similarly situated (collectively, "Class members"), by and through his attorneys, brings this Class Action Complaint against Empress Ambulance Service, LLC ("Empress") 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 Empress for its failure to secure and safeguard his and approximately 318,558 other individuals' personally identifying information ("PII") and personal health information ("PHI"), including names, dates of service, insurance information, and in some instances, Social Security numbers.

2. Empress is a company that provides emergency medical services with its principal place of business in Yonkers, New York. Empress provides emergency medical response for the cities of Yonkers, New Rochelle, Yorktown, Pelham, Poughkeepsie, Mount Vernon, White Plains, and the Bronx. Empress is a limited liability company formed in Delaware.

3. Between May 26, 2022 and July 13, 2022, unauthorized individuals gained access to Empress' network systems and accessed and acquired files from the system that contained the PII/PHI of Plaintiff and Class members (the "Data Breach").

4. Empress 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. Empress breached that duty by, among other things, failing to implement and maintain reasonable security procedures and practices to protect its patients' and former patients' PII/PHI from unauthorized access and disclosure.

5. As a result of Empress' 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 himself and all persons whose PII/PHI was exposed as a result of the Data Breach, which Empress first publicly acknowledged on or about September 9, 2022, almost two months after the breach occurred.

6. Plaintiff, on behalf of himself and all other Class members, asserts claims for negligence, negligence per se, breach of fiduciary duty, breach of express contract, breach of implied contract, unjust enrichment, and violations of New York General Business Law § 349, and seeks declaratory relief, injunctive relief, monetary damages, statutory damages, punitive damages, equitable relief, and all other relief authorized by law.

PARTIES

7. Plaintiff Salvatore J. Contristano is a New York resident. Plaintiff Contristano received services from Empress. He received a letter from Empress notifying him that his PII/PHI

was exposed in the Data Breach. Plaintiff Contristano would not have accepted services from Empress had he known that his PII/PHI would not be adequately safeguarded by Empress.

8. Defendant Empress Ambulance Service, LLC is a limited liability company formed in Delaware. Empress' principal place of business is located at 722 Nepperhan Ave., Yonkers, New York 10703.

JURISDICTION AND VENUE

9. This Court has personal jurisdiction over Empress because Empress has its principal place of business in New York.

10. Venue is proper in Westchester County because Empress' principal place of business is located in Westchester County.

FACTUAL ALLEGATIONS

Overview of Empress

11. Empress provides emergency medical services, including emergency response, community paramedicine, and basic and advanced life support.[1] The company claims to have over 700 personnel.[2]

12. In the regular course of its business, Empress collects and maintains the PII/PHI of its patients.

13. On its website, Empress has a Privacy Practices Statement. The Privacy Practices Statement states that the company is "committed to protecting your personal health information"

[1] *Empress EMS Services*, EMPRESS EMS, https://empressems.com/services/ (last accessed Sep. 26, 2022).
[2] *About Empress EMS*, EMPRESS EMS, https://empressems.com/about/ (last accessed Sep. 26, 2022).

and that it is "required by law to maintain the privacy of health information."[3] The statement goes on to state, "We respect your privacy, and treat all healthcare information about our patients with care under strict policies of confidentiality that our staff is committed to following at all times."[4]

14. Plaintiff and Class members are, or were patients of Empress and entrusted Empress with their PII/PHI.

The Data Breach

15. Between May 26, 2022 and July 13, 2022, an unauthorized individual, or unauthorized individuals, gained access to Empress' network systems and accessed and acquired certain files on Empress' computer systems.

16. Empress did not begin to notify government agencies or the public about the data breach until almost two months after the breach, on or about September 9, 2022. The notice that Empress posted to its website states that the information that the cybercriminal extracted from Empress' network includes "names, dates of service, insurance information, and in some instances, Social Security numbers."[5]

17. Empress' notice stated that it discovered the Data Breach on July 14, 2022.[6] Despite this, Empress waited almost two months to tell its patients that the breach occurred.

Empress Knew that Criminals Target PII/PHI

18. At all relevant times, Empress knew, or should have known, that the PII/PHI that it collected was a target for malicious actors. Despite such knowledge, Empress failed to implement

[3] *Privacy Practices Statement*, EMPRESS EMS, https://empressems.com/wp-content/uploads/2022/07/empressprivacy.pdf (last accessed Sep. 26, 2022).
[4] *Id.*
[5] *Notice of Security Incident*, EMPRESS EMS, https://empressems.com/notice-of-security-incident/ (last accessed Sep. 26, 2022).
[6] *Id.*

and maintain reasonable and appropriate data privacy and security measures to protect Plaintiff's and Class members' PII/PHI from cyber-attacks that Empress should have anticipated and guarded against.

