

**SUPREME COURT OF THE STATE OF NEW YORK
COUNTY OF WESTCHESTER**

JOHN FINN and SALVATORE J.
CONTRISTANO, individually and on
behalf of all others similarly situated,

Plaintiffs,

v.

EMPRESS AMBULANCE SERVICE,
LLC,

Defendant.

Index No.

CLASS ACTION

JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiffs John Finn and Salvatore J. Contristano (“Plaintiffs”), individually and on behalf of all others similarly situated (collectively, “Class members”), by and through their attorneys, bring this Class Action Complaint against Defendant Empress Ambulance Service, LLC (“Empress” or the “Defendant”) and complain and allege upon personal knowledge as to themselves and information and belief as to all other matters.

INTRODUCTION

1. Plaintiffs bring this class action against Empress for its failure to secure and safeguard their and approximately 318,556 other individuals’ personally identifiable information (“PII”) and personal health information (“PHI”) (collectively “PII/PHI” or “Personal Information”), including names, dates of service, Social Security numbers, and insurance information.

2. Defendant is a corporation in Yonkers, New York that provides emergency medical services and mutual aid to the neighboring communities.

3. On or about July 14, 2022, Empress discovered that unauthorized individuals had gained access to Empress's network systems and had access to the PII/PHI of Plaintiffs and Class members (the "Data Breach" or "Network Incident").

4. Empress owed a duty to Plaintiffs 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' PII/PHI from unauthorized access and disclosure.

5. As a result of Empress's inadequate security and breach of its duties and obligations, the Data Breach occurred, and Plaintiffs' and Class members' PII/PHI was accessed and disclosed. This action seeks to remedy these failings and their consequences. Plaintiffs bring this action on behalf of themselves and all natural persons who are residents of the United States whose Personal Information was potentially compromised in the Network Incident and were sent via U.S. Mail notice by Empress that their Personal Information may have been compromised in the Network Incident.

6. Plaintiffs, on behalf of themselves and all other Class members, assert 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 seek declaratory relief, injunctive relief, monetary damages, statutory damages, punitive damages, equitable relief, and all other relief authorized by law.

PARTIES

7. Plaintiff John Finn is a New York resident. Plaintiff Finn received services from Empress. He provided his PII/PHI, or his PII/PHI was provided, to Empress in connection with

receiving health care services from Empress. He received a letter from Empress on or about September 18, 2022 notifying him that his PII/PHI may have been exposed in the Data Breach. Plaintiff Finn would not have accepted services from Empress or agreed to have Empress receive his PII/PHI had he known that his PII/PHI would not be adequately safeguarded by Empress.

8. Plaintiff Salvatore J. Contristano is a New York resident. Plaintiff Contristano received services from Empress. He provided his PII/PHI to Empress in connection with receiving health care 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.

9. Defendant Empress Ambulance Service, LLC is a corporation organized under the laws of New York and maintains its principal place of business at 722 Nepperhan Avenue, Yonkers, New York 10703.

JURISDICTION AND VENUE

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

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

FACTUAL ALLEGATIONS

Overview of Empress

12. Empress is a corporation that provides emergency medical services and after care transportation in New York state.

13. In the regular course of its business, Empress collects and maintains the PII/PHI of patients, former patients, and other persons to whom it is currently providing or previously

provided health-related or other services.

14. Empress requires patients to provide personal information before it provides them services. That information includes, *inter alia*, names, addresses, dates of birth, health insurance information, and Social Security numbers. Empress stores this information digitally.

15. In their Privacy Notice, Empress states that it is “committed to protecting your personal health information” and that “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.”¹

16. Plaintiffs and Class members are, or were, patients of Empress or received health-related or other services from Empress, and entrusted Empress with their PII/PHI.

The Data Breach

17. On or about July 14, 2022, Empress discovered that an unauthorized individual, or unauthorized individuals, gained access to Empress’s network systems. Empress revealed that unknown parties first accessed Empress’s computer networks on May 26, 2022 and copied files on July 13, 2022.

