UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

SALVATORE J. CONTRISTANO, individually and on behalf of all others similarly situated, Plaintiff, vs. EMPRESS AMBULANCE SERVICE, LLC, Defendant.	Case No. **NOTICE OF REMOVAL**

Pursuant to 28 U.S.C. §§ 1441, 1446, and 1453, Defendant, Empress Ambulance Service, LLC, files this Notice of Removal of Plaintiff's civil action from the Supreme Court of the State of New York, County of Westchester, to this Court based on diversity of citizenship under 28 U.S.C. § 1332. In support of its Notice, Defendant states as follows:

PLEADINGS AND BACKGROUND

1. On or about September 28, 2022, Plaintiff Salvatore J. Contristano ("Plaintiff") filed a purported class action complaint in the Supreme Court of the State of New York, County of Westchester, Case No. 65746/2022 (the "State Court Action"). *See* State Court Action Complaint, attached hereto as **Exhibit A** ("Complaint").

2. Service of the Complaint was made upon Defendant Empress Ambulance Service, LLC ("Empress" or "Defendant") on October 10, 2022. A true and correct copy of the Summons and Proof of Service are attached as **Exhibit B**.

3. The Complaint alleges that Empress failed to properly safeguard its patients' sensitive personal information and seeks damages and injunctive relief.

4. A copy of the docket in the State Court Action is attached as **Exhibit C**.

5. In accordance with 28 U.S.C. § 1446(a), all process, pleadings, and orders that have been filed and served in the state court action are attached to this Notice of Removal as Exhibits A-C.

6. Nothing in this Notice of Removal shall constitute a waiver of Defendant's right to assert any defense, including a motion to dismiss, as the case progresses.

PROCEDURAL REQUIREMENTS

7. Removal of this action is timely because Empress was served with Plaintiff's Complaint on October 10, 2022. *See* Exhibit B. In accordance with 28 U.S.C. § 1446(b), Empress seeks to remove the Complaint within thirty (30) days of first being served. *See Murphy Brothers, Inc. v. Michetti Pipe Stringing, Inc.*, 526 U.S. 344, 356 (1999) (holding that the time to remove an action runs from receipt of service of process).

8. This Court is in the judicial district and division embracing the place where the state court case was brought and is pending. Thus, this Court is the proper district court to which this case should be removed. 28 U.S.C. §§ 1441(a), 1446(a).

9. Pursuant to 28 U.S.C. § 1446(b), Empress will promptly provide written notice of removal of the action to Plaintiff and will promptly file a copy of this Notice of Removal with the Clerk of the Supreme Court of the State of New York for the County of Westchester.

SUBJECT MATTER JURISDICTION

10. This is a civil action over which this Court has original subject matter jurisdiction under 28 U.S.C. § 1332, and removal is proper under the Class Action Fairness Act of 2005 ("CAFA"), codified in pertinent part at 28 U.S.C. § 1332(d).

11. Section 1332(d) provides that a district court shall have original jurisdiction over a class action with one hundred (100) or more putative class members, in which the matter in

controversy, in the aggregate, exceeds the sum or value of $5 million. Section 1332(d) further provides that, for original jurisdiction to exist, "any member of a class of plaintiffs" must be a "citizen of a State different from any Defendant." 28 U.S.C. § 1332(d)(2)(A).

12. As set forth below, pursuant to 28 U.S.C. § 1332(d) and § 1441(a), Empress may remove the State Court Action to federal court under CAFA because: (i) this action is pled as a class action; (ii) the putative class includes more than one hundred (100) members; (iii) members of the putative class are citizens of a state different from that of Defendant; and (iv) the matter in controversy, in the aggregate, exceeds the sum or value of $5,000,000, exclusive of interest and costs. *See Gale v. Chi. Title Ins. Co.*, 929 F.3d 74, 77 (2d Cir. 2019).

This Action is Pled as a Class Action

13. CAFA defines a "class action" as "any civil action filed under rule 23 of the Federal Rules of Civil Procedure or similar State statute or rule of judicial procedure authorizing an action to be brought by 1 or more representative persons as a class action." 28 U.S.C. § 1332 (d)(1)(B).

14. Plaintiff brings this action as a "class action" and seeks certification under New York law pursuant to the New York Civil Practice Law and Rules (NY CPLR) § 901, *et seq*. *See* Exhibit A at ¶¶ 37-46. Because New York's class action rules are "patterned on Federal Rule of Civil Procedure 23," *Alix v. Wal-Mart Stores, Inc.*, 838 N.Y.S. 2d 885, 852 n.6 (Sup. Ct. 2007); *Ramirez v. Oscar De La Renta, LLC*, No. 16-CV-7855 (RA), 2017 WL 2062960, at *1, *9 (S.D.N.Y. May 12, 2017), the first CAFA requirement is met, *see* Exhibit A at ¶ 37 ("This action is brought and may be properly maintained as a class action . . .").

The Putative Class Includes at Least One Hundred (100) Members

15. 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." Exhibit A at ¶ 1. Plaintiff alleges that, "[b]etween 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 PII/PHI of Plaintiff and Class members," (the "Security Incident"). *Id*. at ¶ 3. Plaintiff further alleges that the Security Incident occurred as a result of Empress' failure to "implement and maintain reasonable security procedures and practices to protect its patients' and former patients' PII/PHI from unauthorized access and disclosure." *Id*. at ¶ 4.

16. Based on these allegations, Plaintiff asserts seven causes of action against Empress: (1) negligence, (2) negligence *per se*, (3) breach of fiduciary duty, (4) breach of contract, (5) breach of implied contract, (6) breach of unjust enrichment, and (7) violations of New York General Business Law ("NYGBL") § 349. *See* Exhibit A.

