UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

JOSH COLON, on behalf of himself and all others similarly situated, Plaintiff, vs. EMPRESS AMBULANCE SERVICE, LLC, d/b/a EMPRESS EMERGENCY MEDICAL SERVICES, Defendant.	Case No. **NOTICE OF REMOVAL**

Pursuant to 28 U.S.C. §§1441, 1446, and 1453, Defendant Empress Ambulance Service, LLC, d/b/a Empress Emergency Medical Services, files this Notice of Removal of Plaintiff's civil action from the Supreme Court of the State of New York, County of Bronx, 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 October 11, 2022, Plaintiff Josh Colon ("Plaintiff") filed a purported class action complaint in the Supreme Court of the State of New York, County of Bronx, Case No. 815075/2022E (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, d/b/a Empress Emergency Medical Services ("Empress" or "Defendant") on October 13, 2022. A true and correct copy of the Summons is attached as **Exhibit B**.

3. The Complaint alleges that Empress failed to properly safeguard its patient's sensitive personal information and seeks damages and injunctive relief on behalf of Plaintiff and putative class members.

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 13, 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 Bronx.

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 ¶¶ 14-25. 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 ¶ 114 ("Plaintiff

brings this nationwide class action . . .").

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

15. "Plaintiff brings this class action against [Empress] for failing to secure and safeguard" the "personally identifiable information [('PII')] and protected health information ('PHI') . . . (collectively, 'Personal Information') of more than 300,000 current or former patients," including their "name, dates of service, Social Security numbers, and insurance information." Exhibit A at ¶¶ 1, 4. Plaintiff alleges that "[o]n or around July 14, 2022, [Empress] determined that unauthorized, unknown third parties had gained access to [Empress's] internal system on May 26, 2022, via a malicious internet protocol address and subsequently copied and exfiltrated a subsect of files on July 13, 2022," (the "Security Incident"). *Id*. at ¶ 3. Plaintiff further alleges that the Security Incident occurred as a result of Empress's failure to: "(i) adequately protect the Personal Information of Plaintiff and Class Members; (ii) warn Plaintiff and Class Members of its inadequate information security practices; and (iii) avoid sharing the Personal Information of Plaintiff and Class Members without adequate safeguards." *Id*. at ¶ 11.

16. Based on these allegations, Plaintiff asserts five causes of action against Empress: (1) negligence, (2) negligence *per se*, (3) breach of implied contract, (4) breach of confidence, and (5) 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 ¶ 114. Plaintiff defines the Class as: "[a]ll individuals whose Personal Information was compromised during the [Security Incident] referenced in the Website Notice published by [Empress] on or around September 9, 2022." *Id*.

18. Plaintiff alleges that "[w]hile the exact number of Class members is unknown to Plaintiff at this time, Plaintiff is informed and believes that there are at least hundreds of thousands

Class Members." *Id*. at ¶ 120. Plaintiff also alleges that "the attacker compromised . . . Personal Information . . . of more than 300,000 current or former patients of [Empress]." *Id*. at ¶ 4.

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 a citizen of New York." Exhibit A at ¶ 14. Accordingly, as alleged in the Complaint, Plaintiff is a citizen of New York.

23. Plaintiff also seeks to represent a class that (1) includes "[a]ll individuals whose

Personal Information was compromised during the [Security Incident] referenced in the Website Notice published by [Empress] on or around September 9, 2022," *id*. at ¶ 115, 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*, 292 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, Empress is a limited liability company organized under the laws of Delaware, and Empress's principal place of business is in New York. *See* Exhibit A at ¶ 16.

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 the 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, Connecticut, Florida, New York, 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 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

[1] In addition, after the filing of the Finn Class Action and before the filing 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).

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

[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.

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-Implied-Contract Claim. Plaintiff alleges that "Plaintiff and Class members entered into implied contracts with [Empress]," and, in exchange for money, Empress "agreed to," among other things, "safeguard and protect [their personal] information." Exhibit A at ¶ 171. Plaintiff further alleges that Empress "breached the implied contracts it made with Plaintiff and the [ ] Class by making their Personal Information accessible from the internet" and by, among other things, "failing to safeguard and protect their Personal Information." *Id*. at ¶ 175.

35. As a result of the alleged breach of implied contract, Plaintiff claims that he and the Class members were damaged because they "are now subject to the present and continuing risk of fraud, and are suffering (and will continue to suffer) the ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the diminished value of services provided by [Empress]; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic and non-economic harm." *Id*. at ¶ 191.

36. 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 implied contract. However, because Plaintiff seeks damages based on an "ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse" and "expenses and/or time spent on credit monitoring and identity theft insurance" for which they are "entitled and demand" 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.

37. 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).

---

[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).

38. Negligence and Negligence *Per Se* Claims. Plaintiff alleges that Empress owed a duty to Plaintiff and Class members "to exercise reasonable care in safeguarding, securing, and protecting [their PII/PHI]," and Empress "breached its duties to Plaintiff and the [ ] Class by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the Personal Information of Plaintiff and the [ ] Class during the time the Personal Information was within [Empress's] possession or control." *Id*. at ¶¶ 130, 144.

39. Plaintiff alleges that "as a direct and proximate result of Empress's negligence, Plaintiff and the . . . Class have suffered and will suffer the continued risks of exposure of their Personal Information," and "are entitled to and demand actual, consequential, and nominal damages." *Id*. at ¶¶ 153-54.

40. Plaintiff further alleges that Empress violated Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45, the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), 42 U.S.C. § 1302d *et seq*., and the Health Information Technology Act ("HITECH"), 42 U.S.C. § 17921, by, among other things, "failing to use reasonable measures to protect [Personal Information]," which constitutes negligence *per se*. *Id*. at ¶¶ 156-64.

41. Plaintiff alleges that as a direct and proximate result of Empress's alleged negligence *per se*, "Plaintiff and the [ ] Class have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their Personal Information is used; (iii) the compromise, publication, and/or theft of their Personal Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Personal Information; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the [Security Incident], including but not limited to efforts

spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their Personal Information, which remain in [Empress's] possession and are subject to further unauthorized disclosures so long as [Empress] fails to undertake appropriate and adequate measures to protect the Personal Information of Plaintiff and the . . . Class; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Personal Information compromised as a result of the [Security Incident] for the remainder of the lives of Plaintiff and the . . . Class." *Id*. at ¶ 165.

42. 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.

43. Breach-of-Confidence Claim. Plaintiff alleges that Plaintiff and the Class: (1) "provided their PII to [Empress] with the explicit and implicit understandings that [Empress] would protect and not permit the PII to be disseminated to any unauthorized parties," (2) that, as a

result of Empress's "failure to prevent and avoid the [Security Incident]," Plaintiff's and the Class's "PII was disclosed and misappropriated to unauthorized third parties beyond [their] confidence, and without their express permission," and (3) as "a direct and proximate cause of [Empress's] actions and/or omissions, Plaintiff and the [ ] Class have suffered damages." Exhibit A at ¶¶ 194-99.

44. Plaintiff alleges that "[a]s a direct and proximate result of [Empress's] breach of its confidence . . . , Plaintiff and the . . . Class have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the [Security Incident], including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remain in [Empress's] possession and is subject to further unauthorized disclosures so long as [Empress] fails to undertake appropriate and adequate measures to protect the PII of Plaintiff and the Nationwide Class; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the [Security Incident] for the remainder of the lives of Plaintiff and the . . . Class." *Id*. at ¶ 203.

45. Plaintiff's Complaint, however, contains no allegations that would support or suggest the amount in actual damages he or any member of the Class are allegedly sustained as a result of Empress's alleged breach of confidence. Therefore, Empress does not include in the

calculation of the total amount in controversy Plaintiff's or the Class's alleged breach-of-confidence damages. However, when Plaintiff's and the Class's alleged breach-of-confidence 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.

46. NYGBL Claim. Plaintiff alleges that "Empress has engaged in unlawful practices within the meaning of NYGBL § 349" and "violated NYGBL § 349 by misrepresenting, both by affirmative conduct and by omission, the safety of Empress's storage and services" and "by failing to implement reasonable and appropriate security measures." *Id*. at ¶¶ 205-12.

47. Plaintiff further alleges that as a result of Empress's alleged violations of NYGBL § 349, "Plaintiff and Class Members suffered damages including, but not limited to: unauthorized use of their Personal Information; theft of their personal and financial information; costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts; damages arising from the inability to use their Personal Information; costs associated with time spent and the loss of productivity or the enjoyment of one's life from taking time to address an attempt to ameliorate, mitigate and deal with the actual and future consequences of the [Security Incident], including finding fraudulent charges, purchasing credit monitoring and identity theft protection services, initiating and monitoring credit freezes, and the stress, nuisance, and annoyance of dealing with all issues resulting from the [Security Incident]; the imminent and certainly impending injury flowing from potential fraud and identity theft posed by their Personal Information being placed in the hands of criminals; damages to and diminution in value of their Personal Information entrusted to Empress; and the loss of Plaintiff's and Class Members' privacy." *Id*. at ¶ 219.

48. 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."

49. Plaintiff's Complaint contains no allegations that would support or suggest the amount of "great 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).

50. 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.

51. 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 Class Action 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

52. 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 Bronx 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 Bronx 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

JOSH COLON, on behalf of himself and all others similarly situated,

Plaintiff,

vs.