18. Empress began to notify patients about the Data Breach on or about September 9, 2022. The letter sent to those affected by the Data Breach states that the information that was accessed included: “[P]atient names, dates of service, insurance information, and in some instances, Social Security numbers.”²

¹ Empress Emergency Medical Service, *Notice of Privacy Practices*, EMPRESSEMS.COM, <http://empressems.com/files/empressprivacy.pdf> (last visited May 5, 2023).

² Jeff Edwards, *300K Patients’ Data Compromised in Ransomware Attack on Empress EMS*, PATCH (Sep. 22, 2022), <https://patch.com/new-york/newrochelle/300k-patients-compromised-ransomware-attack-empress-ems>.

Empress Knew that Criminals Target PII/PHI

19. At all relevant times, Empress knew, or should have known, its patients' PII/PHI was a target for malicious actors. Despite such knowledge, Empress failed to implement and maintain reasonable and appropriate data privacy and security measures to protect Plaintiffs' and Class members' PII/PHI from cyber-attacks that Empress should have anticipated and guarded against.

20. Cyber criminals seek out PII/PHI at a greater rate than other sources of personal information. In a 2021 report, the healthcare compliance company Protenus found that there were 758 medical data breaches in 2020 with over 40 million patient records exposed.³ This was an increase from the 572 medical data breaches that Protenus compiled in 2019.⁴ In 2021, 905 health data breaches were reported and, according to Protenus's assessment, although a record number of data breaches were reported, the impact of breaches continues to be underreported overall and underrepresented to the public.⁵ In 2022, 956 health data breaches were reported in a steady increase year over year with approximately 60 million patient records affected.⁶

21. PII/PHI is a valuable property right.⁷ The value of PII/PHI as a commodity is

³ Protenus, *2021 Breach Barometer*, PROTENUS.COM, <https://www.protenus.com/resources/2021-breach-barometer> (last accessed May 5, 2023).

⁴ Protenus, *2020 Breach Barometer*, PROTENUS.COM, <https://www.protenus.com/resources/2020-breach-barometer> (last accessed May 5, 2023).

⁵ Protenus, *2022 Breach Barometer*, PROTENUS.COM, https://www.protenus.com/hubfs/Breach_Barometer/BreachBarometer_Privacy_2022_Protenus.pdf?utm_campaign=Forbes%2520Articles&utm_source=forbes&utm_medium=article&utm_content=breach%2520barometer (last accessed May 5, 2023).

⁶ Protenus, *2023 Breach Barometer*, PROTENUS.COM, https://email.protenus.com/hubfs/Breach_Barometer/2023/BreachBarometer_Privacy_2023_Protenus.pdf (last accesses May 5, 2023).

⁷ 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

measurable.⁸ “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.”⁹ American companies are estimated to have spent over \$19 billion on acquiring personal data of consumers in 2018.¹⁰ 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 its real value and the recent large-scale data breaches, identity thieves and cyber criminals have openly posted credit card numbers, Social Security numbers (“SSNs”), 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 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.”¹¹ A cybercriminal who steals a person’s PHI can end up with as many as “seven to ten

possible...”),

https://www.researchgate.net/publication/283668023_The_Value_of_Personal_Data.

⁸ 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>.

⁹ 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.

¹⁰ 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/>.

¹¹ 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-percon> (quoting Tom Kellermann, Chief Cybersecurity Officer, Carbon Black, stating “Health information is a treasure trove for criminals.”).

personal identifying characteristics of an individual.”¹² A study by Experian found that the “average total cost” of medical identity theft is “about \$20,000” per incident, and that a majority 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.¹³

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.¹⁴ 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.¹⁵

25. Criminals can use stolen PII/PHI to extort a financial payment by “leveraging details specific to a disease or terminal illness.”¹⁶ 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.”¹⁷

¹² *Id.*

¹³ 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>.

¹⁴ 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>.

¹⁵ 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>.