17. Furthermore, Plaintiff purports to bring these causes of action on behalf of himself and a nationwide class (the "Class"). Exhibit A at ¶ 38. Plaintiff defines the Class as: "[a]ll persons whose PII/PHI was exposed to unauthorized persons in the [Security Incident], including all persons who were sent a notice of the [Security Incident]." *Id*.

18. While Plaintiff does not allege the exact number of the Class, Plaintiff alleges that "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 [Security Incident]." *Id*. at ¶ 41.

19. Empress mailed notification to approximately 318,558 people within the United States that their information may have been impacted in the Security Incident.

20. Therefore, the number of putative class members exceeds the statutorily required

minimum of 100.

Minimal Diversity of Citizenship Exists

21. Pursuant to 28 U.S.C. § 1332(d)(2)(A), the "district court shall have original jurisdiction" over a "class in which . . . any member of the class of plaintiffs is a citizen of a State different from any defendant." *See also* 28 U.S.C. § 1332(d)(1)(D) (Under CAFA, "the term 'class members' means the persons (named or unnamed) who fall within the definition of the proposed or certified class in a class action"); *Fleisher v. Phoenix Life Ins. Co.*, 997 F. Supp. 2d 230, 238 (S.D.N.Y. 2014) ("[M]inimal diversity [is] diversity between ***any plaintiff class member*** and any defendant." (emphasis added)).

22. Plaintiff's and the Putative Class's Citizenship. "An individual's citizenship . . . is determined by his domicile." *Palazzo ex rel. Delmage v. Corio*, 232 F.3d 38, 42 (2d Cir. 2000); *Emiabata v. Farmers Ins. Co.*, 848 F. App'x 27, 28 (2d Cir. 2021) (citing 28 U.S.C. § 1332(a)(1)). And a person's domicile, in turn, represents "the place where [the] person has his true fixed home and principal establishment, and to which, whenever he is absent, he has the intention of returning." *Id*. (quoting *Linardos v. Fortuna*, 157 F.3d 945, 948 (2d Cir. 1998)). Here, Plaintiff alleges in the Complaint that he "is New York resident." Exhibit A at ¶ 7. Accordingly, absent other evidence to the contrary, Plaintiff is a citizen of New York.

23. Plaintiff also seeks to represent a class that (1) includes "[a]ll persons whose PII/PHI was exposed to unauthorized persons in the [Security Incident], including all persons who were sent a notice of the [Security Incident]," *id*. at ¶ 38, and (2) that is not geographically limited. To date, Empress has sent notification of the Security Incident to addresses in all 50 states and the District of Columbia. And while residency does not equate to citizenship, in this case, where only one putative class member must reside and intend to remain in a state diverse from Empress, and

where Empress sent notifications to addresses in all 50 states, it is more likely than not that at least one of the approximately 318,558 putative class members is diverse from Empress.

24. Defendant's Citizenship. Under 28 U.S.C. § 1332(d)(10), "an unincorporated association shall be deemed to be a citizen of the State where it has its principal place of business and the State under whose laws it is organized." Though the "Second Circuit has not provided guidance as to a limited liability company's citizenship for purposes of CAFA jurisdiction," this Court and sister courts in New York have concluded that a limited liability company is an unincorporated association and citizenship is determined pursuant to 28 U.S.C. § 1332(d)(10). *Kim v. Trulia, LLC*, No. 19-cv-06733, 2021 WL 8743946, *3 (E.D.N.Y. Mar. 31, 2021) (citing *Carter v. HealthPort Techs., LLC*, 822 F.3d 47, 60 (2d Cir. 2016) ("The term 'unincorporated association' is not defined in CAFA, and this Court has not addressed the question of whether it encompasses limited liability companies."); *Claridge v. N. Am. Power & Gas Co., LLC*, No. 15–cv–1261 (PKC), 2015 WL 5155934, at *1-2 (S.D.N.Y. Sept. 2, 2015) ("This Court concludes that as an LLC, [defendant] is an unincorporated association, and its citizenship in a CAFA action is determined pursuant to section 1332(d)(10)."); *see also Shulman v. Chaitman LLP*, 392 F. Supp. 3d 340, 351 (S.D.N.Y. 2019) (noting that defendants were citizens of New York because they are organized under the laws of New York and have their principal places of business in New York); *Ventimiglia v. Tishman Speyer Archstone–Smith Westbury, L.P.*, 588 F. Supp. 2d 329, 336 (E.D.N.Y. 2008) (applying section 1332(d)(10) to a limited partnership). Here, Plaintiff alleges that Empress is a "limited liability company formed in Delaware" and Empress's principal place of business is in New York. Exhibit A at ¶ 8.

25. Thus, minimal diversity of citizenship exists pursuant to CAFA. Empress is a citizen of New York and Delaware for purposes of diversity jurisdiction. Accordingly, "minimal

diversity" of citizenship is established because it is more likely than not that members of the putative class are citizens of a state other than New York or Delaware.