EMPRESS AMBULANCE SERVICE, LLC, d/b/a EMPRESS EMERGENCY MEDICAL SERVICES,

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 Bronx 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 Bronx, 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:

Brian P. Murray, Esq.
GLANCY PRONGAY & MURRAY LLP
230 Park Avenue, Ste. 358
New York, New York 10169
Tel.: (212) 682-5340
Fax: (212) 884-0988
bmurray@glancylaw.com

Jean S. Martin
Francesca Kester
MORGAN & MORGAN COMPLEX
LITIGATION GROUP

201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
(813) 223-5505
jeanmartin@ForThePeople.com
fkester@ForThePeople.com

/s/ Robyn Feldstein
Robyn Feldstein

EXHIBIT A

SUPREME COURT OF THE STATE OF NEW YORK
BRONX COUNTY

JOSH COLON, on behalf of himself and all others similarly situated, Plaintiff, v. EMPRESS AMBULANCE SERVICE, LLC, d/b/a/ EMPRESS EMERGENCY MEDICAL SERVICES, Defendant.	Index No. **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Josh Colon ("Plaintiff"), individually and on behalf of all others similarly situated ("Class Members"), brings this Class Action Complaint against Empress Ambulance Service, LLC, d/b/a Empress Emergency Medical Services ("Empress" or "Defendant"), and alleges, upon personal knowledge as to his own actions and his counsels' investigations, and upon information and belief as to all other matters, as follows:

I. INTRODUCTION

1. Plaintiff brings this class action against Defendant for its failure to properly secure and safeguard sensitive information that Defendant's patients entrusted to it, including, without limitation: name, dates of service, Social Security numbers, and insurance information.[1]

2. Empress is a medical transportation and services provider based in Yonkers, New York.

3. On or around July 14, 2022, Defendant determined that unauthorized, unknown

[1] Exhibit 1 (*Website Notice* posted on the Empress EMS website).

third parties had gained access to Defendant's internal system on May 26, 2022, via a malicious internet protocol address and subsequently copied and exfiltrated a subset of files on July 13, 2022. The intrusion remained undetected until July 14, 2022 (the "Data Breach").

4. During the Data Breach, the attacker compromised the personally identifiable information[2] and protected health information ("PHI") (collectively, "Personal Information") of more than 300,000 current or former patients of Defendant.

5. Although Defendant failed to disclose additional details of the Data Breach to the public, upon information and belief, the cyberattack was perpetuated by a ransomware group called "Hive," which has already published Empress patient Personal Information on the Dark Web[3] and shared it with other sources.[4]

6. On or around September 9, 2022, Defendant finally notified the U.S. Department of Health and Human Services Office for Civil Rights ("HHS") of the Data Breach and indicated that 318,558 individuals were impacted.

7. On or around September 9, 2022, Defendant also began notifying Plaintiff and Class Members of the Data Breach and cautioned them to review their healthcare statements for instances of fraud. According to Defendant's Website Notice, Defendant will continue to notify Class Members of the Data Breach until October 9, 2022.

---

[2] Personally identifiable information ("PII") generally incorporates information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information. 2 CFR § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual. PII also is generally defined to include certain identifiers that do not on their face name an individual, but that are considered to be particularly sensitive and/or valuable if in the wrong hands (for example, Social Security number, passport number, driver's license number, financial account number).

[3] *See* https://www.bleepingcomputer.com/news/security/new-york-ambulance-service-discloses-data-breach-after-ransomware-attack/ (last accessed Sept. 22, 2022).

[4] *See* https://www.databreaches.net/ny-empress-ems-hit-by-hive-ransomware/ (last accessed Sept. 22, 2022).

8. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Personal Information, Defendant assumed legal and equitable duties to those individuals.

9. The exposed Personal Information of Plaintiff and Class Members can be sold on the dark web. Hackers can access and then offer for sale the unencrypted, unredacted Personal Information to criminals. As already acknowledged by Defendant, Plaintiff and Class Members face a lifetime risk of identity theft, which is heightened here by the loss of Social Security numbers.

10. This Personal Information was compromised due to Defendant's negligent and/or careless acts and omissions and the failure to protect the Personal Information of Plaintiff and Class Members.

11. Plaintiff brings this action on behalf of all persons whose Personal Information was compromised as a result of Defendant's failure to: (i) adequately protect the Personal Information of Plaintiff and Class Members; (ii) warn Plaintiff and Class Members of its inadequate information security practices; and (iii) avoid sharing the Personal Information of Plaintiff and Class Members without adequate safeguards. Defendant's conduct amounts to negligence and violates federal and state statutes.

12. Plaintiff and Class Members have suffered injury as a result of Defendant's conduct. These injuries include: (i) lost or diminished value of their Personal Information; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Personal Information; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time, and significantly (iv) the continued and certainly an increased risk to their Personal

Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; (b) may remain backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Personal Information; (c) likely remains freely available for cybercriminals to use and abuse on the Dark Web.

13. Defendant disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, or negligently failing to take and implement adequate and reasonable measures to ensure that Plaintiff's and Class Members' Personal Information was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required and appropriate protocols, policies and procedures regarding the encryption of data, even for internal use. As the result, the Personal Information of Plaintiff and Class Members was compromised through disclosure to and exfiltration by an unknown and unauthorized third party. Plaintiff and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

II. PARTIES

14. Plaintiff Josh Colon is a citizen of New York residing in Bronx County, New York. Plaintiff was, at all relevant times, a patient of Defendant whose Personal Information was retained on Defendant's systems.

15. On or about September 18, 2022, Plaintiff received a Notice of Data Breach in the mail from Defendant.

16. Defendant Empress is an emergency medical response company with its principal place of business located at 722 Nepperhan Avenue, Yonkers, New York, 10703.

17. The true names and capacities of persons or entities, whether individual, corporate, associate, or otherwise, who may be responsible for some of the claims alleged herein are currently unknown to Plaintiff. Plaintiff will seek leave of court to amend this complaint to reflect the true names and capacities of such other responsible parties when their identities become known.

18. All of Plaintiff's claims stated herein are asserted against Defendant and any of its owners, predecessors, successors, subsidiaries, agents, and/or assigns.

III. JURISDICTION AND VENUE

19. This Court has original jurisdiction over this matter because Defendant is at home in this State.

20. Defendant is subject to the jurisdiction of this Court because Plaintiff resides in this county. Additionally, the Defendant regularly and systematically conducts business and provides medical care in this county. Defendant also regularly and systematically collects and stores personal and medical information in the course of providing medical care to patients or employment to employees in this county, including Plaintiff and members of the putative class.

21. Venue is appropriate in Bronx County pursuant to NY CPLR § 503 (2012); a substantial part of the acts and omissions giving rise to this lawsuit occurred in this county.

IV. FACTUAL ALLEGATIONS

Background

22. Empress is an emergency care and medical transportation provider based in Yonkers, New York.

23. Originally founded in 1985 and based in the City of Yonkers, Empress has concentrated its efforts on providing "state of the art patient care and 9-1-1 emergency response" to Yonkers and neighboring communities. Empress also has emergency and non-emergency

contracts throughout New York with hospitals, correctional institutions and private care facilities.[5]

24. Defendant claims that its personnel is of "the highest caliber in the industry" and that its "24-hour communications center houses one of the most advanced computer aided systems in the region."[6]

25. Defendant collects and stores some of Plaintiff's and Class Members' most sensitive and confidential information, including their Social Security numbers, as a condition of rendering medical services.

26. On its website, Empress has a posted Privacy Policy that states, in part: "We are the sole owners of the information collected on this site. We will use your information to respond to you, regarding the reason you contacted us. We will not share your information with any third party outside of our organization, other than necessary to fulfill your request.…We take precautions to protect your information. We use encryption to protect sensitive information transmitted online, we also protect your information offline. Only employees who need the information to perform a specific job (for example billing or customer service) are granted access to personally identifiable information. The computers/servers in which we store personally identifiable information are kept in a secure environment."[7]

27. Plaintiff and Class Members relied on this sophisticated Defendant's promises to keep their Personal Information confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information. Plaintiff and Class Members demand security to safeguard their Personal Information.

28. Defendant had a duty to adopt reasonable measures to protect Plaintiff's and Class

[5] *See* http://empressems.com/about.html (last accessed Sept. 22, 2022).
[6] *See id.*
[7] *See* http://empressems.com/privacy.html (last accessed Sept. 22, 2022)

Members' Personal Information from involuntary disclosure to third parties.

29. The healthcare sector is a favored target by cybercriminals, yet recent studies, including one by the Massachusetts Institute of Technology, found medical centers lagged behind other businesses in safeguarding their computer systems.[8] A Tenable study analyzing healthcare sector breaches from January 2020 to February 2021 reported that "records were confirmed to have been exposed in nearly 93% of the breaches."[9]

30. This case involves a breach of a computer system by a known cybercriminal group called Hive and accordingly resulted in the unauthorized access, disclosure, and/or acquisition of the Personal Information of Plaintiff and Class Members to unknown third-parties. As a result of Defendant's failure to implement and follow basic security procedures, the Personal Information of Plaintiff and Class Members was more likely than not accessed, disclosed, and/or acquired and is now in the hands of criminals.

31. Once information is placed onto the internet, it is virtually impossible to remove. Plaintiff and Class Members now and will forever face a substantial increased risk of identity theft. Consequently, Plaintiff and Class Members have had to spend, and will continue to spend, significant time and money in the future to protect themselves due to Defendant's failures.

32. Additionally, as a result of Defendant's failure to follow industry standard security procedures, Plaintiff and Class Members received only a diminished value of the services Defendant was to provide.