19. It is well known amongst companies that store sensitive personally identifying information that sensitive information—such as the Social Security numbers ("SSNs") and medical information 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."[7]

20. Cyber criminals seek out PHI at a greater rate than other sources of personal information. In a 2022 report, the healthcare compliance company Protenus found that there were 905 medical data breaches in 2021 with over 50 million patient records exposed.[8] This is an increase from the 758 medical data breaches which exposed approximately 40 million records that Protenus compiled in 2020.[9]

21. PII/PHI is a valuable property right.[10] The value of PII/PHI as a commodity is measurable.[11] "Firms are now able to attain significant market valuations by employing business

---

[7] Dennis Green, Mary Hanbury & Aine Cain, *If you bought anything from these 19 companies recently, your data may have been stolen*, BUSINESS INSIDER (Nov. 19, 2019, 8:05 A.M.), https://www.businessinsider.com/data-breaches-retailers-consumer-companies-2019-1.

[8] PROTENUS, *2022 Breach Barometer*, PROTENUS.COM, https://www.protenus.com/breach-barometer-report (last accessed Sep. 26, 2022).

[9] *Id.*

[10] *See* Marc van Lieshout, *The Value of Personal Data*, 457 International Federation for Information 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.COM (April 28, 2014), http://www.medscape.com/viewarticle/824192.

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/PHI has been disclosed, criminals often trade it on the "cyber black-market," or the "dark web," for many years.

22. As a result of their real and significant value, identity thieves and other cyber criminals have openly posted credit card numbers, SSNs, 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 and become more valuable to thieves and more damaging to victims.

23. PHI is particularly valuable and has been referred to as a "treasure trove for criminals."[14] A cybercriminal who steals a person's PHI can end up with as many as "seven to ten personal identifying characteristics of an individual."[15] A study by Experian found that the "average total cost" of medical identity theft is "about $20,000" per incident, and that a majority

[12] OECD, *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD iLIBRARY (April 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*, IAB.COM (Dec. 5, 2018), https://www.iab.com/news/2018-state-of-data-report/.
[14] *See* Andrew Steager, *What Happens to Stolen Healthcare Data*, HEALTHTECH MAGAZINE (Oct. 20, 2019), https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon ("*What Happens to Stolen Healthcare Data* Article") (quoting Tom Kellermann, Chief Cybersecurity Officer, Carbon Black, stating "Health information is a treasure trove for criminals.").
[15] *Id.*

of victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[16]

24. All-inclusive health insurance dossiers containing sensitive health insurance information, names, addresses, telephone numbers, email addresses, SSNs, and bank account information, complete with account and routing numbers, can fetch up to $1,200 to $1,300 each on the black market.[17] 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.[18]

25. Criminals can use stolen PII/PHI to extort a financial payment by "leveraging details specific to a disease or terminal illness."[19] Quoting Carbon Black's Chief Cybersecurity Officer, one recent article explained: "Traditional criminals understand the power of coercion and extortion . . . By having healthcare information—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."[20]

26. Consumers place a high value on the privacy of that 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

---

[16] *See* Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (Mar. 3, 2010), https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims.
[17] SC Staff, *Health Insurance Credentials Fetch High Prices in the Online Black Market*, SC MAGAZINE (July 16, 2013), https://www.scmagazine.com/news/breach/health-insurance-credentials-fetch-high-prices-in-the-online-black-market.
[18] Federal Bureau of Investigation, *Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain* (April 8, 2014), https://www.illuminweb.com/wp-content/uploads/ill-mo-uploads/103/2418/health-systems-cyber-intrusions.pdf.
[19] *See* Andrew Steager, *What Happens to Stolen Healthcare Data*, *supra* at n.14.
[20] *Id.*

accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[21]

27. 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

28. Theft of PII/PHI is serious. 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.[22]

29. Identity thieves use personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[23] According to Experian, one of the largest credit reporting companies in the world, "[t]he research shows that personal information is valuable to identity thieves, and if they can get access to it, they will use it" to among other things: open a new credit card or loan; change a billing address so the victim no longer receives bills; open new utilities; obtain a mobile phone; open a bank account and write bad checks; use a

[21] Janice Y. Tsai et al., *The Effect of Online Privacy Information on Purchasing Behavior, An Experimental Study*, 22(2) INFORMATION SYSTEMS RESEARCH 254 (June 2011) https://www.jstor.org/stable/23015560?seq=1.

