IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF FLORIDA
FORT LAUDERDALE DIVISION

ROB BREWSTER and ANITA GOFFMAN, on behalf of themselves and all others similarly situated,	)	Case No. _____
Plaintiffs,	)	[On Removal from the Circuit Court of the Seventeenth Judicial Circuit in and for Broward County, Case No. CACE-22-008510]
v.	)	
TENET HEALTHCARE CORPORATION, d/b/a TENET,	)	
Defendant.	)	

TENET HEALTHCARE CORPORATION'S NOTICE OF REMOVAL

PLEASE TAKE NOTICE that, pursuant to 28 U.S.C. §§ 1332(d), 1441(a), 1446, and 1453, Defendant Tenet Healthcare Corporation ("Tenet") hereby removes the above-captioned action, *Rob Brewster et al. v. Tenet Healthcare Corporation, d/b/a Tenet*, Case No. CACE-22-008510 (the "State Court Action"), from the Circuit Court of the Seventeenth Judicial Circuit in and for Broward County, Florida, to the United States District Court for the Southern District of Florida, Fort Lauderdale Division. Tenet hereby provides "a short and plain statement of the grounds for removal" pursuant to 28 U.S.C. § 1446(a) and *Dart Cherokee Basin Operating Co., LLC v. Owens*, 574 U.S. 81, 87 (2014).

1. This Court has original jurisdiction over this action under the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d) ("CAFA"). In relevant part, CAFA grants district courts original jurisdiction over civil class actions filed under federal or state law in which any member of a class of plaintiffs is a citizen of a state different from any defendant, where the putative class includes more than 100 members, and where the amount in controversy for the putative class members in the aggregate exceeds the sum or value of $5 million, exclusive of interest and costs. As set forth

below, this case meets all of CAFA's requirements for original jurisdiction and removal and is timely and properly removed by the filing of this Notice.

VENUE

2. The State Court Action was filed in Broward County, Florida. Therefore, venue properly lies in the United States District Court for the Southern District of Florida, Fort Lauderdale Division. *See* 28 U.S.C. §§ 89(c), 1391.

PLEADINGS, PROCESS, AND ORDERS

3. On or about June 10, 2022, Plaintiffs Rob Brewster and Anita Goffman ("Plaintiffs") filed the State Court Action, on behalf of themselves and all others they claim to be similarly situated. In accordance with 28 U.S.C. § 1446(a), a true and correct copy of the Summons and Complaint filed in the State Court Action, which is the only process, pleadings, and orders served upon Tenet in the State Court Action, is attached as **Exhibit A** to this Notice. A true and correct copy of the docket in the State Court Action is attached as **Exhibit B** to this Notice. Copies of all other process, pleadings, and orders in the State Court Action, exclusive of the Summons and Complaint, are attached together as **Exhibit C** to this Notice.

4. According to the allegations in the Complaint, Plaintiffs and the members of the putative class they purport to represent are persons whose information was allegedly compromised "during the Cybersecurity Incident reported by Tenet on or about April 26, 2022." *See* Compl. ¶ 101.

5. The Complaint alleges three counts for: (1) negligence; (2) breach of express contract; and (3) breach of implied contract. *Id.* ¶¶ 117-155.

SERVICE ON THE STATE COURT

6. Pursuant to 28 U.S.C. § 1446(d), promptly after filing this Notice of Removal in the United States District Court for the Southern District of Florida, written notice of such filing will be given by the undersigned to Plaintiffs' counsel of record, and a copy of the Notice of Removal will be filed with the Clerk of the Circuit Court of the Seventeenth Judicial Circuit in and for Broward County, Florida.

TIMELINESS OF REMOVAL

7. Tenet was served with a copy of the Summons and Complaint on June 15, 2022. This Notice has been filed within thirty (30) days after Tenet was served with a copy of the Summons and Complaint and is therefore timely under 28 U.S.C. § 1446(b).

ORIGINAL JURISDICTION PURSUANT TO CAFA

8. This Court has jurisdiction over this case under CAFA, 28 U.S.C. § 1332(d), and this case may be removed pursuant to the provisions of 28 U.S.C. § 1441(a). As set forth more fully below, this is a civil putative class action wherein: (1) the proposed classes contain at least 100 members in the aggregate; (2) there is minimal diversity; (3) no defendant is a state, state official, or other governmental entity; (4) the total amount in controversy for all class members, based on the allegations of the Complaint, exceeds $5 million, exclusive of interest and costs; and (5) none of the exceptions to CAFA jurisdiction applies. CAFA authorizes removal of such actions in accordance with 28 U.S.C. § 1446. As discussed below, this case meets each CAFA requirement for removal.