---

[8] Jane Musgrave, *How two Palm Beach County Hospitals used paper to cope with a cyber attack,* PALM BEACH POST (Apr. 30, 2022), https://www.palmbeachpost.com/story/news/healthcare/2022/04/30/west-palm-beach-hospitals-handle-cyber-attack-ransomware-hive/9575400002/.

[9] Tenable Security Response Team, *Healthcare Security*, TENABLE (Mar. 10, 2021), https://www.tenable.com/blog/healthcare-security-ransomware-plays-a-prominent-role-in-covid-19-era-breaches.

33. By obtaining, collecting, using, and deriving a benefit from the Personal Information of Plaintiff and Class Members, Defendant assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access, intrusion, and/or acquisition.

34. Moreover, Defendant now puts the burden squarely on Plaintiff and Class Members to enroll in the credit monitoring services, among other steps Plaintiff and Class Members must take to protect themselves. Time is a compensable and valuable resource in the United States. According to the U.S. Bureau of Labor Statistics, 55.5% of U.S.-based workers are compensated on an hourly basis, while the other 44.5% are salaried.[10]

35. According to the U.S. Bureau of Labor Statistics' 2018 American Time Use Survey, American adults have only 36 to 40 hours of "leisure time" outside of work per week;[11] leisure time is defined as time not occupied with work or chores and is "the time equivalent of 'disposable income.'"[12] Usually, this time can be spent at the option and choice of the consumer, however, having been notified of the Data Breach, consumers now have to spend hours of their leisure time self-monitoring their accounts, communicating with financial institutions and government entities, and placing other prophylactic measures in place to attempt to protect themselves.

---

[10] U.S. BUREAU OF LABOR STATISTICS, Wage Worker Survey, *available at* https://www.bls.gov/opub/reports/minimum-wage/2020/home.htm#:~:text=In%202020%2C%2073.3%20million%20workers,wage%20of%20%247.25%20per%20hour (last visited Aug. 2, 2022); *see also* U.S. BUREAU OF LABOR STATISTICS, *Average Weekly Wage Data, available at* https://data.bls.gov/cew/apps/table_maker/v4/table_maker.htm%23type=1&year=2021&qtr=3&own=5&ind=10&supp=0 (last visited Aug. 2, 2022) (finding that on average, private-sector workers make $1,253 per 40-hour work week.).

[11] *See* https://www.cnbc.com/2019/11/06/how-successful-people-spend-leisure-time-james-wallman.html (last visited Aug. 2, 2022).

[12] *Id.*

36. Plaintiff and Class Members are now deprived of the choice as to how to spend their valuable free hours and seek renumeration for the loss of valuable time as another element of damages.

The Data Breach

37. On or about September 9, 2022, Defendant posted on its website that it was the victim of a ransomware attack on July 14, 2022 ("Website Notice"). The Website Notice read, in part:

> At Empress EMS, we are committed to protecting the privacy and security of our patients' information. Regrettably, we recently identified and addressed a cybersecurity incident involving some of that information. This letter explains the incident, measures we have taken, and some steps you may consider taking in response.
>
> On July 14, 2022, we identified a network incident resulting in the encryption of some of our systems. We took measures to contain the incident, reported it to law enforcement, and we conducted a thorough investigation with the assistance of a third-party forensic firm. Our investigation determined that an unauthorize party first gained access to certain systems on our network on May 26, 2022 and then copied a small subset of files on July 13, 2022.
>
> Some of these files contained patient names, dates of service, insurance information, and in some instances, Social Security numbers. Empress EMS is mailing letters to affected individuals and offering eligible individuals credit monitoring services. We're also recommending that patients review their healthcare statements for accuracy and contact their provider if they see services they did not receive. If you believe you may be affected but do not receive a letter by October 9, 2022, please contact our dedicated external call center at 844-690-1251, Monday through Friday 9:00 a.m. to 9:00 p.m. Eastern Time, except major US Holidays.
>
> We take this matter very seriously and deeply regret any inconvenience to our patients. To help prevent something like this from happening again, we strengthened the security of our systems and will continue enhancing our protocols to further safeguard the information in our care.

38. On or about September 9, 2022, Defendant notified the U.S. Department of Health and Human Services Office for Civil Rights of the Data Breach. Defendant reported to the HHS that 318,558 individuals were impacted by the Data Breach.

39. In response to the Data Breach, Defendant claims that it " took measures to contain the incident, reported it to law enforcement, and [] conducted a thorough investigation with the assistance of a third-party forensic firm." However, the details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure a breach does not occur again have not been shared with regulators or Plaintiff and Class Members, who retain a vested interest in ensuring that their information remains protected.

40. Indeed, additional details of the Data Breach have surfaced not from Defendant, but from third parties. On September 15, 2022, Databreaches.net reported that a ransomware group called "Hive" contacted Defendant on July 14 and July 15, 2022, and warned Defendant that it had infiltrated its network, stayed there for 12 days, encrypted Defendant's servers, and downloaded Personal Information.[13]

41. Upon information and belief, Plaintiff's and Class Members' unencrypted information was already published on the Dark Web. Further, Databreaches.net reported that it received a sample of files from Hive containing Personal Information of Empress patients. Unauthorized individuals can now easily access the Personal Information of Plaintiff and Class Members.

42. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted information it was maintaining for Plaintiff and Class

[13] *See* https://www.databreaches.net/ny-empress-ems-hit-by-hive-ransomware/ (last accessed Sept. 22, 2022).

Members, causing their Personal Information to be exposed.

43. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[14]

44. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.

[14] *See* How to Protect Your Networks from RANSOMWARE, at 3, *available at* https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (last visited Aug. 2, 2022).

- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.

- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.

- Consider disabling Remote Desktop protocol (RDP) if it is not being used.

- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.

- Execute operating system environments or specific programs in a virtualized environment.

- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[15]

45. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

- **Update and patch your computer**. Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks….

- **Use caution with links and when entering website addresses**. Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net)….

- **Open email attachments with caution**. Be wary of opening email attachments, even from senders you think you know, particularly

[15] *Id.* at 3-4.

when attachments are compressed files or ZIP files.

- **Keep your personal information safe**. Check a website's security to ensure the information you submit is encrypted before you provide it….

- **Verify email senders**. If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.

- **Inform yourself**. Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.

- **Use and maintain preventative software programs**. Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic….[16]

46. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

Secure internet-facing assets

- Apply latest security updates
- Use threat and vulnerability management
- Perform regular audit; remove privileged credentials;

Thoroughly investigate and remediate alerts

- Prioritize and treat commodity malware infections as potential full compromise;

Include IT Pros in security discussions

- Ensure collaboration among [security operations], [security admins], and

[16] *See* Security Tip (ST19-001) Protecting Against Ransomware (original release date Apr. 11, 2019), *available at* https://us-cert.cisa.gov/ncas/tips/ST19-001 (last visited June 15, 2021).

[information technology] admins to configure servers and other endpoints securely;

Build credential hygiene

- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords

Apply principle of least-privilege

- Monitor for adversarial activities
- Hunt for brute force attempts
- Monitor for cleanup of Event Logs
- Analyze logon events

Harden infrastructure

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[17]

47. Given that Defendant was storing the Personal Information of more than 318,558 individuals, Defendant could and should have implemented all of the above measures to prevent and detect ransomware attacks.

48. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent ransomware attacks, resulting in the Data Breach and the exposure of the PII of more than 318,558 individuals, including Plaintiff and Class Members.

The Healthcare Sector is Particularly Vulnerable to Ransomware Attacks

49. Defendant was on notice that companies in the healthcare industry are targets for data breaches.

[17] *See* Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), *available at* https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/ (last visited Aug. 1, 2022).

50. Defendant was on further notice regarding the increased risks of inadequate cybersecurity. In February 2022, the cybersecurity arm of the U.S. Department of Health and Human Services ("HHS") issued a warning to hospitals and healthcare systems about a dramatic rise in cyberattacks, including ransomware attacks, urging facilities to shore up their cyber defenses.[18] Indeed, just days before, HHS's cybersecurity arm issued yet another warning about increased cyberattacks that urged vigilance with respect to data security.[19]

51. In the context of data breaches, healthcare is "by far the most affected industry sector."[20] Further, cybersecurity breaches in the healthcare industry are particularly devastating, given the frequency of such breaches and the fact that healthcare providers maintain highly sensitive and detailed PII.[21] A Tenable study analyzing publicly disclosed healthcare sector breaches from January 2020 to February 2021 reported that "records were confirmed to have been exposed in *nearly 93% of the breaches*."[22]

52. Defendant was also on notice that the FBI has been concerned about data security in the healthcare industry. In August 2014, after a cyberattack on Community Health Systems, Inc., the FBI warned companies within the healthcare industry that hackers were targeting them. The warning stated that "[t]he FBI has observed malicious actors targeting healthcare related

---

[18] Rebecca Pifer, *Tenet says 'cybersecurity incident' disrupted hospital operations*, HEALTHCAREDIVE (Apr. 26, 2022), https://www.healthcaredive.com/news/tenet-says-cybersecurity-incident-disrupted-hospital-operations/622692/.

[19] *Id.* (HHS warned healthcare providers about the increased potential for attacks by a ransomware group called Hive, "[c]alling it one of the 'most active ransomware operators in the cybercriminal ecosystem,' the agency said reports have linked Hive to attacks on 355 companies within 100 days of its launch last June — nearly three a day.").