[22] *See* Federal Trade Commission, *What to Know About Identity Theft*, FEDERAL TRADE COMMISSION CONSUMER INFORMATION, https://www.consumer.ftc.gov/articles/what-know-about-identity-theft (last accessed Sep. 26, 2022).

[23] 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. 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. *Id*.

debit card number to withdraw funds; obtain a new driver's license or ID; use the victim's information in the event of arrest or court action.[24]

30. With access to an individual's PII, criminals can do more than just empty a victim's bank account—they can also commit all manner of fraud, including: opening utility accounts using the victim's identity; file a fraudulent tax return using the victim's information; or even give the victim's personal information to police during an arrest.[25]

31. Identity theft is not an easy problem to solve. In a survey, the Identity Theft Resource Center found that most victims of identity crimes need more than a month to resolve issues stemming from identity theft and some need over a year.[26]

32. 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."[27] It "is also more difficult to detect, taking almost twice as long as normal identity theft."[28] 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 devices, submit claims with your insurance provider, or get other

[24] *See* Susan Henson, *What Can Identity Thieves Do with Your Personal Information and How Can You Protect Yourself*, EXPERIAN, https://www.experian.com/blogs/ask-experian/what-can-identity-thieves-do-with-your-personal-information-and-how-can-you-protect-yourself/ (last accessed Sep. 26, 2022).
[25] *See* Federal Trade Commission, *Warning Signs of Identity Theft*, IDENTITYTHEFT.GOV https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft (last accessed Sep. 26, 2022).
[26] Identity Theft Resource Center, *2021 Consumer Aftermath Report*, IDENTITY THEFT RESOURCE CENTER (2021), https://www.idtheftcenter.org/identity-theft-aftermath-study/ (last accessed Sep. 26, 2022).
[27] Pam Dixon and John Emerson, *The Geography of Medical Identity Theft*, FTC.GOV (Dec. 12, 2017), https://www.ftc.gov/system/files/documents/public_comments/2018/01/00037-142815.pdf.
[28] *See* Federal Bureau of Investigation, *Health Care Systems and Medical Devices at Risk…*, *supra* at n.18.

medical care." [29] 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. It could also hurt your credit."[30]

33. 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:

- 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.
- Significant bills for medical goods and services not sought nor received.
- Issues with insurance, co-pays, and insurance caps.
- Long-term credit problems based on problems with debt collectors reporting debt due to identity theft.
- 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.
- 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.
- Phantom medical debt collection based on medical billing or other identity information.
- Sales of medical debt arising from identity theft can perpetuate a victim's debt collection and credit problems, through no fault of their own.[31]

[29] *See* Federal Trade Commission, *What to Know About Medical Identity Theft*, Federal Trade Commission Consumer Information, https://www.consumer.ftc.gov/articles/what-know-about-medical-identity-theft (last accessed Sep. 26, 2022).
[30] *Id.*
[31] *See* Pam Dixon and John Emerson, *The Geography of Medical Identity Theft*, *supra* at 27.

34. There may also be a time lag between when sensitive personal information is stolen, when it is used, and when a person discovers it has been used. For example, 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.[32]

35. It is within this context that Plaintiff and Class members must now live with the knowledge that their PII/PHI is forever in cyberspace and was taken by people willing to use the 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 the Other Class Members

36. 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 effort attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII/PHI which remains in Empress' possession; (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; and (vii) overpayment for the services that were received without adequate data security.

CLASS ALLEGATIONS

37. This action is brought and may be properly maintained as a class action pursuant to N.Y. C.P.L.R. §§ 901, *et seq*.

[32] John W. Coffey, *Difficulties in Determining Data Breach Impacts*, 17 Journal of Systemics, Cybernetics and Informatics 9 (2019), http://www.iiisci.org/journal/pdv/sci/pdfs/IP069LL19.pdf.

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

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

39. Excluded from the Class is Empress Ambulance Service, LLC 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(s).

40. 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.

41. The members in the Class are so numerous that joinder of each of the Class members in a single proceeding would be impracticable. Empress reported to the United States Department of Health and Human Services Office of Civil Rights that approximately 318,558 persons' information was exposed in the Data Breach.

42. 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 Empress 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 Empress failed to exercise reasonable care to secure and safeguard Plaintiff's and Class members' PII/PHI;

c. Whether an implied contract existed between Class members and Empress, providing that Empress would implement and maintain reasonable security

measures to protect and secure Class members' PII/PHI from unauthorized access and disclosure;

d. Whether Empress 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.

43. Empress 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.

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

45. 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.