¹⁶ *What Happens to Stolen Healthcare Data*, *supra* at n.11.

¹⁷ *Id.*

26. Consumers place a high value on the privacy of that data. 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.”¹⁸

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 exhaust financial accounts, receive medical treatment, start new utility accounts, and incur charges and credit in a person’s name.¹⁹

29. Identity thieves use personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.²⁰ 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:

¹⁸ 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>.

¹⁹ 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 May 5, 2023).

²⁰ 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).

open a new credit card or loan; change a billing address so the victim no longer receives bills; open new utility accounts; obtain a mobile phone; open a bank account and write bad checks; use a 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.²¹

30. With access to an individual's PII/PHI, criminals can do more than just empty a victim's bank account—they can also commit all manner of fraud, including: obtaining a driver's license or official identification card in the victim's name but with the thief's picture; using the victim's name and SSN to obtain government benefits; or, filing a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's SSN, rent a house, or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest, resulting in an arrest warrant being issued in the victim's name.²²

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.²³

32. Theft of SSNs, which are reportedly exposed in this breach, creates a particularly alarming situation for victims because those numbers cannot easily be replaced. In order to obtain

²¹ See Susan Henson, *What Can Identity Thieves Do with Your Personal Information and How Can You Protect Yourself?*, EXPERIAN (Sept. 1, 2017), <https://www.experian.com/blogs/ask-experian/what-can-identity-thieves-do-with-your-personal-information-and-how-can-you-protect-yourself/>.

²² See Federal Trade Commission, *Warning Signs of Identity Theft*, IDENTITYTHEFT.GOV <https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft> (last accessed May 5, 2023).

²³ Identity Theft Resource Center, *2021 Consumer Aftermath Report*, IDENTITY THEFT RESOURCE CENTER (2021), <https://www.idtheftcenter.org/identity-theft-aftermath-study/> (last accessed May 5, 2023).

a new number, a breach victim has to demonstrate ongoing harm from misuse of her SSN, and a new SSN will not be provided until after the harm has already been suffered by the victim.

33. Due to the highly sensitive nature of SSNs, theft of SSNs in combination with other PII (e.g., name, address, date of birth) is akin to having a master key to the gates of fraudulent activity. TIME quotes data security researcher Tom Stickley, who is employed by companies to find flaws in their computer systems, as stating, “If I have your name and your Social Security number and you don’t have a credit freeze yet, you’re easy pickings.”²⁴

34. 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.”²⁵ It “is also more difficult to detect, taking almost twice as long as normal identity theft.”²⁶ 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 medical care.”²⁷ The FTC also warns, “If the thief’s health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected.”²⁸

35. 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:

²⁴ Patrick Lucas Austin, *‘It Is Absurd.’ Data Breaches Show it’s Time to Rethink How We Use Social Security Numbers, Experts Say*, TIME (August 5, 2019), <https://time.com/5643643/capital-one-equifax-data-breach-social-security/>.

²⁵ Pam Dixon and John Emerson, *The Geography of Medical Identity Theft*, FTC.GOV (Dec. 12, 2017), <https://www.worldprivacyforum.org/2017/12/new-report-the-geography-of-medical-identity-theft/>.

²⁶ See *Health Care Systems and Medical Devices at Risk...*, *supra* at n.15.

²⁷ 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 May 5, 2023).

²⁸ *Id.*

- 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.²⁹

36. 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 and it takes some individuals up to three years to learn that information.³⁰

37. It is within this context that Plaintiffs and all other Class members must now live with the knowledge that their PII/PHI is forever in cyberspace and was taken by people willing to

²⁹ See *The Geography of Medical Identity Theft*, *supra* at 25.

³⁰ 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>.

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 Plaintiffs and the Other Class Members

38. Plaintiffs and all other Class members have suffered injury and damages, 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's 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) of overpayment for the services that were received without adequate data security.