[20] Tenable Security Response Team, *Healthcare Security*, TENABLE (Mar. 10, 2021), https://www.tenable.com/blog/healthcare-security-ransomware-plays-a-prominent-role-in-covid-19-era-breaches

[21] *See id.*

[22] Tenable Security Response Team, *Healthcare Security*, TENABLE (Mar. 10, 2021), https://www.tenable.com/blog/healthcare-security-ransomware-plays-a-prominent-role-in-covid-19-era-breaches.

systems, perhaps for the purpose of obtaining the Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PII)."[23]

53. The American Medical Association ("AMA") has also warned healthcare companies about the importance of protecting their patients' confidential information:

> Cybersecurity is not just a technical issue; it's a patient safety issue. AMA research has revealed that 83% of physicians work in a practice that has experienced some kind of cyberattack. Unfortunately, practices are learning that cyberattacks not only threaten the privacy and security of patients' health and financial information, but also patient access to care.[24]

54. The number of U.S. data breaches surpassed 1,000 in 2016, a record high and a forty percent increase in the number of data breaches from the previous year.[25] In 2017, a new record high of 1,579 breaches were reported representing a 44.7 percent increase.[26] That trend continues.

55. The healthcare sector reported the second largest number of breaches among all measured sectors in 2018, with the highest rate of exposure per breach.[27] Indeed, when compromised, healthcare related data is among the most sensitive and personally consequential. A

---

[23] Jim Finkle, *FBI Warns Healthcare Firms that they are Targeted by Hackers*, Reuters (Aug. 2014), *available at*: https://www.reuters.com/article/us-cybersecurity-healthcare-fbi/fbi-warns-healthcare-firms-they-are-targeted-by-hackers-idUSKBN0GK24U20140820 (last visited Aug. 1, 2022).

[24] Andis Robeznieks, *Cybersecurity: Ransomware attacks shut down clinics, hospitals*, Am. Med. Ass'n (Oct. 4, 2019), *available at*: https://www.ama-assn.org/practice-management/sustainability/cybersecurity-ransomware-attacks-shut-down-clinics-hospitals (last visited Aug. 1, 2022).

[25] Identity Theft Resource Center, *Data Breaches Increase 40 Percent in 2016, Finds New Report From Identity Theft Resource Center and CyberScout* (Jan. 19, 2017), *available at:* https://www.idtheftcenter.org/surveys-studys (last visited Aug. 1, 2022).

[26] Identity Theft Resource Center, *2017 Annual Data Breach Year-End Review, available at:* https://www.idtheftcenter.org/2017-data-breaches/ (last visited Aug. 1, 2022).

[27] Identity Theft Resource Center, *2018 End -of-Year Data Breach Report, available at*: https://www.idtheftcenter.org/2018-data-breaches/ (last visited Aug. 1, 2022).

report focusing on healthcare breaches found that the "average total cost to resolve an identity theft-related incident . . . came to about $20,000," and that the victims were often forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[28] Almost 50 percent of the victims lost their healthcare coverage as a result of the incident, while nearly 30 percent said their insurance premiums went up after the event. Forty percent of the customers were never able to resolve their identity theft at all. Data breaches and identity theft have a crippling effect on individuals and detrimentally impact the economy as a whole.[29]

56. Healthcare related breaches have continued to rapidly increase because electronic patient data is seen as a valuable asset. According to the 2019 HIMSS Cybersecurity Survey, 82 percent of participating hospital information security leaders reported having a significant security incident in the last 12 months, with a majority of these known incidents being caused by "bad actors" such as cybercriminals.[30] "Hospitals have emerged as a primary target because they sit on a gold mine of sensitive personally identifiable information for thousands of patients at any given time. From social security and insurance policies, to next of kin and credit cards, no other organization, including credit bureaus, have so much monetizable information stored in their data centers."[31]

Defendant Acquires, Collects, and Stores Plaintiff's and Class Members' Personal Information.

57. In the course of its regular business operations, Defendant acquired, collected, and

[28] Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (March 3, 2010), *available at:* https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/ (last visited Aug. 1, 2022).
[29] *Id.*
[30] *2019 HIMSS Cybersecurity Survey, available at*: https://www.himss.org/2019-himss-cybersecurity-survey (last visited Aug. 1, 2022).
[31] Inside Digital Health, *How to Safeguard Hospital Data from Email Spoofing Attacks*, April 4, 2019, *available at*: https://www.idigitalhealth.com/news/how-to-safeguard-hospital-data-from-email-spoofing-attacks (last visited Aug. 1, 2022).

stored Plaintiff's and Class Members' Personal Information.

58. As a condition of its relationships with Plaintiff and Class Members, Defendant required that Plaintiff and Class Members entrust Defendant with highly confidential PII.

59. By obtaining, collecting, and storing the PII of Plaintiff and Class Members, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting the Personal Information from disclosure.

60. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their Personal Information and relied on Defendant to keep their Personal Information confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

61. Yet, despite the prevalence of public announcements of these data breach and data security compromises, Defendants failed to take appropriate steps to protect Plaintiff's and Class Members' Personal Information from being compromised.

Securing PII and Preventing Breaches

62. Defendant could have prevented this Data Breach by properly securing and encrypting the Personal Information of Plaintiff and Class Members. Alternatively, Defendant could have destroyed the data, especially decade-old data from former patients or employees.

63. Defendant's negligence in safeguarding the Personal Information of Plaintiff and Class Members is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

64. Indeed, despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the Personal Information of Plaintiff and Class Members from being compromised.

65. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[32] 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."[33]

66. The ramifications of Defendant's failure to keep secure the Personal Information of Plaintiff and Class Members are long lasting and severe. Once stolen, particularly Social Security numbers, fraudulent use of that information and damage to victims may continue for years.

Value of Personal Identifiable Information

67. The Personal Information of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[34] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[35] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[36]

---

[32] 17 C.F.R. § 248.201 (2013).
[33] *Id*.
[34] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last visited Aug. 1, 2022).
[35] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited Aug. 1, 2022).
[36] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last visited Aug. 1, 2022).

68. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[37]

69. What is more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

70. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[38]

71. Based on the foregoing, the information compromised in the Data Breach is

---

[37] Social Security Administration, *Identity Theft and Your Social Security Number*, *available at*: https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Aug. 1, 2022).

[38] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), *available at*: http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft (last visited Aug. 1, 2022).

significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change—name, Social Security number, and potentially date of birth.

72. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[39]

73. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

74. The Personal Information of Plaintiff and Class Members was taken by hackers to engage in identity theft or and or to sell it to other criminals who will purchase the Personal Information for that purpose. The fraudulent activity resulting from the Data Breach may not come to light for years.

75. There may be a time lag between when harm occurs versus when it is discovered, and also between when Personal Information is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[40]

[39] Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), *available at*: https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited Aug. 1, 2022).

[40] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* https://www.gao.gov/products/gao-07-737 (last visited Aug. 1, 2022).

76. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the Personal Information of Plaintiff and Class Members, including Social Security numbers and/or dates of birth, and of the foreseeable consequences that would occur if the PII was compromised, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members a result.

77. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. Plaintiff and Class Members are incurring and will continue to incur such damages in addition to any fraudulent use of their Personal Information.

78. Defendant was, or should have been, fully aware of the unique type and the significant volume of data stored on and/or shared on its system and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

79. To date, Defendant has offered Plaintiff and Class Members only "eligible individuals" credit monitoring services. The offered service is wholly inadequate to protect Plaintiff and Class Members from the threats they face for years to come, particularly in light of the PII at issue here.

80. Further, there is a market for Plaintiff's and Class Members PHI, and the stolen PII has inherent value.

81. PHI is particularly valuable because criminals can use it to target victims with frauds and scams that take advantage of the victim's medical conditions or victim settlements. It can be used to create fake insurance claims, allowing for the purchase and resale of medical equipment, or gain access to prescriptions for illegal use or resale. Drug manufacturers, medical device manufacturers, pharmacies, hospitals, and other healthcare service providers often purchase

PII on the black market for the purpose of target marketing their products and services to the physical maladies of the data breach victims themselves. Insurance companies purchase and use wrongfully disclosed PHI to adjust their insureds' medical insurance premiums.

82. Medical identify theft can result in inaccuracies in medical records and costly false claims. It can also have life-threatening consequences. If a victim's health information is mixed with other records, it can lead to misdiagnosis or mistreatment. "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy Forum. "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."[41]

83. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the Personal Information of Plaintiff and Class Members.

Defendant's Conduct Violates the Rules and Regulations of HIPAA and HITECH

84. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§ 1301, et seq. These provisions require, among other things, that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling PII like the data Defendant left unguarded. The HHS has subsequently promulgated five rules under authority of the Administrative Simplification provisions of HIPAA.

85. Defendant is a covered entity pursuant to HIPAA. *See* 45 C.F.R. § 160.102. Defendant must therefore comply with the HIPAA Privacy Rule and Security Rule. See 45 C.F.R. Part 160 and Part 164, Subparts A through E.

[41] Michael Ollove, *The Rise of Medical Identity Theft in Healthcare*, Kaiser Health News (Feb. 7, 2014), *available at* https://khn.org/news/rise-of-indentity-theft/ (last visited Aug. 2, 2022).

86. Defendant is a covered entity pursuant to the Health Information Technology Act ("HITECH").[42] *See* 42 U.S.C. §17921, 45 C.F.R. § 160.103.

87. Plaintiff's and Class Members' Personal Information is "protected health information" as defined by 45 CFR § 160.103.

88. 45 CFR § 164.402 defines "breach" as "the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part which compromises the security or privacy of the protected health information."

89. 45 CFR § 164.402 defines "unsecured protected health information" as "protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the [HHS] Secretary[.]"

90. Plaintiff's and Class Members' Personal Information is "unsecured protected health information" as defined by 45 CFR § 164.402.