26. However, even if this Court were to consider Empress's citizenship under the traditional test for determining diversity jurisdiction, Empress would still establish minimal diversity. Traditionally, "a limited liability company . . . takes the citizenship of each of its members." *Bayerische Landesbank, N.Y. Branch v. Aladdin Cap. Mgmt. LLC*, 692 F.3d 42, 49 (2d Cir. 2012). Here, Empress is wholly-owned by Paramedics Logistics Operating Company, LLC ("Paramedics Operating Company"), which in turn is wholly-owned by Paramedics Logistics Holding Company, LLC ("Paramedics Holding Company"). Paramedics Holding Company is comprised of seven different members which are either limited liability companies, limited partnerships, or corporations. Therefore, because Empress is 100% owned by its parent, which is 100% owned by Paramedics Holding Company, Paramedics Holding Company's seven members are the members the Court can evaluate to determine the citizenship of Empress. *See id*. Based on an analysis of the available information of these seven members, Empress is a citizen of Delaware, Connecticut, Florida, New York, and Oregon. For example, one of the relevant Paramedics Holding Company's members is CAS Holdings, Inc., which was incorporated in Connecticut and has its headquarters in Connecticut. Another member is Williams Transportation Group, Inc., which is incorporated in Florida, with its headquarters in Florida.

27. Accordingly, minimal diversity exists under the traditional test applied to the analysis of citizenship of limited liability companies because Empress is, at a minimum, a citizen of Delaware, New York, Connecticut, Florida, and Oregon, and it is more likely than not that members of the putative class are citizens of a state other than Delaware, Connecticut, Florida, New York, and Oregon.

28. No CAFA Exceptions Apply. There are "[t]hree enumerated exceptions to the exercise of CAFA jurisdiction [that] exists: the 'local controversy' and 'home state controversy' are mandatory exceptions; whereas the 'interests of justice' exception is discretionary." *Brook v. UnitedHealth Group Inc.*, No. 06-cv-12954, 2007 WL 2827808, at *3 (S.D.N.Y. Sept. 27, 2007) (citing 28 U.S.C. §§ 1332(2)(4)(A)-(B)). Under the "local controversy exception," the court is required to decline to exercise jurisdiction when, among other things, "during the 3–year period preceding the filing of that class action, no other class action has been filed asserting the same or similar factual allegations against any of the defendants on behalf of the same or other persons." *Carter v. CIOX Health, LLC*, 260 F. Supp. 3d 277, 282 (W.D.N.Y. 2017) (quoting 28 U.S.C. § 1332(d)(4)(A)). Similarly, under the "interests of justice exception" the court may decline jurisdiction if "during the 3–year period preceding the filing of that class action, 1 or more other class actions asserting the same or similar claims on behalf of the same or other persons have been filed." *Hart v. Rick's NY Cabaret Intern., Inc.*, 967 F. Supp. 2d 955, 968 (S.D.N.Y. 2014) (quoting 28 U.S.C. § 1332(d)(3)). And under the "home state" exception, "[a] district court is to decline jurisdiction [ ] where the primary defendants and at least two-thirds of the class members are citizens of the State in which the action was originally filed." *Brook*, 2007 WL 2827808, at *5.

29. First, the "local controversy" and "interests of justice" exceptions do not apply because there has been a class action filed within the last three years that asserts the same or similar claims on behalf of the same persons.[1] *See id*. at *4. Specifically, on September 22, 2022, plaintiff

[1] In addition, prior the filing of the Finn Class Action and the instant case, three other similar class actions were filed against Empress in the Southern District of New York alleging the same or similar facts and asserting the same or similar claims. *See Egan v. Empress Ambulance Service, LLC*, No. 7:22-cv-08584 (S.D.N.Y., Compl. filed Oct. 7, 2022); *Normand v. Empress Ambulance Services, Inc., d/b/a Empress EMS*, No. 7:22-cv-08590 (S.D.N.Y. Compl. filed Oct. 9, 2022); *Cardwell v. Empress Ambulance Services, LLC d/b/a Empress Emergency Medical Services f/k/a Empress Ambulance Services, Inc.*, No. 7:22-cv-08603 (S.D.N.Y. Compl. filed Oct. 10, 2022).

John Finn, individually and on behalf of all other similarly situated, filed a class action in this Court against Empress Ambulance Services, Inc., d/b/a Empress EMS that alleges Empress failed to properly safeguard patients' sensitive information and that as a result hackers were able to access plaintiff's and putative class members' sensitive information in the Security Incident. *Finn v. Empress Ambulance Service, Inc. d/b/a/ Empress EMS*, No. 7:22-cv-08101 (S.D.N.Y) ("Finn Class Action"), Complaint attached hereto as **Exhibit D**. Based on these allegations, plaintiff Finn asserts claims for breach of fiduciary duty, breach of implied contract, negligence, negligence *per se*, unjust enrichment, and violations of NYGBL § 349. *Id*. There can be no dispute that (1) the Finn Class Action involves the same factual allegations as those at issue in this case; (2) both class actions were brought against the same defendant—Empress; and (3) it was filed within three years before this case. *See Carter*, 260 F. Supp. 3d at 282. There is also no requirement that the purported plaintiff classes be the exact same for these exceptions to apply. *Id*. at 284. Rather, "[t]he inquiry is whether **similar factual allegations** have been made against the defendant in multiple class actions." *Id.* at 284 (quoting S. REP. NO. 109–14 at 41(2005)). The purpose of the "no other class action" requirement "was to prevent the remand to state courts of 'copy cat' class actions, where 'duplicative class actions asserting similar claims on behalf of essentially the same people' were filed and pending in different courts." *Hart*, 967 F. Supp. 2d at 967 (quoting *Brook*, 2017 WL 282808, at *4)). Accordingly, the "local controversy" mandatory exception and the "interests of justice" discretion exceptions do not apply here, and the Court may exercise jurisdiction under CAFA.