CLASS ALLEGATIONS

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

40. Plaintiffs bring this action on behalf of themselves and all members of the following Class of similarly situated persons:

All natural persons who are residents of the United States whose Personal Information was potentially compromised in the Network Incident and were sent via U.S. Mail notice by Empress that their Personal Information may have been compromised in the Network Incident.

41. Excluded from the Class are: (1) the Judges presiding over the action and members of their families; (2) Empress, its subsidiaries, parent companies, successors, predecessors, and any entity in which Empress or its parents, have a controlling interest, and its current or former

officers and directors; (3) natural persons who properly submit a timely request for exclusion from the Class; and (4) the successors or assigns of any such excluded natural person.

42. Certification of Plaintiffs' claims for class-wide treatment is appropriate because Plaintiffs can prove the elements of their 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.

43. The members in the Class are so numerous that joinder of all Class members in a single proceeding would be impracticable. Empress reported to the U.S. Department of Health and Human Services' Office of Civil Rights that approximately 318,558 individuals' information was exposed in the Data Breach.

44. 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 Plaintiffs' and Class Members' PII/PHI from unauthorized access and disclosure;
- b. Whether Empress failed to exercise reasonable care to secure and safeguard Plaintiffs' and Class Members' PII/PHI;
- c. Whether an express and/or 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 Plaintiffs' and Class members' PII/PHI; and

- e. Whether Plaintiffs and all other members of the Class are entitled to damages and the measure of such damages and relief.

45. Empress engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiffs on behalf of themselves 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.

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

47. Plaintiffs will fairly and adequately protect the interests of the Class members. Plaintiffs are adequate representatives of the Class in that they have no interests adverse to, or that conflict with, the Class they seek to represent. Plaintiffs have retained counsel with substantial experience and success in the prosecution of complex consumer protection class actions of this nature.

48. 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 Plaintiffs and all other 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'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

49. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

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

51. Empress knew the risks of collecting and storing Plaintiffs' and all other Class members' PII/PHI and the importance of maintaining secure systems. Empress knew of the many data breaches that targeted healthcare providers in recent years.

52. Given the nature of Empress's 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.

53. Empress breached these duties by failing to exercise reasonable care in safeguarding and protecting Plaintiffs' 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 Plaintiffs' and Class members' PII/PHI.

54. It was reasonably foreseeable to Empress that its failure to exercise reasonable care in safeguarding and protecting Plaintiffs' 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 Plaintiffs' and Class members' PII/PHI to unauthorized individuals.

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

56. As a result of Empress's above-described wrongful actions, inaction, and want of ordinary care that directly and proximately caused the Data Breach, Plaintiffs and all other 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 risk of identity theft and medical theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII/PHI; (iii) breach of the confidentiality of their PII/PHI; (iv) deprivation of the value of their PII/PHI, for which there is a well-established national and international market; (v) 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; (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) of overpayment for the services that were received without adequate data security.

COUNT II

NEGLIGENCE PER SE

57. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully

set forth herein.

58. Empress'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").

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

60. Empress violated HIPAA Privacy and Security Rules and Section 5 of the FTCA by failing to use reasonable measures to protect Plaintiffs' and all other Class members' PII/PHI and not complying with applicable industry standards. Empress'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 Plaintiffs and the other Class members.

61. Empress's violations of HIPAA Privacy and Security Rules and Section 5 of the FTCA constitutes negligence per se.

62. Plaintiffs 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.

63. 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.

64. It was reasonably foreseeable to Empress that its failure to exercise reasonable care in safeguarding and protecting Plaintiffs' 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 Plaintiffs' and Class members' PII/PHI to unauthorized individuals.

65. The injury and harm that Plaintiffs and the other Class members suffered was the direct and proximate result of Empress's violations of HIPAA Privacy and Security Rules and Section 5 of the FTCA. Plaintiffs 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 risk of identity theft and medical theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII/PHI; (iii) breach of the confidentiality of their PII/PHI; (iv) deprivation of the value of their PII/PHI, for which there is a well-established national and international market; (v) 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; (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) of overpayment for the services that were received without adequate data security.