91. Plaintiff's and Class Members' unsecured protected health information has been acquired, accessed, used, or disclosed in a manner not permitted under 45 CFR Subpart E as a result of the Data Breach.

92. Plaintiff's and Class Members' unsecured protected health information acquired, accessed, used, or disclosed in a manner not permitted under 45 CFR Subpart E as a result of the Data Breach was not rendered unusable, unreadable, or indecipherable to unauthorized persons.

93. Plaintiff's and Class Members' unsecured protected health information that was acquired, accessed, used, or disclosed in a manner not permitted under 45 CFR Subpart E as a result of the Data Breach, and which was not rendered unusable, unreadable, or indecipherable to unauthorized persons, was viewed by unauthorized persons.

[42] HIPAA and HITECH work in tandem to provide guidelines and rules for maintaining protected health information. HITECH references and incorporates HIPAA

94. Plaintiff's and Class Members' unsecured protected health information was viewed by unauthorized persons in a manner not permitted under 45 CFR Subpart E as a result of the Data Breach.

95. After receiving notice that they were victims of a data breach that required the filing of a Breach Report in accordance with 45 CFR § 164.408(a), it is reasonable for recipients of that notice, including Plaintiff and Class Members in this case, to believe that future harm (including identity theft) is real and imminent, and to take steps to mitigate that risk of future harm.

96. The Data Breach could have been prevented if Defendant implemented HIPAA mandated, industry standard policies and procedures for securely disposing of Personal Information when it was no longer necessary and/or had honored its obligations to its patients.

97. It can be inferred from Defendant's Data Breach that Defendant either failed to implement, or inadequately implemented, information security policies or procedures in place to protect Plaintiff and Class Members' Personal Information.

98. Defendant's security failures include, but are not limited to:

a. Failing to maintain an adequate data security system to prevent data loss;

b. Failing to mitigate the risks of a data breach and loss of data;

c. Failing to ensure the confidentiality and integrity of electronic protected health information Defendant creates, receives, maintains, and transmits in violation of 45 CFR 164.306(a)(1);

d. Failing to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights in violation of 45 CFR 164.312(a)(1);

e. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 CFR 164.308(a)(1);

f. Failing to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 CFR 164.308(a)(6)(ii);

g. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic protected health information in violation of 45 CFR 164.306(a)(2);

h. Failing to protect against any reasonably-anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 CFR 164.306(a)(3);

i. Failing to ensure compliance with HIPAA security standard rules by Defendant's workforce in violation of 45 CFR 164.306(a)(94);

j. Impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons in violation of 45 CFR 164.502,et seq.; and

k. Retaining information past a recognized purpose and not deleting it.

99. The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414, also required Defendant to provide notice of the breach to each affected individual "without unreasonable delay and in no case later than 60 days following discovery of the breach."

100. Because Defendant has failed to comply with industry standards, while monetary relief may cure some of Plaintiff and Class Members' injuries, injunctive relief is necessary to

ensure Defendant's approach to information security is adequate and appropriate. Defendant still maintains the protected health information and other Personal Information of Plaintiff and Class Members; and without the supervision of the Court via injunctive relief, Plaintiff's and Class Members' protected health information and other Personal Information remains at risk of subsequent Data Breaches.

Plaintiff's Experience

101. Plaintiff was a patient of Empress when Empress used its ambulance services to transport Plaintiff to a hospital for medical treatment.

102. As a condition of receiving transportation services from Empress, Plaintiff provided Empress with his name, address, telephone number, date of birth, Social Security number, and other Personal Information.

103. Upon information and belief, Plaintiff's Personal Information was in Defendant's computer systems during the Data Breach and remains in Defendant's possession.

104. Plaintiff received a Notice of Data Breach from Defendant on or about September 18, 2022. The letter stated that Plaintiff's Personal Information was compromised in the Data Breach.

105. As a result of the Data Breach, Plaintiff has spent time dealing with the consequences of the Data Breach, which includes time spent on the telephone and sorting through his unsolicited emails and text messages, time spent verifying the legitimacy of the Data Breach, exploring credit monitoring and identity theft insurance options, attempting to enroll and enrolling in the credit monitoring and identity theft protection services offered by Defendant, and self-monitoring his accounts. This time has been lost forever and cannot be recaptured.

106. Further, Plaintiff has experienced an uptick in spam telephone calls, emails, and text messages since the Data Breach.

107. Since the Data Breach, Plaintiff has suffered from actual misuse of his Personal Information. Plaintiff has received mail at his residence, with unknown person's name connected to Plaintiff's address.

108. Plaintiff is very careful about sharing his Personal Information. He has never knowingly transmitted unencrypted Personal Information over the internet or any other unsecured source.

109. Plaintiff stores any documents containing his Personal Information in a safe and secure location. Moreover, he diligently chooses unique usernames and passwords for his online accounts.

110. Plaintiff suffered actual injury in the form of damages to and diminution in the value of his PII—a form of intangible property that Plaintiff entrusted to Defendant for the purpose of receiving medical care from Defendant, which was compromised in and as a result of the Data Breach.

111. Plaintiff suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of his privacy.

112. Plaintiff is now subject to the present and continuing risk of fraud, identity theft, and misuse resulting from his Personal Information, especially his Social Security number, in combination with his name, being placed in the hands of unauthorized third parties and criminals. This injury was worsened by Defendant's continuing delay in revealing the true nature of the threat to Plaintiff's Personal Information.

113. Plaintiff has a continuing interest in ensuring that his Personal Information, which, upon information and belief, remain backed up in Defendant's possession, is protected and safeguarded from future breaches.

V. CLASS ALLEGATIONS

114. Plaintiff brings this nationwide class action on behalf of himself and on behalf of all others similarly situated pursuant to NY CPLR § 901 (2015), *et seq*. and other applicable law.

115. The Nationwide Class that Plaintiff seeks to represent is defined as follows:

> All individuals whose Personal Information was compromised during the Data Breach referenced in the Website Notice published by Defendant on or around September 9, 2022 (the "Nationwide Class").

116. In the alternative to claims asserted on behalf of the Nationwide Class, Plaintiff asserts claims on behalf of a separate subclass, defined as follows:

> All individuals residing in New York whose Personal Information was compromised during the Data Breach referenced in the Website Notice published by Defendant on or around September 9, 2022 (the "New York Class").

117. Excluded from the Classes are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

118. Plaintiff reserves the right to modify or amend the definition of the proposed classes before the Court determines whether certification is appropriate.

119. This action is brought and may be maintained as a class action because there is a well-defined community of interest among many persons who comprise a readily ascertainable class. A well-defined community of interest exists to warrant classwide relief because Plaintiff and all members of the Nationwide Class were subjected to the same wrongful practices by Defendant, entitling them to the same relief.

120. The Nationwide Class is so numerous that individual joinder of its members is impracticable. While the exact number of Class Members is unknown to Plaintiff at this time, Plaintiff is informed and believes that there are at least hundreds of thousands of Class Members.

121. Common questions of law and fact exist as to members of the Nationwide Class and predominate over any questions which affect only individual members of the Class. These common questions include, but are not limited to:

a. Whether and to what extent Defendant had a duty to protect the Personal Information of Plaintiff and Class Members;

b. Whether Defendant had a duty not to disclose the Personal Information of Plaintiff and Class Members to unauthorized third parties;

c. Whether Defendant had a duty not to use the Personal Information of Plaintiff and Class Members for non-business purposes;

d. Whether Defendant failed to adequately safeguard the Personal Information of Plaintiff and Class Members;

e. Whether and when Defendant actually learned of the Data Breach;

f. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their Personal Information had been compromised;

g. Whether Defendant violated the law by failing to promptly notify Plaintiff and Class

Members that their Personal Information had been compromised;

h. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

i. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

j. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the Personal Information of Plaintiff and Class Members;

k. Whether Plaintiff and Class Members are entitled to actual, damages, and/or statutory damages as a result of Defendant's wrongful conduct;

l. Whether Plaintiff and Class Members are entitled to restitution as a result of Defendant's wrongful conduct; and

m. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

122. Plaintiff is a member of the Classes he seeks to represent and his claims and injuries are typical of the claims and injuries of the other Class Members.

123. Plaintiff will adequately and fairly protect the interests of other Class Members. Plaintiff has no interests adverse to the interests of absent Class Members. Plaintiff is represented by legal counsel with substantial experience in class action litigation. The interests of Class Members will be fairly and adequately protected by Plaintiff and his counsel.

124. Defendant has acted or refused to act on grounds that apply generally to the Class Members, so that final injunctive relief or corresponding declaratory relief is appropriate respecting the Class as a whole.

125. A class action is superior to other available means for fair and efficient adjudication of the claims of the Class and would be beneficial for the parties and the court. Class action treatment will allow a large number of similarly situated persons to prosecute their common claims in a single forum, simultaneously, efficiently, and without the unnecessary duplication of effort and expense that numerous individual actions would require. The amounts owed to the many individual Class Members are likely to be relatively small, and the burden and expense of individual litigation would make it difficult or impossible for individual members of the class to seek and obtain relief. A class action will serve an important public interest by permitting such individuals to effectively pursue recovery of the sums owed to them. Further, class litigation prevents the potential for inconsistent or contradictory judgments raised by individual litigation. Plaintiff is unaware of any difficulties that are likely to be encountered in the management of this action that would preclude its maintenance as a class action.