30. Second, Plaintiff could never demonstrate that CAFA's "home state exception" applies. With over 300,000 putative class members with addresses in all 50 states, there simply is no way to know the citizenship of each putative class member without speaking directly to each

of those 300,000 individuals. *See Hart*, 967 F. Supp. 2d at 964 (stating that the key question is whether the class member "intended to make New York [their] permanent home"). That is especially true here, where many putative class members may just have been visiting New York or may have lived in New York while working "but who lacked the intent to make New York [their] home," when they received their ambulance services from Empress. *See id*. And, as the Court noted in *Hart*, those who "lack[ ] the intent to make New York [their] home [are] not a New York citizen for purposes of 28 U.S.C. § 1332." *Id*.

31. In sum, none of the CAFA exceptions apply and minimal diversity exists.

The Amount in Controversy Exceeds the CAFA Threshold[2]

32. Where a complaint does not specify the amount of damages sought, as is the case with Plaintiff's Complaint, the removing defendant must prove by a preponderance of the evidence that the jurisdictional amount-in-controversy is satisfied. 28 U.S.C.A. § 1446(c)(2)(B). The United States Supreme Court has held that "a defendant's notice of removal need include only a plausible allegation that the amount in controversy exceeds the jurisdictional threshold" to meet the amount-in-controversy requirement. *Dart Cherokee Basin Operating Co., LLC v. Owens*, 574 U.S. 81, 90 (2014).

33. As demonstrated below, the allegations in the Complaint make it more likely than not that the amount in controversy under CAFA exceeds $5,000,000.

34. Breach-of-Express-Contract and Breach-of-Implied-Contract Claims. Plaintiff alleges that "Plaintiff and Class members entered into written agreements regarding their medical

[2] The amounts set forth in this Notice of Removal are solely for the purposes of establishing that the amount in controversy exceeds the $5,000,000 threshold and are not intended and cannot be construed as an admission that Plaintiff can state a claim or is entitled to damages in any amount. Empress denies liability, denies Plaintiff is entitled to recover any amount, and denies that a class can be properly certified in this matter.

care and other services that Empress was to provide to Plaintiff and Class members." Exhibit A at ¶ 69. Plaintiff further alleges that "Empress breached its obligations under the contracts . . . by failing to implement and maintain reasonable security measures to protect and secure their PII/PHI." *Id*. at ¶ 71.

35. Plaintiff also alleges that "Plaintiff and all other Class members entered into implied contracts with Empress," and, in exchange for money, "Empress agreed to, among other things, . . . take reasonable measures to protect the security and confidentiality of Plaintiff's and Class members' PII/PHI." Exhibit A at ¶¶ 75-76. Plaintiff further alleges that "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." *Id*. at ¶ 79.

36. As a result of the alleged breaches of express and implied contracts, Plaintiff claims that he and the Class members were damaged 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) [they] lost time and money incurred to mitigate and remediate the effects of the [Security Incident], including the increased risks of medical identity theft they face and will continue to face; and (vii) [they were injured via] overpayment for the services that were received without adequate data security." *Id*. at ¶¶ 73, 81.

37. Plaintiff's Complaint contains no allegations that would support or suggest the amount in actual damages to which he or any member of the Class are allegedly entitled for

Empress's alleged breach of express and implied contracts. However, because Plaintiff seeks damages based on an "increased risk of identity theft and medical theft—risks [they claim] justify[] expenditures for protective and remedial services for which they are entitled to compensation," and because their PII/PHI was allegedly exposed, one option for assigning a value to these damages is through the cost of credit monitoring. *Id*. The cost of credit monitoring is the "out-of-pocket expenses" associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or authorized use of their PII and PHI that Plaintiff alleges he and the Class are at risk of in the future.

38. Three main identity-protection agencies—Equifax, LifeLock, and Experian—advertise monthly rates for credit-monitoring services ranging from $8.99 to $19.99 per person per month. For example, LifeLock offers a product, titled Norton360 with LifeLock, that provides 1-Bureau credit monitoring with up to $25,000 in "stolen funds reimbursement" for $8.99 per month.[3] Similarly, both Equifax[4] and Experian[5] offer products that provide 3-Bureau credit monitoring with up to $1 million in identity theft insurance for $19.95 and $19.99 per month. Multiplying just the cost of providing two months of credit-monitoring services at $8.99 (the cheapest of the three products) by the number of putative class members, the amount in controversy for just credit monitoring is approximately $5,727,672.84 (calculated as: 318,558 individuals notified, times 2 months, times $8.99 per month).

39. Negligence and Negligence *Per Se* Claims. Plaintiff alleges that "Empress owed a

[3] *See* https://lifelock.norton.com/products?inid=lifelock-lifelock-standard_subnav_products (last visited: October 18, 2022).
[4] *See* https://www.equifax.com/equifax-complete/Equifax/?CID=2_equifax%20credit%20monitoring_G_e&adID=502355 (last visited: October 18, 2022).
[5] *See* https://www.experian.com/lp/creditlock.html?bcd=ad_c_sem_427_515842009606 (last visited: October 18, 2022).

duty to Plaintiff and Class members to exercise reasonable care in safeguarding and protecting their PII/PHI in its possession, custody, and control," and "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 data security processes, controls, policies, protocols, and software and hardware systems to safeguard and protect PII/PHI entrusted to it." *Id*. at ¶¶ 48, 51.

40. Plaintiff alleges that as a result of Empress's "wrongful actions, inaction, and want of ordinary care that directly and proximately caused the [Security Incident], 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 [Security Incident]; (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 [Security Incident]; and (vii) overpayment for the services that were received without adequate data security." *Id*. at ¶ 54.

41. Plaintiff further alleges that Empress violated Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45, and the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), 42 U.S.C. § 1302d *et seq*., by, among other things, "failing to use reasonable measures to protect Plaintiff's and other Class members' PII/PHI and not complying with applicable industry standards," which constitutes negligence *per se*. Exhibit A at ¶¶ 56-59.