The Proposed Class Contains At Least 100 Members in the Aggregate

9. Under CAFA, a "class action" is "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).

Plaintiffs allege that they "bring this nationwide class action on behalf of themselves and on behalf of all others similarly situated," citing Fla. R. Civ. P. 1.220 for support. Compl. ¶ 101. This meets CAFA's definition of a putative class action. *See* 28 U.S.C. § 1332(d)(1)(B).

10. Plaintiffs purport to bring claims on behalf of a putative class of individuals they define as: "All individuals residing in the United States whose information was accessed, viewed, copied, and/or acquired during the Cybersecurity Incident reported by Tenet on or about April 26, 2022." Compl. ¶ 101 (the "Nationwide Putative Class").

11. Plaintiffs estimate that the putative class contains "millions of individuals[.]" Compl. ¶ 104 ("[b]ased upon the 'millions' of patient encounters at Defendant's health system every year and the nature of Defendant's business, it is more **likely that there are millions of individuals** whose PII and PHI may have been improperly accessed in the Cybersecurity Incident.") (emphasis added).

12. Based on Plaintiffs' allegations in the Complaint, CAFA's 100-person requirement is satisfied. *See Roe v. Michelin N. Am., Inc.*, 613 F.3d 1058, 1061-62 (11th Cir. 2010) (courts may "make reasonable deductions, reasonable inferences, or other reasonable extrapolations" and "may use their judicial experience and common sense" in assessing federal jurisdictional requirements) (citations and quotations omitted); *see also Kelly v. State Farm Mut. Auto. Ins. Co.*, No. 5:10-cv-194-OC-32GRJ, 2010 WL 9888731, at *3 (M.D. Fla. Sept. 23, 2010) (concluding "CAFA's 100 person requirement" was satisfied because "Plaintiffs have alleged in the First Amended Class Complaint that it is believed the class contains more than 1,000 persons"), *report and recommendation adopted*, No. 5:10-cv-194-OC-32TEM, 2010 WL 10096066 (M.D. Fla. Nov. 9, 2010). Tenet has also reviewed its records and determined that there are more than 100 individuals whose information was involved in the cyberattack that gives rise to Plaintiffs' claims.

Minimal Diversity Exists

13. CAFA's diversity requirement is satisfied when at least one plaintiff is a citizen of a state different from any defendant. 28 U.S.C. §§ 1332(d)(2)(A), 1453.

14. Plaintiffs allege that they are both citizens of the state of Florida. Compl. ¶¶ 21, 22.

15. Tenet is incorporated in Nevada[1] and has its principal place of business in Texas. Compl. ¶ 23. Thus, Tenet is a citizen of Nevada and Texas. *See Hertz Corp. v. Friend*, 559 U.S. 77, 93 (2010); *see also* 28 U.S.C. § 1332(c)(1) (for diversity purposes, "a corporation shall be deemed to be a citizen of every State and foreign state by which it has been incorporated and of the State or foreign state where it has its principal place of business . . .").

16. CAFA's minimal diversity requirement is met here because at least one member of the putative class is a citizen of Florida, and Tenet is a citizen of Nevada and Texas.

No Defendant Is a Governmental Entity

17. Tenet, the only Defendant, is not a state, state official, or other governmental entity.

The Amount in Controversy Exceeds $5,000,000, Exclusive of Interest and Costs[2]

[1] Tenet Healthcare Corporation, SEC Form 10-Q for period ended March 31, 2022, https://s23.q4cdn.com/674051945/files/doc_financials/2022/q1/6b982089-1648-48d9-970b-eb244c1549fc.pdf (last visited Jul. 14, 2022).

[2] Though Tenet disputes that Plaintiffs are entitled to bring this action, vehemently denies liability, and contends that Plaintiffs and the members of the putative class can recover nothing under the claims in the Complaint, for purposes of removal only, Plaintiffs' allegations and the relief sought by Plaintiffs are to be considered in determining the value of the claims as pled and the amount in controversy. *See Brill v. Countrywide Home Loans, Inc.*, 427 F.3d 446, 448 (7th Cir. 2005) ("The question is not what damages the plaintiff will recover, but what amount is 'in controversy' between the parties. That the plaintiff may fail in its proof, and the judgment be less than the threshold (indeed, a good chance that the plaintiff will fail and the judgment will be zero) does not prevent removal."); *Dudley v. Eli Lilly & Co.*, 778 F.3d 909, 913 (11th Cir. 2014).