COUNT I
Negligence
(On Behalf of Plaintiff and the Nationwide Class)

126. Plaintiff and the Nationwide Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 125.

127. Plaintiff and the Nationwide Class provided and entrusted Defendant with certain Personal Information as a condition of receiving medical services and care based upon the premise and with the understanding that Defendant would safeguard their information, use their Personal Information for business purposes only, and/or not disclose their Personal Information to unauthorized third parties.

128. Defendant has full knowledge of the sensitivity of the Personal Information and the types of harm that Plaintiff and the Nationwide Class could and would suffer if the Personal

Information were wrongfully disclosed.

129. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the Personal Information of Plaintiff and the Nationwide Class involved an unreasonable risk of harm to Plaintiff and the Nationwide Class, even if the harm occurred through the criminal acts of a third party.

130. Defendant had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Defendant's security protocols to ensure that the Personal Information of Plaintiff and the Nationwide Class in Defendant's possession was adequately secured and protected.

131. Defendant owed a duty to Plaintiff and the Nationwide Class to implement intrusion detection processes that would detect a data breach or unauthorized access to its systems in a timely manner.

132. Defendant also had a duty to exercise appropriate clearinghouse practices to remove Personal Information it was no longer required to retain pursuant to regulations, including that of former patients.

133. Defendant also had a duty to employ proper procedures to detect and prevent the improper access, misuse, acquisition, and/or dissemination of the Personal Information of Plaintiff and the Nationwide Class.

134. Defendant's duty to use reasonable security measures arose as a result of the special relationship that existed between Defendant and Plaintiff and the Nationwide Class. That special relationship arose because Plaintiff and the Nationwide Class entrusted Defendant with their confidential Personal Information, a necessary part of their relationships with Defendant.

135. Defendant owed a duty to disclose the material fact that Defendant's data security practices were inadequate to safeguard the personal and medical information of Plaintiff and the Nationwide Class.

136. Defendant's Privacy Policies acknowledge Defendant's duty to adequately protect the personal and medical information of Plaintiff and the Nationwide Class.

137. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Nationwide Class was reasonably foreseeable, particularly in light of Defendant's inadequate security practices.

138. Plaintiff and the Nationwide Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the Personal Information of Plaintiff and the Nationwide Class, the critical importance of providing adequate security of that Personal Information, and the necessity for encrypting Personal Information stored on Defendant's systems.

139. Defendant's own conduct created a foreseeable risk of harm to Plaintiff and the Nationwide Class. Defendant's misconduct included, but was not limited to, its failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendant's misconduct also included its decisions not to comply with industry standards for the safekeeping of the Personal Information of Plaintiff and the Nationwide Class, including basic encryption techniques freely available to Defendant.

140. Plaintiff and the Nationwide Class had no ability to protect their Personal Information that was in, and likely remains in, Defendant's possession.

141. Defendant was in a position to protect against the harm suffered by Plaintiff and the Nationwide Class as a result of the Data Breach.

142. Defendant had and continues to have a duty to adequately disclose that the Personal Information of Plaintiff and the Nationwide Class within Defendant's possession was compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiff and the Nationwide Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their Personal Information by third parties.

143. Defendant has admitted that the Personal Information of Plaintiff and the Nationwide Class was wrongfully accessed, acquired, and/or released to unauthorized third persons as a result of the Data Breach.

144. Defendant, through its actions and/or omissions, unlawfully breached its duties to Plaintiff and the Nationwide Class by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the Personal Information of Plaintiff and the Nationwide Class during the time the Personal Information was within Defendant's possession or control.

145. Defendant improperly and inadequately safeguarded the Personal Information of Plaintiff and the Nationwide Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

146. Defendant failed to heed industry warnings and alerts to provide adequate safeguards to protect the Personal Information of Plaintiff and the Nationwide Class in the face of increased risk of theft.

147. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and the Nationwide Class by failing to have appropriate procedures in place to detect unauthorized access or intrusions and prevent dissemination of their Personal Information.

Additionally, Defendant failed to disclose to Plaintiff and the Nationwide Class that Defendant's security practices were inadequate to safeguard the Personal Information of Plaintiff and the Nationwide Class.

148. Defendant breached its duty to exercise appropriate clearinghouse practices by failing to remove Personal Information it was no longer required to retain pursuant to regulations, including PII of former patients and employees.

149. Defendant, through its actions and/or omissions, unlawfully breached its duty to adequately and timely disclose to Plaintiff and the Nationwide Class the existence and scope of the Data Breach.

150. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and the Nationwide Class, the Personal Information of Plaintiff and the Nationwide Class would not have been compromised.

151. There is a close causal connection between Defendant's failure to implement security measures to protect the Personal Information of Plaintiff and the Nationwide Class and the harm, or risk of imminent harm, suffered by Plaintiff and the Nationwide Class. The Personal Information of Plaintiff and the Nationwide Class was accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such Personal Information by adopting, implementing, and maintaining appropriate security measures.

152. As a direct and proximate result of Defendant's negligence, Plaintiff and the Nationwide Class have suffered and will continue to suffer injury.

153. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiff and the Nationwide Class have suffered and will suffer the continued risks of exposure of their Personal Information, which remains in Defendant's possession and is subject to further

unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in its continued possession.

154. As a direct and proximate result of Defendant's negligence, Plaintiff and the Nationwide Class are entitled to and demand actual, consequential, and nominal damages.

COUNT II
Negligence Per Se
(On Behalf of Plaintiff and the Nationwide Class)

155. Plaintiff and the Nationwide Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 125.

156. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

157. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and the Nationwide Class.

158. Defendant's violation of Section 5 of the FTC Act constitutes negligence *per se*.

159. Plaintiff and the Nationwide Class are within the class of persons that the FTC Act was intended to protect.

160. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was 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 and

deceptive practices, caused the same harm as that suffered by Plaintiff and the Nationwide Class.

161. Defendant's violations of HIPAA and HITECH also independently constitute negligence *per se*.

162. HIPAA privacy laws were enacted with the objective of protecting the confidentiality of patients' healthcare information and set forth the conditions under which such information can be used, and to whom it can be disclosed. HIPAA privacy laws not only apply to healthcare providers and the organizations they work for, but to any entity that may have access to healthcare information about a patient that—if it were to fall into the wrong hands—could present a risk of harm to the patient's finances or reputation.

163. Plaintiff and Class Members are within the class of persons that HIPAA privacy laws were intended to protect.

164. The harm that occurred as a result of the Data Breach is the type of harm HIPAA privacy laws were intended to guard against.

165. As a direct and proximate result of Defendant's negligence *per se*, Plaintiff and the Nationwide Class have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their Personal Information is used; iii) the compromise, publication, and/or theft of their Personal Information ; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Personal Information ; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their Personal Information, which

remain in Defendant's possession and are subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Personal Information of Plaintiff and the Nationwide Class; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Personal Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and the Nationwide Class.

COUNT III
Breach of Implied Contract
(On Behalf of Plaintiff and the Nationwide Class)

166. Plaintiff and the Nationwide Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 125.

167. Defendant required Plaintiff and the Nationwide Class to provide and entrust their Personal Information as a condition of obtaining medical care from Defendant.

168. Plaintiff and the Nationwide Class paid money to Defendant in exchange for goods and services, as well as Defendant's promises to protect their protected health information and other Personal Information from unauthorized disclosure.

169. In its written Privacy Policy, Defendant expressly promised Plaintiff and Class Members that Defendant would only disclose Personal Information under certain circumstances, none of which relate to the Data Breach.

170. Defendant promised to comply with HIPAA and HITECH standards and to make sure that Plaintiff's and Class Members' Personal Information would remain protected.

171. As a condition of obtaining medical care and/or employment from Defendant, Plaintiff and the Nationwide Class provided and entrusted their personal information. In so doing, Plaintiff the Nationwide Class entered into implied contracts with Defendant by which Defendant

agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and the Nationwide Class if their data had been breached and compromised or stolen.

172. A meeting of the minds occurred, as Plaintiff and Class Members agreed, *inter alia*, to provide accurate and complete Personal Information and to pay Defendant in exchange for Defendant's agreement to, *inter alia*, protect their Personal Information.

173. Plaintiff and the Nationwide Class Members would not have entrusted their Personal Information to Defendant in the absence of Defendant's implied promise to adequately safeguard this confidential personal and medical information.

174. Plaintiff and the Nationwide Class fully performed their obligations under the implied contracts with Defendant.

175. Defendant breached the implied contracts it made with Plaintiff and the Nationwide Class by making their Personal Information accessible from the internet (regardless of any mistaken belief that the information was protected) and failing to make reasonable efforts to use the latest security technologies designed to help ensure that the Personal Information was secure, failing to encrypt Plaintiff and Class Members' sensitive Personal Information, failing to safeguard and protect their Personal Information, and by failing to provide timely and accurate notice to them that Personal Information was compromised as a result of the data breach.

176. Defendant further breached the implied contracts with Plaintiff and Class Members by failing to comply with its promise to abide by HIPAA and HITECH.

177. Defendant further breached the implied contracts with Plaintiff and Class Members by failing to ensure the confidentiality and integrity of electronic protected health information Defendant created, received, maintained, and transmitted in violation of 45 CFR 164.306(a)(1).

178. Defendant further breached the implied contracts with Plaintiff and Class Members by failing to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights in violation of 45 CFR 164.312(a)(1).

179. Defendant further breached the implied contracts with Plaintiff and Class Members by failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 CFR 164.308(a)(1).

180. Defendant further breached the implied contracts with Plaintiff and Class Members by failing to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 CFR 164.308(a)(6)(ii).