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

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

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

49. Empress knew the risks of collecting and storing Plaintiff's and all other Class members' PII/PHI and the importance of maintaining secure systems. Empress knew of the many data breaches that targeted companies that stored PII/PHI in recent years.

50. Given the nature of Empress' business, the sensitivity and value of the PII/PHI it maintains, and the resources at its disposal, Empress should have identified the vulnerabilities to their systems and prevented the Data Breach from occurring.

51. Empress 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.

52. It was reasonably foreseeable to Empress 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.

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

54. As a result of Empress' 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 effort attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII/PHI which remains in Empress' possession; (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; and (vii) overpayment for the services that were received without adequate data security.

COUNT II
NEGLIGENCE PER SE

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

56. Empress' 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").

57. Empress' 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 businesses, such as Empress, of failing to employ reasonable measures to protect and secure PII/PHI.

58. Empress 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 and not complying with applicable industry standards. Empress' 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.

59. Empress' violation of HIPAA Privacy and Security Rules and Section 5 of the FTCA constitutes negligence per se.

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

61. The harm occurring as a result of the Data Breach is the type of harm 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 Brach.

62. It was reasonably foreseeable to Empress 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.

63. The injury and harm that Plaintiff and the other Class members suffered was the direct and proximate result of Empress' violations of harm 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 effort attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII/PHI which remains in Empress' possession; (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; and (vii) overpayment for the services that were received without adequate data security.

COUNT III
BREACH OF FIDUCIARY DUTY

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

65. Plaintiff and Class members gave Empress their PII/PHI in confidence, believing that Empress would protect that information. Plaintiff and Class members would not have provided Empress with this information had they known it would not be adequately protected. Empress' acceptance and storage of Plaintiff's and Class members' PII/PHI created a fiduciary relationship between Empress and Plaintiff and Class members. In light of this relationship, Empress must act primarily for the benefit of its patients, which includes safeguarding and protecting Plaintiff's and Class members' PII/PHI.

66. Empress has a fiduciary duty to act for the benefit of Plaintiff and Class members upon matters within the scope of their relationship. It breached that duty by failing to properly protect the integrity of the system containing Plaintiff's and Class members' PII/PHI, failing to comply with the data security guidelines set forth by HIPAA, and otherwise failing to safeguard Plaintiff's and Class members' PII/PHI that it collected.

67. As a direct and proximate result of Empress' breaches of its fiduciary duties, 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 effort attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII/PHI which remains in Empress' possession; (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; and (vii) overpayment for the services that were received without adequate data security.

COUNT IV
BREACH OF EXPRESS CONTRACT

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

69. Plaintiff and Class members and Empress entered into written agreements regarding their medical care and other services that Empress was to provide to Plaintiff and Class members. Plaintiff and Class members paid Empress monies, directly or through an insurance carrier, and provided Empress with their PII/PHI as consideration for these agreements. Empress' Privacy Practices Statement is evidence that data security was a material term of these contracts.

70. Plaintiff and Class members complied with the express contract when they paid Empress, directly or through an insurance carrier and provided their PII/PHI to Empress.

71. Empress breached its obligations under the contracts between itself and Plaintiff and Class members by failing to implement and maintain reasonable security measures to protect and secure their PII/PHI.

72. Empress' breach of the express contracts between itself, on the one hand, and Plaintiff and Class members, on the other hand directly caused the Data Breach.

73. Plaintiff and all other Class members were damaged by Empress' breach of express contracts because: (i) they paid—directly or through their insurers—for data security protection they did not receive; (ii) they face a substantially increased risk of identity theft and medical theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (iii) their PII/PHI was improperly disclosed to unauthorized

individuals; (iv) the confidentiality of their PII/PHI has been breached; (v) they were deprived of the value of their PII/PHI, for which there is a well-established national and international market; (vi) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face; and (vii) overpayment for the services that were received without adequate data security.

COUNT V
BREACH OF IMPLIED CONTRACT

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

75. In connection with receiving health care services, Plaintiff and all other Class members entered into implied contracts with Empress.

76. Pursuant to these implied contracts, Plaintiff and Class members paid money to Empress and provided Empress with their PII/PHI. In exchange, Empress agreed to, among other things, and Plaintiff understood that Empress would: (1) provide health care or other services to Plaintiff and Class member; (2) take reasonable measures to protect the security and confidentiality of Plaintiff's and Class members' PII/PHI; and (3) protect Plaintiff's and Class members PII/PHI in compliance with federal and state laws and regulations and industry standards.

77. The protection of PII/PHI was a material term of the implied contracts between Plaintiff and Class members, on the one hand, and Empress, on the other hand. Indeed, as set forth *supra*, Empress recognized the importance of data security and the privacy of its patients' PII/PHI in its Privacy Practices Statement. Had Plaintiff and Class members known that Empress would not adequately protect its patients' and former patients' PII/PHI, they would not have received services from Empress.