42. Plaintiff alleges that as a direct and proximate result of Empress's alleged negligence *per se*, "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 [Security Incident]; (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 [Security Incident]; and (vii) overpayment for the services that were received without adequate data security." *Id*. at ¶ 63.

43. The Complaint contains no allegations that would support or suggest the amount in actual damages to which he or any member of the Class are allegedly entitled for Empress's alleged negligence and negligence *per se*. But, as stated above, just two months of Norton360 with LifeLock for each member of the Class would amount to, at a minimum, $5,727,672.84. Plaintiff's other allegations do not support or suggest the amount in other economic and noneconomic damages, especially given that Plaintiff does not allege that either he or any member of the Class has suffered fraud, attempted fraud, or any specific out-of-pocket expenses as a result of the Security Incident. Therefore, Empress does not include in the calculation of the total amount in controversy Plaintiff's alleged damages arising from Empress's alleged negligent acts or omissions. However, when these alleged damages are combined with the cost of just two months of credit monitoring for the entire Class, the amount in controversy further exceeds CAFA's $5,000,000 threshold.

44. Breach-of-Fiduciary Duty Claim. Plaintiff alleges that (1) they "gave Empress their

PII/PHI in confidence," (2) "Empress' acceptance and storage of Plaintiff's and Class members' PII/PHI created a fiduciary relationship between them," and (3) Empress "breached that duty by," among other things, "failing to properly protect the integrity of the system containing Plaintiff's and Class members' PII/PHI." *Id*. at ¶¶ 65-66.

45. Plaintiff alleges that "[a]s 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 [Security Incident]; (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 [Security Incident]; and (vii) overpayment for the services that were received without adequate data security." *Id*. at ¶ 67.

46. Plaintiff's Complaint, however, contains no allegations that would support or suggest the amount in actual damages he or any member of the Class allegedly sustained as a result of Empress's alleged breach of fiduciary duty. Therefore, Empress does not include in the calculation of the total amount in controversy Plaintiff's or the Class's alleged breach-of-fiduciary-duty damages. However, when Plaintiff's and the Class's alleged breach-of-fiduciary-duty damages are combined with the cost of just two months of Norton360 with LifeLock credit monitoring for each member of the Class, the amount in controversy further exceeds CAFA's $5,000,000 threshold.

47. Unjust-Enrichment Claim. In the alternative to the breach of express and breach of

implied contract claims, Plaintiff alleges that "Plaintiff and Class members conferred a monetary benefit upon Empress in the form of monies paid for services," "Empress accepted . . . the benefits conferred upon it," and "[a]s 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." *Id*. at ¶¶ 83-86.

48. Plaintiff's Complaint, however, contains no allegations that would support or suggest the "value" or amount of "reasonable data privacy security practices and procedures" that they allegedly paid for versus what they allegedly received. Therefore, Empress does not include in the calculation of the total amount in controversy Plaintiff's or the Class's alleged unjust-enrichment damages. However, when Plaintiff's and the Class's alleged unjust-enrichment damages are combined with the cost of just two months of Norton360 with LifeLock credit monitoring for each member of the Class, the amount in controversy further exceeds CAFA's $5,000,000 threshold.

49. NYGBL Claim. Plaintiff alleges that "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 [NYGBL] § 349." *Id*. at ¶ 94.

50. Plaintiff further alleges that as a result of Empress's alleged violations of NYGBL § 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 [Security Incident]; (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 [Security Incident]; and (vii) overpayment for the services that were received without adequate data security." *Id*. at ¶ 97. Plaintiff seeks statutory damages on behalf of himself and the putative class in the amount of the greater of actual damages or $50 for each violation. *Id*. at ¶ 98.

51. Under the NYGBL § 349(h), "any person who has been injured by reason of any violation of this section may bring an action in his own name to enjoin such unlawful act or practice, an action to recover his actual damages or fifty dollars, whichever is greater, or both such actions. The court may, in its discretion, increase the award of damages to an amount not to exceed three times the actual damages up to one thousand dollars if the court finds the defendant willfully or knowingly violated this section. The court may award reasonable attorney's fees to a prevailing plaintiff."

52. Plaintiff's Complaint contains no allegations that would support or suggest the amount of "greater or actual damages" that Plaintiff and the putative class are entitled for Empress's alleged violations of NYGBL § 349. Thus, assuming the statutory damages amount of $50 per putative class member was valid and awarded, the amount in controversy would increase by $15,927,900 (calculated as: 318,558 individuals notified, times $50).

53. Total Amount in Controversy. Based on the discussion above, the amount in controversy based just on two months of Norton360 with LifeLock credit monitoring and the statutory damages under NYGBL § 349 for each member of the putative class, exceeds the $5,000,000 CAFA minimum before ever taking into account other forms of compensatory

damages, injunctive relief, or attorneys' fees, which, as discussed below, adds even more to the total amount in controversy.

54. Other Claims. In addition to the damages discussed above, Plaintiff also requests injunctive relief for himself and the Class. Exhibit A, Prayer for Relief. In certain circumstances, where the value of injunctive relief is ascertainable, the value can be considered when determining the amount in controversy. *Correspondent Servs. Corp. v. First Equities Corp. of Fla.*, 442 F.3d 767, 769 (2d Cir. 2006) ("In actions seeking [ ] injunctive relief, it is well established that the amount in controversy is measured by the value of the object of the litigation."); *Parker v. Riggio*, No. 10 Civ. 9504, 2012 WL 3240837, at *7 (S.D.N.Y. Aug. 6, 2012) (internal quotation marks and citation omitted) (The prevailing calculation method is the "plaintiff's viewpoint" approach, where the Court calculates the value to the plaintiff not the cost to the defendant.). Here, however, no allegations in the Complaint allow Empress to calculate the amount of Plaintiff's injunctive relief demand, and therefore, Empress has not included that value in the calculation of the total amount in controversy. Nevertheless, Empress underscores the allegations to the Court as further evidence that the amount in controversy exceeds the $5,000,000, as already established above.