181. Defendant further breached the implied contracts with Plaintiff and Class Members by failing to protect against any reasonably anticipated threats or hazards to the security or integrity of electronic protected health information in violation of 45 CFR 164.306(a)(2).

182. Defendant further breached the implied contracts with Plaintiff and Class Members by failing to protect against any reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 CFR 164.306(a)(3).

183. Defendant further breached the implied contracts with Plaintiff and Class Members by failing to ensure compliance with the HIPAA security standard rules by its workforce violations in violation of 45 CFR 164.306(a)(94).

184. Defendant further breached the implied contracts with Plaintiff and Class Members by impermissibly and improperly using and disclosing protected health information that is and

remains accessible to unauthorized persons in violation of 45 CFR 164.502, *et seq*.

185. Defendant further breached the implied contracts with Plaintiff and Class Members by failing to design, implement, and enforce policies and procedures establishing physical administrative safeguards to reasonably safeguard protected health information, in compliance with 45 CFR 164.530(c).

186. Defendant further breached the implied contracts with Plaintiff and Class Members by otherwise failing to safeguard Plaintiff's and Class Members' Personal Information.

187. Defendant's failures to meet these promises constitute breaches of the implied contracts.

188. Because Defendant allowed unauthorized access to Plaintiff and Class Members' Personal Information and failed to safeguard the Personal Information, Defendant breached its contracts with Plaintiff and Class Members.

189. Defendant breached its contracts by not meeting the minimum level of protection of Plaintiff and Class Members' protected health information and other Personal Information, because Defendant did not prevent against the breach of over 300,000 patients' Personal Information.

190. Furthermore, the failure to meet its confidentiality and privacy obligations resulted in Defendant providing goods and services to Plaintiff and Class Members that were of a diminished value.

191. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiff and the Nationwide Class are now subject to the present and continuing risk of fraud, and are suffering (and will continue to suffer) the ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual

identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the diminished value of services provided by Defendant; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

192. As a result of Defendant's breach of implied contract, Plaintiff and the Nationwide Class are entitled to and demand actual, consequential, and nominal damages.

COUNT IV
Breach of Confidence
(On Behalf of Plaintiff and the Nationwide Class)

193. Plaintiff and the Nationwide Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 125.

194. At all times during Plaintiff's and the Nationwide Class's interactions with Defendant, as a medical provider, Defendant was fully aware of the confidential and sensitive nature of Plaintiff's and the Nationwide Class's PII that Plaintiff and the Nationwide Class provided to Defendant.

195. As alleged herein and above, Defendant's relationship with Plaintiff and the Nationwide Class was governed by terms and expectations that Plaintiff and the Nationwide Class's PII would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

196. Plaintiff and the Nationwide Class provided their PII to Defendant with the explicit and implicit understandings that Defendant would protect and not permit the PII to be disseminated to any unauthorized third parties.

197. Plaintiff and the Nationwide Class also provided their PII to Defendant with the explicit and implicit understandings that Defendant would take precautions to protect that PII from unauthorized disclosure.

198. Defendant voluntarily received in confidence the PII of Plaintiff and the Nationwide Class with the understanding that PII would not be disclosed or disseminated to the public or any unauthorized third parties.

199. Due to Defendant's failure to prevent and avoid the Data Breach from occurring, the PII of Plaintiff and the Nationwide Class was disclosed and misappropriated to unauthorized third parties beyond Plaintiff and the Nationwide Class's confidence, and without their express permission.

200. As a direct and proximate cause of Defendant's actions and/or omissions, Plaintiff and the Nationwide Class have suffered damages.

201. But for Defendant's disclosure of Plaintiff and the Nationwide Class's PII in violation of the parties' understanding of confidence, their PII would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. The Data Breach was the direct and legal cause of the theft of Plaintiff and the Nationwide Class's PII as well as the resulting damages.

202. The injury and harm Plaintiff and the Nationwide Class suffered was the reasonably foreseeable result of Defendant's unauthorized disclosure of Plaintiff and the Nationwide Class's PII. Defendant knew or should have known its methods of accepting and securing Plaintiff and the Nationwide Class's PII was inadequate as it relates to, at the very least, securing servers and other equipment containing Plaintiff and the Nationwide Class's PII.

203. As a direct and proximate result of Defendant's breach of its confidence with Plaintiff and the Nationwide Class, Plaintiff and the Nationwide Class have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII of Plaintiff and the Nationwide Class; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and the Nationwide Class.

204. As a direct and proximate result of Defendant's breaches of confidence, Plaintiff and the Nationwide Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

205. As a result of Defendant's breaches of confidence, Plaintiff and the Nationwide Class are entitled to and demand actual, consequential, and nominal damages.

COUNT V
VIOLATION OF THE NEW YORK CONSUMER LAW FOR DECEPTIVE ACTS AND PRACTICES ACT
N.Y. Gen. Bus. Law § 349
(On Behalf of Plaintiff and the Nationwide Class, or in the alternative, on behalf of Plaintiff and the New York SubClass)

206. Plaintiff and the Nationwide Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 125.

207. The New York General Business Law ("NYGBL") § 349 prohibits deceptive acts or practices in the conduct of any business, trade, or commerce, or in the furnishing of any service in the state of New York.

208. By reason of the conduct alleged herein, Empress has engaged in unlawful practices within the meaning of the NYGBL § 349. The conduct alleged herein is a "business practice" within the meaning of the NYGBL § 349, and the deception occurred within New York State.

209. Empress stored Plaintiff's and Class Members' Personal Information on the aforementioned servers. Empress knew or should have known it did not employ reasonable, industry standard, and appropriate security measures that complied "with federal regulations" and

that would have kept Plaintiff's and Class Members' Personal Information secure and prevented the loss or misuse of Plaintiff's and Class Members' PII.

210. Plaintiff and Class Members never would have provided their sensitive and personal Personal Information to Empress if they had been told or knew that Empress would fail to maintain sufficient security to keep such Personal Information from being taken by others.

211. Empress violated NYGBL § 349 by misrepresenting, both by affirmative conduct and by omission, the safety of Empress's storage and services, specifically the security thereof, and its ability to safely store and dispose of Plaintiff's and Class Members' Personal Information.

212. Empress also violated NYGBL § 349 by failing to implement reasonable and appropriate security measures or follow industry standards for data security, and by failing to immediately notify Plaintiff and Class Members of the Data Breach. If Empress had complied with these legal requirements, Plaintiff and Class Members would not have suffered the damages related to the Data Breach.

213. Empress's practices, acts, policies, and course of conduct violate NYGBL § 349 in that:

a. Empress actively and knowingly misrepresented or omitted disclosure of material information to Plaintiff and Class Members at the time they provided such Personal Information that Empress did not have sufficient security or mechanisms to protect Personal Information; and

b. Empress failed to give timely warnings and notices regarding the defects and problems with the security of their computer systems to protect Plaintiff's and

Class Members' Personal Information. Empress possessed actual knowledge of the inherent risks in inadequate data security.

214. Plaintiff and the Class were entitled to assume, and did assume, Empress would take appropriate measures to keep their Personal Information safe. Empress did not disclose that Plaintiff's and Class Members' Personal Information was vulnerable to malicious actors, and Empress was the only one in possession of that material information, which it had a duty to disclose.

215. The aforementioned conduct constitutes an unconscionable commercial practice in that Empress has, by the use of false or deceptive statements and/or knowing intentional material omissions, misrepresented and/or concealed the inadequate nature of its security practices, resulting in the Data Breach.

216. Members of the public were deceived by Empress's misrepresentations and failures to disclose.

217. Such acts by Empress are and were deceptive acts or practices which are and/or were likely to mislead a reasonable consumer providing his or her Personal Information to Empress. Said deceptive acts and practices are material. The requests for and use of such Personal Information in New York through deceptive means occurring in New York were consumer-oriented acts and thereby falls under the New York consumer fraud statute, NYGBL § 349.

218. Empress's wrongful conduct caused Plaintiff and Class Members to suffer a consumer-related injury by causing them to incur substantial expense to protect from misuse of

the Personal Information by third parties and placing Plaintiff and Class Members at serious risk for monetary damages.

219. As a direct and proximate result of Empress's violations of the above, Plaintiff and Class Members suffered damages including, but not limited to: unauthorized use of their Personal Information; theft of their personal and financial information; costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts; damages arising from the inability to use their Personal Information; costs associated with time spent and the loss of productivity or the enjoyment of one's life from taking time to address an attempt to ameliorate, mitigate and deal with the actual and future consequences of the Data Breach, including finding fraudulent charges, purchasing credit monitoring and identity theft protection services, initiating and monitoring credit freezes, and the stress, nuisance, and annoyance of dealing with all issues resulting from the Data Breach; the imminent and certainly impending injury flowing from potential fraud and identity theft posed by their Personal Information being placed in the hands of criminals; damages to and diminution in value of their Personal Information entrusted to Empress; and the loss of Plaintiff's and Class Members' privacy.

220. In addition to or in lieu of actual damages, because of the injury, Plaintiff and the Class seek statutory damages for each injury and violation which has occurred.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and Class Members, requests judgment against Defendant and that the Court grant the following:

A. For an Order certifying the Nationwide Class and the New York Class, and appointing Plaintiff and their Counsel to represent each such Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the PII of Plaintiff and Class Members, and from refusing to issue prompt, complete, and accurate disclosures to Plaintiff and Class Members;

C. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:

i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state, or local laws;

iii. requiring Defendant to delete, destroy, and purge the personal identifying information of Plaintiff and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the Personal Information of Plaintiff and Class Members;

v. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly

correct any problems or issues detected by such third-party security auditors;

vi. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

vii. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

viii. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

ix. requiring Defendant to conduct regular database scanning and securing checks;

x. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;

xi. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xii. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees compliance with Defendant's policies, programs, and systems for protecting

personal identifying information;

xiii. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xiv. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

xv. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

D. For an award of damages, including actual, consequential, nominal, and statutory damages, as allowed by law in an amount to be determined;

E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

F. For prejudgment interest on all amounts awarded; and

G. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff, by counsel, hereby demands that this matter be tried before a jury.