78. Plaintiff and Class members performed their obligations under the implied contract when they provided Empress with their PII/PHI and paid Empress for services.

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

80. Empress' 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.

81. Plaintiff and all other Class members were damaged by Empress' breach of implied contracts because: (i) they paid—directly or through their insurers—for data security protection they did not receive; (ii) they face a substantially increased risk of identity theft and medical theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (iii) their PII/PHI was improperly disclosed to unauthorized individuals; (iv) the confidentiality of their PII/PHI has been breached; (v) they were deprived of the value of their PII/PHI, for which there is a well-established national and international market; (vi) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face; and (vii) overpayment for the services that were received without adequate data security.

COUNT VI
UNJUST ENRICHMENT

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

83. This claim is pleaded in the alternative to the breach of express contract and breach of implied contract claims.

84. Plaintiff and Class members conferred a monetary benefit upon Empress in the form of monies paid for services.

85. Empress accepted or had knowledge of the benefits conferred upon it by Plaintiff and Class Members. Empress also benefitted from the receipt of Plaintiff's and Class members' PII/PHI.

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

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

88. Empress 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.

COUNT VII
VIOLATIONS OF NEW YORK GENERAL BUSINESS LAW § 349

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

90. New York General Business Law § 349(a) states, "Deceptive acts or practices in the conduct of any business, trade or commerce or in the furnishing of any service in this state are hereby declared unlawful."

91. Empress engaged in "business," "trade," or "commerce" within the meaning of N.Y. Gen. Bus. Law § 349(a).

92. Plaintiff, Class members, and Empress are "persons" within the meaning of N.Y. Gen. Bus. Law § 349(h).

93. Empress makes explicit statements to its patients that their PII/PHI will remain private.

94. Empress' failure to make Plaintiff and Class members aware that it would not adequately safeguard their information while maintaining that it would is a "deceptive act or practice" under N.Y. Gen. Bus. Law § 349.

95. Had Plaintiff and Class members been aware that Empress omitted or misrepresented facts regarding the adequacy of its data security safeguards, Plaintiff and Class members would not have accepted services from Empress.

96. Due to the Data Breach, Plaintiff and Class members have lost property in the form of their PII/PHI. Further, Empress' failure to adopt reasonable practices in protecting and safeguarding its patients' PII/PHI will force Plaintiff and Class members to spend time or money to protect against identity theft. Plaintiff and Class members are now at a higher risk identity theft and other crimes. This harm sufficiently outweighs any justifications or motives for Empress' practice of collecting and storing PII/PHI without appropriate and reasonable safeguards to protect such information.

97. As a result of Empress' violations of the N.Y Gen. Bus. Law § 349, 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 effort attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII/PHI which remains in Empress' possession; (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; and (vii) overpayment for the services that were received without adequate data security.

98. Pursuant to N.Y. Gen. Bus. Law § 349(h), Plaintiff seeks damages on behalf of himself and the Class in the amount of the greater of actual damages or $50 for each violation of N.Y. Gen. Bus. Law § 349. Because Empress' conduct was committed willfully and knowingly, Plaintiff and Class members are entitled to recover up to three times their actual damages up to $1,000.

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 Empress 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, seeks appropriate injunctive relief designed to prevent Empress 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: September 28, 2022

Respectfully submitted,

/s/ Jeremiah Frei-Pearson

Jeremiah Frei-Pearson
Todd S. Garber
Andrew C. White
FINKELSTEIN, BLANKINSHIP, FREI-PEARSON & GARBER, LLP
One North Broadway, Suite 900
White Plains, NY 10601
Tel: 914-298-3284
Fax: 914-908-6722
jfrei-pearson@fbfglaw.com
tgarber@fbfglaw.com
awhite@fbfglaw.com

Anthony L. Parkhill*
Riley W. Prince*
BARNOW AND ASSOCIATES, P.C.
205 West Randolph Street, Ste. 1630
Chicago, IL 60606
Tel: 312-621-2000
Fax: 312-641-5504
aparkhill@barnowlaw.com
rprince@barnowlaw.com

Seth A. Meyer*
Alex J. Dravillas*
KELLER POSTMAN LLC
150 N. Riverside, Suite 4100
Chicago, Illinois 60606
Tel: (312) 741-5220
sam@kellerlenkner.com
ajd@kellerlenkner.com

*pro hac vice to be submitted

Attorneys for Plaintiff
and the Putative Class