NOTICE

55. Defendant is providing written notice of the removal of this case on Plaintiff's counsel, and a notice of filing this Notice of Removal will be promptly filed with the Clerk of the Supreme Court of New York, County of Westchester in accordance with 28 U.S.C. §1446(d).

CONCLUSION

WHEREFORE, Defendant removes the State Court Action from the Supreme Court of the State of New York, County of Westchester to the United States District Court for the Southern District of New York.

Dated: October 31, 2022
New York, New York

Respectfully Submitted,

/s/ Robyn Feldstein

Robyn Feldstein
BAKER & HOSTETLER LLP
45 Rockefeller Plaza
New York, New York 10111-0100
Tel: 212-589-4278
Fax: 212-589-4201
E-Mail: rfeldstein@bakerlaw.com
Attorney for Defendant

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

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

Plaintiff,

vs.

EMPRESS AMBULANCE SERVICE, LLC,

Defendant.

Case No.

CERTIFICATE OF SERVICE

I hereby certify that on October 31, 2022, I electronically filed a Notice of Removal of this action that was originally filed in the Supreme Court of New York, County of Westchester in this Court. Also, on October 31, 2022, I filed formal notice of the removal (including a copy of the Notice of Removal Papers filed in this Court) with the Supreme Court of New York, County of Westchester, using the NYSCEF electronic filing system, which sent notice of such filing to Plaintiff's counsel. On the same date, I also served a copy of the removal papers, the Rule 7.1 Disclosure Statement, Civil Cover Sheet, Electronic Case Filing Rules & Instructions and the Individual Practices of the assigned Judge via first class mail to Plaintiff's counsel below:

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

/s/ Robyn Feldstein
Robyn Feldstein

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

EXHIBIT B

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. SUMMONS

To the above-named Defendants:

You are hereby summoned and required to answer the attached complaint of the Plaintiff in this action and to serve a copy of your answer upon the attorneys for the Plaintiff at the address stated below.

If this summons was personally delivered to you in the State of New York, you must serve the answer within 20 days after such service, excluding the day of service. If this summons was not personally delivered to you in the State of New York, you must serve the answer within 30 days after service of the summons is complete, as provided by law.

If you do not serve an answer to the attached complaint within the applicable time limitation stated above, a judgment may be entered against you, by default, for the relief demanded in the complaint.

Plaintiff designates Westchester County as the place of trial.

The basis of venue is Defendant Empress Ambulance Service, LLC's principal place of business which is in Westchester County, Yonkers, New York.

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

P7370661

AFFIDAVIT OF SERVICE

FINKELSTEIN, BLANKINSHIP, FREI-PEARSON & GARBER, LLP Faina Simon

SUPREME COURT WESTCHESTER COUNTY STATE OF NEW YORK

SALVATORE J. CONTRISTANO, INDIVIDUALLY, AND ON BEHALF OF ALL OTHERS SIMILARLY SITUATED

PLAINTIFF

- vs -

EMPRESS AMBULANCE SERVICE, LLC

DEFENDANT

index No. 65746/2022
Date Filed
File No.
Court Date:
AFFIDAVIT OF SERVICE

STATE OF New York, COUNTY OF Westchester :SS:

Keith Hawthorne, being duly sworn deposes and says:

Deponent is not a party herein, is ver 18 years f age and resides in the State of New York.

On October 10, 2022 at 9:45 Am,

at 722 NEPPERHAN AVENUE YONKERS, NY 10703,

deponent served the within **SUMMONS, CLASS ACTION COMPLAINT AND CLASS ACTION JURY TRIAL DEMANDED** on: **EMPRESS AMBULANCE SERVICE, LLC**, the **DEFENDANT** therein named.

___#1 INDIVIDUAL By delivering a true copy of each to said recipient personally; dep nent knew the person served to be the person described as said person therein.

✓ #2 CORPORATION By delivering a true copy each personally to Marie Hart, who provided verbal confirmation that he or she is authorized by appointment r law to receive service on behalf of the **DEFENDANT**.

Deponent knew the person so served to be the Administrative Assistant of the c rporation, and authorized to accept service on behalf f the corporation.

___#3 SUITABLE AGE PERSON By delivering a true copy of each to _____ a pers n of suitable age and discretion.
Said premises is **DEFENDANT's:** [ ] actual place f business [ ] dwelling house (usual place of abode) within the state.

___#4 AFFIXING TO DOOR By affixing a true copy of each to the door of said premises, which is **DEFENDANT's:** [ ] actual place of business [ ] dwelling house (usual pla e f abode) within the state.

Deponent was unable, with due diligence to find **DEFENDANT** r a pers n of suitable age and discretion, having called thereat

r the	_____	day f	_____ at _____
r the	_____	day f	_____ at _____
r the	_____	day of	_____ at _____
r the	_____	day of	_____ at _____

Address confirmed by

___#5 MAIL COPY ~~On _____ I deposited in the United States mail a true copy of the~~ aforementioned documents properly enclosed and sealed in a post-paid wrapper addressed to the above address. Copy mailed 1st class mail marked personal and confidential not indicating on the outside thereof by return address or otherwise that said notice is from an attorney or concerns an action against the person to be served.