Date: October 10, 2022

GLANCY PRONGAY & MURRAY LLP

/s/ Brian P. Murray
By: Brian P. Murray, Esq.
230 Park Avenue, Ste. 358
New York, New York 10169
Tel.: (212) 682-5340
Fax: (212) 884-0988
bmurray@glancylaw.com

JEAN S. MARTIN
(*Pro Hac Vice application forthcoming*)
FRANCESCA KESTER
(*Pro Hac Vice application forthcoming*)
MORGAN & MORGAN COMPLEX LITIGATION GROUP
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
(813) 223-5505
jeanmartin@ForThePeople.com
fkester@ForThePeople.com

Attorneys for Plaintiff and the Putative Class

(https://empressems.com)

NEWS (/NEWS)

NOTICE OF SECURITY INCIDENT

July 2022 (https://empressems.com/2022/07/)

At Empress EMS, we are committed to protecting the privacy and security of our patients' information. Regrettably, we recently identified and addressed a cybersecurity incident involving some of that information. This letter explains the incident, measures we have taken, and some steps you may consider taking in response.

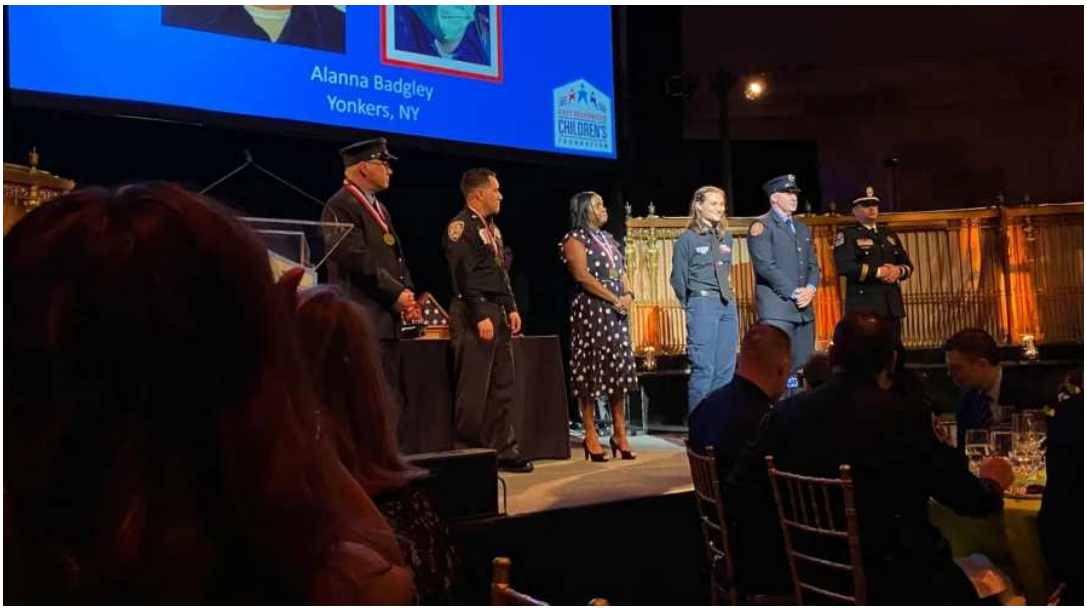
On July 14, 2022, we identified a network incident resulting in the encryption of some of our systems. We took measures to contain the incident, reported it to law enforcement, and we conducted a thorough investigation with the assistance of a third-party forensic firm. Our investigation determined that an unauthorized party first gained access to certain systems on our network on May 26, 2022, and then copied a small subset of files on July 13, 2022.

Some of these files contained patient names, dates of service, insurance information, and in some instances, Social Security numbers. Empress EMS is mailing letters to affected individuals and offering eligible individuals credit monitoring services. We're also recommending that patients review their healthcare statements for accuracy and contact their provider if they see services they

did not receive. If you believe you may be affected but do not receive a letter by October 9, 2022, please contact our dedicated external call center at 844-690-1251, Monday through Friday, 9:00 a.m. to 9:00 p.m., Eastern Time, except major US holidays.

We take this matter very seriously and deeply regret any inconvenience to our patients. To help prevent something like this from happening again, we strengthened the security of our systems and will continue enhancing our protocols to further safeguard the information in our care.

MORE NEWS (/NEWS)



Time Magazine Shines Light on Amazing Emergency Paramedic Alanna Ba
(https://empressems.com/time-magazine-shines-light-on-amazing-emergen
paramedic-alanna-badgley/)

READ MORE
(HTTPS://EMPRESSEMS.COM/TIME-MAGAZINE-SHINES-LIGHT-ON-AMAZING-EMEI
PARAMEDIC-ALANNA-BADGLEY/)

FIND A CAREER (/CAREERS)

Employee eSchedule (http://empress.emseschedule.com/schedule/logon.asp?)

MAIN HEADQUARTERS

722 Nepperhan Ave
Yonkers, NY 10703

(https://www.facebook.com/empressems) (https://twitter.com/EmpressEMS) (https://www.instagram.com/empressems) (https://www.linkedin.com/company/empress-ambulance-svc)

ABOUT (/ABOUT)

Our Story(/about)

Certifications(/about#certifications)

Our Team(/about#team)

NEWS (/NEWS)

CONTACT (/CONTACT)

Send Us a Message(/contact)

P: 1-888-965-5040(tel:18889655040)

F: 914-965-9776

SERVICES (/SERVICES)

911 Emergency Response(/services#911-emergency-response)

Community Paramedicine / Mobile Integrated Healthcare (/community-paramedicine-mobile-integrated-healthcare/)

Paramedic Fly Car Service(/services#paramedic-fly-car-service)

Advanced Life Support (ALS)(/services#advanced-life-support-als)

Basic Life Support (BLS)(/services#basic-life-support-bls)

Special Operations Division(/services#special-operations-division)

Event Standbys(/services#event-standbys)

Education and Training(/services#education-and-training)

Student Rotations(/student-rotations)

EMS Cadet Program(/services#ems-cadet-program)

CUSTOMER SERVICE (/CUSTOMER-SERVICE/)

Privacy Practices Statement(/wp-content/uploads/2022/07/empressprivacy.pdf)

Facility NY Physician Certification Statement(/wp-content/uploads/2022/07/facility-pcs.pdf)

BILLING

Submit Insurance Information Online(https://secure.jotformpro.com/form/22565260017952)

Submit Payment to Empress EMS (https://www.patientnotebook.com/empress/Enhanced/SendMoney/MakePayment)

Submit Payment to Emergacare NY (https://www.patientnotebook.com/emergacare/Enhanced/SendMoney/MakePayment)

EXHIBIT B

SUPREME COURT OF THE STATE OF NEW YORK
BRONX COUNTY

JOSH COLON, on behalf of himself and all others similarly situated, Plaintiff, v. EMPRESS AMBULANCE SERVICE, LLC, d/b/a/ EMPRESS EMERGENCY MEDICAL SERVICES, Defendant.	Case No. **SUMMONS**

TO THE ABOVE-NAMED DEFENDANT:

YOU ARE HEREBY SUMMONED to serve a notice of appearance on the Plaintiffs' attorney within twenty (20) days after the service of this summons, exclusive of the day of service (or within thirty (30) days after the service is complete if this summons is not personally delivered to you within the State of New York), and in case of your failure to appear, judgment will be taken against you by default for the relief demanded in the Complaint.

The basis of the venue designated is the residence of Plaintiff Josh Colon, who resides in Bronx County. Venue is appropriate in Bronx County pursuant to NY CPLR § 503.

Dated: New York, New York
October 11, 2022

GLANCY PRONGAY & MURRAY LLP

/s/ Brian P. Murray
By: Brian P. Murray, Esq.
230 Park Avenue, Ste. 358
New York, New York 10169
Tel.: (212) 682-5340
Fax: (212) 884-0988
bmurray@glancylaw.com

JEAN S. MARTIN
(*Pro Hac Vice application forthcoming*)
FRANCESCA KESTER
(*Pro Hac Vice application forthcoming*)
MORGAN & MORGAN COMPLEX LITIGATION GROUP
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
(813) 223-5505
jeanmartin@ForThePeople.com
fkester@ForThePeople.com

Attorneys for Plaintiffs

EXHIBIT C

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

815075/2022E - Bronx County Supreme Court

JOSH COLON v. EMPRESS AMBULANCE SERVICE, LLC, d/b/a/ EMPRESS EMERGENCY MEDICAL SERVICES

Short Caption: **SERVICES**
Case Type: **Commercial - Other (Violation of NY GBL 349)**
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 *Corrected*	Kennedy, T. Filed: 10/11/2022 *Received: 10/12/2022*	**Processed** Confirmation Notice
2	COMPLAINT *Corrected*	Kennedy, T. Filed: 10/11/2022 *Received: 10/11/2022*	**Processed** Confirmation Notice
3	EXHIBIT(S) - 1 *Notice of Security Incident _ Empress EMS*	Kennedy, T. Filed: 10/11/2022 *Received: 10/11/2022*	**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

ClassAction.org