COUNT III

BREACH OF FIDUCIARY DUTY

66. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

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

68. Empress has a fiduciary duty to act for the benefit of Plaintiffs 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 Plaintiffs' and Class Members' PII/PHI, failing to comply with the data security guidelines set forth by HIPAA, and otherwise failing to safeguard Plaintiffs' and Class members' PII/PHI that it collected.

69. As a direct and proximate result of Empress's breaches of its fiduciary duties, Plaintiffs 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's 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) of overpayment for the services that were received without adequate data security.

COUNT IV**BREACH OF EXPRESS CONTRACT**

70. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

71. Plaintiffs and Class members and Empress entered into written agreements regarding their medical care and other services that Empress was to provide to Plaintiffs and Class members. Plaintiffs 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.

72. Plaintiffs 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.

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

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

75. Plaintiffs 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) of overpayment for the services that were received without adequate data security.

COUNT V

BREACH OF IMPLIED CONTRACT

76. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

77. In connection with receiving medical services, Plaintiffs and all other Class members entered into implied contracts with Empress.

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

79. The protection of PII/PHI was a material term of the implied contracts between Plaintiffs 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 Notice. Had Plaintiffs and Class members known that Empress would not adequately protect its patients' and former patients' PII/PHI, they would not have received medical services from Empress.

80. Plaintiffs and Class members performed their obligations under the implied contract when they provided Empress with their PII/PHI and paid—directly or through their insurers—for health care services from Empress.

81. Empress breached its obligations under its implied contracts with Plaintiffs 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 Plaintiffs' and Class members' PII/PHI in a manner that complies with applicable laws, regulations, and industry standards.

82. Empress's breach of its obligations of its implied contracts with Plaintiffs and Class members directly resulted in the Data Breach and the injuries that Plaintiffs and all other Class members have suffered from the Data Breach.

83. Plaintiffs and all other Class members were damaged by Empress's 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) of overpayment for the services that were received without adequate data security.

COUNT VI**UNJUST ENRICHMENT**

84. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

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

86. Plaintiffs and Class members conferred a monetary benefit upon Empress in the form of monies paid for healthcare services or other services.

87. Empress accepted or had knowledge of the benefits conferred upon it by Plaintiffs and Class Members. Empress also benefitted from the receipt of Plaintiffs' and Class members' PII/PHI, as this was used to facilitate payment.

88. As a result of Empress's conduct, Plaintiffs 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 Plaintiffs and Class members paid for, and those payments without reasonable data privacy and security practices and procedures that they received.

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

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

COUNT VII**VIOLATIONS OF THE NEW YORK DECEPTIVE ACTS AND PRACTICES ACT
N.Y. Gen. Bus. Law § 349 (“GBL”)**

91. Plaintiffs re-allege and incorporate by reference the preceding paragraphs as if fully set forth herein.

92. Plaintiffs Finn and Contristano and Class members are “persons” within the meaning of the GBL. N.Y. Gen. Bus. Law § 349(h).

93. Empress is a “person, firm, corporation or association or agent or employee thereof” within the meaning of the GBL. N.Y. Gen. Bus. Law § 349(b).

94. Under GBL section 349, “[d]eceptive acts or practices in the conduct of any business, trade or commerce” are unlawful.

95. Empress violated the GBL through its promise to protect and subsequent failure to adequately safeguard and maintain Plaintiffs’ and Class members’ PII/PHI. Empress failed to notify Plaintiffs and other class members that, contrary to its representations about valuing data security and privacy, it does not maintain adequate controls to protect PII/PHI. It omitted all of this information from Plaintiffs and class members.

96. As a result of Empress’s above-described conduct, Plaintiffs Finn and Contristano and the Class have suffered damages from the disclosure of their information to unauthorized individuals.

97. The injury and harm that Plaintiffs Finn and Contristano and the other Class members suffered was the direct and proximate result of Empress’s violations of the GBL. Plaintiffs Finn and Contristano 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 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's 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) of overpayment for the services that were received without adequate data security.