✓ #6 DESCRIPTION (USE WITH #1, 2 OR 3) Deponent describes the person served as aforesaid to the best of deponent's ability at the time and circumstances of the service as follows.

Sex: Female Color: White Hair: Brown
Age: 45-55 Height: 5'4"-5'7" Weight: 150-175
OTHER IDENTIFYING FEATURES: _____

___#7 WITNESS FEES The authorized witness fee and / or traveling expenses were paid (tendered) to the **DEFENDANT** in the amount of $_____

___#8 MILITARY SRVC Deponent asked person spoken to whether the **DEFENDANT** was presently in military service of the United States Government r of the State f _____ and was informed that **DEFENDANT** was not.

___#9 OTHER

NOTARY NAME & DATE October 12, 2022 KRYSTAL COUNCIL
Notary Public, State of New York
Qualified in Westchester County
Reg. No. 01CO6356347
My Commission Expires 3/27/2025

Keith Hawthorne
Lexitas
1235 BROADWAY 2ND FLOOR
NEW YORK, NY 10001
Reference No: 3-FNFG-7370661

EXHIBIT C

*<< Return to **Search Results***

65746/2022 - Westchester County Supreme Court

Short Caption: **Salvatore J. Contristano v. Empress Ambulance Service, LLC**
Case Type: **Torts - Other (Data Breach)**
Case Status: **Pre-RJI**
eFiling Status: **Partial Participation Recorded**

Narrow By Options

Document Type: Please select... Filed By:
Please select...
Motion Info: Filed Date:
thru
Document Number:
Display Document List with Motion Folders

Sort By: Doc #

#	Document	Filed By	Status
1	SUMMONS + COMPLAINT *Summons and Class Action Complaint*	Frei-Pearson, J. Filed: 09/28/2022 *Received: 09/28/2022*	**Processed** Confirmation Notice
2	AFFIRMATION/AFFIDAVIT OF SERVICE	Frei-Pearson, J. Filed: 10/20/2022 *Received: 10/20/2022*	**Processed** Confirmation Notice

EXHIBIT D

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

JOHN FINN, individually and on behalf of all others similarly situated, Plaintiff, v. EMPRESS AMBULANCE SERVICES, INC., d/b/a EMPRESS EMS Defendant.	Case No. CLASS ACTION JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiff John Finn ("Plaintiff"), individually and on behalf of all others similarly situated (collectively, "Class members"), by and through his attorneys, brings this Class Action Complaint against Defendant Empress Ambulance Service, Inc. d/b/a Empress EMS ("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' private and confidential information, including names, dates of service, Social Security numbers, and insurance information ("PII/PHI").

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 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' 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 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 New York residents whose PII/PHI was exposed as a result of the Data Breach, which Empress learned of on or about July 14, 2022 and first publicly acknowledged on or about September 9, 2022.

6. Plaintiff, on behalf of himself and all other Class members, asserts claims for negligence, negligence per se, breach of fiduciary duty, breach of implied contract, unjust enrichment, and violations New York GBL § 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 Finn is a New York resident. He provided his PII/PHI 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.

8. Defendant Empress EMS, Inc. 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

9. This Court has subject matter jurisdiction over this action pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332 (d), because the matter in controversy, exclusive of interest and costs, exceeds the sum or value of five million dollars ($5,000,000.00), and is a class action involving 100 or more class members. This Court has supplemental jurisdiction over the state law claims pursuant to 28 U.S.C. § 1367.

10. This Court has personal jurisdiction over Empress because Empress is a corporation organized under the laws of New York and has its principal place of business at 722 Nepperhan Ave, Yonkers, New York, 10703.

11. Venue properly lies in this judicial district pursuant to 28 U.S.C. § 1391 because, *inter alia,* the events or omissions giving rise to the conduct alleged herein occurred in, were directed to, and/or emanated from this district; Defendant's principal place of business is in this district; Defendant transacts substantial business and has agents in this district; a substantial part of the conduct giving rise to Plaintiff's claims occurred in this judicial district; and because Plaintiff resides within this district.

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. Plaintiff 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 posted on Empress's website states that the information that was accessed

[1] Empress Emergency Medical Services, *Customer Service*, EMPRESSEMS.COM, http://empressems.com/files/empressprivacy.pdf (last visited Sept. 20, 2022).

included: "[P]atient names, dates of service, insurance information, and in some instances, Social Security numbers."[2]

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 Plaintiff's 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 is 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, and although a record number of data breaches were reported, the impact of breaches continues to be underreported overall, and underrepresented to the public.[5]

21. PII/PHI is a valuable property right.[6] The value of PII/PHI as a commodity is

---

[2] Empress Emergency Medical Services, *Security Incident*, EMPRESSEMS.COM, http://empressems.com/securitynotice.pdf (last visited Sept. 20, 2022).

[3] Protenus, *2021 Breach Barometer*, PROTENUS.COM, https://www.protenus.com/resources/2021-breach-barometer (last accessed Sept. 21, 2022).

[4] Protenus, *2020 Breach Barometer*, PROTENUS.COM, https://www.protenus.com/resources/2020-breach-barometer (last accessed Sept. 21, 2022).

[5] Protenus, 2022 Brach Barometer, PROTENUS.COM, https://www.protenus.com/resources/2022-breach-barometer (last accessed Sept. 21, 2022)

[6] *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.

measurable.[7] "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."[8] American companies are estimated to have spent over $19 billion on acquiring personal data of consumers in 2018.[9] 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, 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."[10] A cybercriminal who steals a person's PHI can end up with as many as "seven to ten personal identifying characteristics of an individual."[11] A study by Experian found that the "average total cost" of medical identity theft is "about $20,000" per incident, and that a majority

---

7 *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.