98. Plaintiffs Finn and Contristano, individually and on behalf of the Class, request that this Court enter such orders or judgments as may be necessary to enjoin Empress from continuing its unfair and deceptive practices.

99. Under the GBL, Plaintiffs Finn and Contristano and Class members are entitled to recover their actual damages or \$50, whichever is greater. Additionally, because Defendant acted willfully or knowingly, Plaintiffs Finn and Contristano and Class members are entitled to recover three times their actual damages. Plaintiffs are also entitled to reasonable attorneys' fees.

PRAYER FOR RELIEF

Plaintiffs, individually and on behalf of all other members of the Class, respectfully request that the Court enter judgment in their favor and against Empress as follows:

A. Certifying the Class as requested herein, designating Plaintiffs as Class representatives, and appointing Plaintiffs' counsel as Class Counsel;

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

C. Awarding Plaintiffs and the Class equitable, injunctive, and declaratory relief, as may be appropriate. Plaintiffs, on behalf of themselves and the Class, seek 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 Plaintiffs and the Class pre-judgment and post-judgment interest to the maximum extent allowable;

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

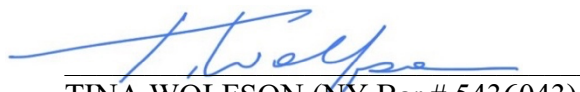
F. Awarding Plaintiffs and the Class such other favorable relief as allowable under law.

JURY TRIAL DEMANDED

Plaintiffs demand a trial by jury of all claims in this Class Action Complaint so triable.

Dated: May 11, 2023

Respectfully submitted,



TINA WOLFSON (NY Bar # 5436043)
521 5th Avenue, 17th Floor
New York, NY 10175
Telephone: 917-336-0171
Facsimile: 917-336-0177
twolfson@ahdootwolfson.com

DEBORAH DE VILLA (NY Bar # 5724315)
AHDOOT & WOLFSON, PC
2600 W. Olive Avenue, Suite 500
Burbank, CA 91505-4521
Telephone: 310-474-9111
Facsimile: 310-474-8585
ddevilla@ahdootwolfson.com

ANDREW W. FERICH*
AHDOOT & WOLFSON, PC

201 King of Prussia Road, Suite 650
Radnor, PA 19087
Telephone: 310-474-9111
Facsimile: 310-474-8585
aferich@ahdootwolfson.com

BEN BARNOW (NY Bar # 2253391)
ANTHONY L. PARKHILL*
BARNOW AND ASSOCIATES, P.C.
205 West Randolph Street, Ste. 1630
Chicago, IL 60606
Telephone: 312-621-2000
Facsimile: 312-641-5504
b.barnow@barnowlaw.com
aparkhill@barnowlaw.com

Attorneys for Plaintiffs

**pro hac vice to be submitted*

ATTORNEY'S VERIFICATION

I, Tina Wolfson, Esq., an attorney duly admitted to practice in the Courts of the State of New York, hereby affirm the following to be true under the penalty of perjury:

That I am associated with the firm AHDOOT & WOLFSON, PC, the attorneys for the Plaintiffs in the within action and as such I am fully familiar with the facts and circumstances surrounding this matter based upon my review of the contents of the file maintained by this office.

That I have read the foregoing SUMMONS and COMPLAINT and know the contents thereof; that the same is true to my own knowledge except as to the matters stated to be alleged upon information and belief; and, as to those matters, I believe them to be true.

That the reason this verification is made by your affirmant and not by the Plaintiffs is that the Plaintiffs do not reside within the count in which my office is maintained.

That the grounds for your affirmant's belief as to all matters not stated upon my own knowledge are as follows: facts, investigations, reports, records, and documents contained in Plaintiffs' file maintained by your affirmant's office.

Dated: Sherman Oaks, CA
May 11, 2023



Tina Wolfson, Esq.