8 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.

9 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/.

10 *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.").

11 *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.[12]

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.[13] 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.[14]

25. Criminals can use stolen PII/PHI to extort a financial payment by "leveraging details specific to a disease or terminal illness."[15] 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."[16]

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

---

12 *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.

13 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.

14 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.

15 *What Happens to Stolen Healthcare Data*, *supra* at n.10.

16 *Id.*

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."[17]

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.[18]

29. Identity thieves use personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[19] 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 debit card

---

17 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.

18 *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 Nov. 15, 2021).

19 The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 16 C.F.R. § 603.2. 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*.

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.[20]

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.[21]

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.[22]

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 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.

---

[20] *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/.

[21] *See* Federal Trade Commission, *Warning Signs of Identity Theft*, IDENTITYTHEFT.GOV https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft (last accessed Sept. 21, 2022).

[22] Identity Theft Resource Center, *2021 Consumer Aftermath Report*, IDENTITY THEFT RESOURCE CENTER (2021), https://www.idtheftcenter.org/identity-theft-aftermath-study/ (last accessed Sept. 20, 2022).

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."[23]

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."[24] It "is also more difficult to detect, taking almost twice as long as normal identity theft."[25] In warning consumers on the dangers of medical identity theft, the FTC states that an identity thief may use PII/PHI "to see a doctor, get prescription drugs, buy medical devices, submit claims with your insurance provider, or get other medical care."[26] The FTC also warns, "If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."[27]

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:

- Changes to their health care records, most often the addition of falsified information, through improper billing activity or activity by imposters. These

---

23 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/.

24 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

25 *See* Federal Bureau of Investigation, *Health Care Systems and Medical Devices at Risk*…, *supra* at n.14.

26 *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 Sept. 20, 2022).

27 *Id*.

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.[28]

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.[29]

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

---

[28] *See* Pam Dixon and John Emerson, *The Geography of Medical Identity Theft*, *supra* at 24.

[29] 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.

Damages Sustained by Plaintiff and the Other Class Members

38. Plaintiff and all other Class members have suffered injury and damages, including, but not limited to: (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; and/or (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of identity theft and medical identity theft they face and will continue to face.

CLASS ALLEGATIONS

39. This action is brought and may be properly maintained as a class action pursuant to Federal Rule of Civil Procedure 23(a) and (b).

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

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

41. Excluded from the Class is Empress 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).

42. 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.

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 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 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 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.

46. 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.

47. 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.

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

50. Empress owed a duty to Plaintiff 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 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 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 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.

54. 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.

55. But for Empress's negligent conduct or breach of the above-described duties owed to Plaintiff 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, Plaintiff 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; and/or (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.

COUNT II

NEGLIGENCE PER SE

57. Plaintiff realleges and incorporates 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 Plaintiff's 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 Plaintiff 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. 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.

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 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.

65. The injury and harm that Plaintiff 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. Plaintiff and Class members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, *inter alia*: (i) a substantially increased 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; and/or (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.

COUNT III

BREACH OF FIDUCIARY DUTY

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

67. 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's 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.

68. 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.

69. As a direct and proximate result of Empress's 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's possession; and (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII/PHI compromised as a result of the Data Breach.

COUNT IV

BREACH OF IMPLIED CONTRACT

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

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

72. Pursuant to these implied contracts, Plaintiff 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 Plaintiff understood that Empress would: (1) provide medical 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.

73. 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 Notice. Had Plaintiff 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.

74. Plaintiff 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.

75. 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.

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

77. Plaintiff 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; and/or (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.

COUNT V

UNJUST ENRICHMENT

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

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

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

81. 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' PHI, as this was used to facilitate payment.

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

83. 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.

84. 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 VI

VIOLATIONS OF THE NEW YORK DECEPTIVE ACTS AND PRACTICES ACT N.Y. Gen. Bus. Law § 349 ("GBL")

85. Plaintiffs re-allege and incorporate by reference the preceding paragraphs.

86. Plaintiff Finn and New York Class members are "persons" within the meaning of the GBL. N.Y. Gen. Bus. Law § 349(h).

87. 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).

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

89. Empress violated the GBL through its promise to protect and subsequent failure to adequately safeguard and maintain Plaintiff and Class members' PII/PHI. Empress failed to notify Plaintiff 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 Plaintiff and class members.

90. As a result of Empress's above-described conduct, Plaintiff and the Class have suffered damages from the disclosure of their information to unauthorized individuals.

91. The injury and harm that Plaintiff and the other Class members suffered was the direct and proximate result of Empress's violations of the GBL. Plaintiff and Class members have

suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, *inter alia*: (i) a substantially increased 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; and/or (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.

92. Plaintiff Finn, individually and on behalf of the New York Class, requests that this Court enter such orders or judgments as may be necessary to enjoin Empress from continuing its unfair and deceptive practices.

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

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 22, 2022

Respectfully submitted,

/s/ Tina Wolfson

TINA WOLFSON (NY Bar # 5436043)
twolfson@ahdootwolfson.com
DEBORAH DE VILLA (NY Bar # 5724315)
ddevilla@ahdootwolfson.com
AHDOOT & WOLFSON, PC
2600 W. Olive Avenue, Suite 500
Burbank, CA 91505-4521
Telephone: 310.474.9111
Facsimile: 310.474.8585

ANDREW W. FERICH*
aferich@ahdootwolfson.com
AHDOOT & WOLFSON, PC
201 King of Prussia Road, Suite 650
Radnor, PA 19087
Telephone: 310.474.9111
Facsimile: 310.474.8585

Attorneys for Plaintiff

**pro hac vice* to be submitted