18. The "matter in controversy" exceeds $5 million, exclusive of interest and costs. *See* 28 U.S.C. § 1332(d)(2). The amount in controversy "is an estimate of the amount that will be put at issue in the course of the litigation." *Pretka v. Kolter City Plaza II, Inc.*, 608 F.3d 744, 751 (11th Cir. 2010) (quotation omitted). "[T]he plaintiffs' likelihood of success on the merits is largely irrelevant to the court's jurisdiction because the pertinent question is what is *in controversy* in the case, not how much the plaintiffs are ultimately likely to recover." *Id.* (quotation omitted); *S. Fla. Wellness v. Allstate Ins. Co.*, 745 F.3d 1312, 1315 (11th Cir. 2014) ("the amount [in controversy] is not discounted by the chance that the plaintiffs will lose on the merits").

19. The complaint does not state an amount in controversy, so this notice must contain only "a plausible allegation that the amount in controversy exceeds the jurisdictional threshold." *Dart Cherokee*, 574 U.S. at 89. "[T]he defendant's amount-in-controversy allegation should be accepted when not contested by the plaintiff or questioned by the court." *Id.* at 87; *see also Dudley*, 778 F.3d at 912 ("[A]ll that is required is a short and plain statement of the grounds for removal, including a plausible allegation that the amount in controversy exceeds the jurisdictional threshold. That is the end of the matter, unless the plaintiff contests, or the court questions, the defendant's allegation.") (internal quotations and citations omitted).

20. Tenet denies all liability on Plaintiffs' claims, denies that Plaintiffs could ever recover damages, and denies that a court could ever certify a class under Federal Rule of Civil Procedure 23. But accepting Plaintiffs' allegations are true—for removal purposes only—their putative class claims put more than $5 million, exclusive of interest and costs, in controversy. Plaintiffs allege that based on "the 'millions' of patient encounters at Defendant's health system every year" it is "likely that there are millions of individuals whose PII and PHI may have been improperly accessed in the Cybersecurity Incident." Compl. ¶ 104. Assuming for purposes of this

removal that there are one million putative class members—a plausible number given Plaintiffs' allegation that there are "millions" of individuals whose information may have been improperly accessed—then so long as Plaintiffs are seeking to recover more than $5 in damages per putative class member, the amount in controversy exceeds $5 million. The Complaint makes it clear that Plaintiffs seek far more than $5 per putative class member.

21. Plaintiffs seek a wide variety of damages, including: "all recoverable compensatory, statutory, nominal, and other damages sustained[.]" Compl. ¶ 156(b). Plaintiff Goffman claims she suffered identity theft in the form of fraudulent credit card charges "totaling over $600" as a result of the cyberattack. *Id.* ¶¶ 94, 97. In further support of their claimed damages, Plaintiffs generally point to a variety of other alleged "injuries", including diminished value of their information, out-of-pocket expenses associated with the prevention of and recovery from fraud, lost opportunity costs associated with alleged mitigation efforts, and the "present, continuing, and certainly increased risk to their PII and PHI[.]" *Id.* ¶ 19. Plaintiffs argue that "[t]ime is a compensable and valuable resource" and "seek remuneration for the loss of valuable time" spent monitoring their accounts and records. *Id.* ¶¶ 72-75. Plaintiffs further "seek a sum of money sufficient to provide to Plaintiffs and Class Members identity theft protective services for their respective lifetimes." *Id.* ¶ 71. Plaintiffs request numerous equitable and injunctive relief measures, such as "requiring Defendant to engage independent third-party security auditors" and "for a period of 10 years, appointing a qualified and independent third-party assessor to conduct a SOC 2 Type attestation on an annual basis[.]" *Id.* ¶ 156(d) (enumerating fifteen distinct injunctive relief measures sought).

22. To take one example, Plaintiff alleges that Tenet should pay for identity theft protective services for each putative class member's full lifetime. Compl. ¶ 71. Even assuming

conservatively that Plaintiffs were seeking identity theft protective services for only five years and that those services cost **only $1.01 *per year***, based on Plaintiffs' allegation that there are at least one million putative class members, then the amount in controversy would still exceed $5 million, exclusive of interest and costs.[3] Indeed, the monthly advertised rates for credit-monitoring services are much higher. For the three national credit-monitoring bureaus, these costs range between $9.95 and 19.95 per month (Equifax), $9.99 and $19.99 per month (Experian), and $29.95 per month (TransUnion). *See* Equifax, https://www.equifax.com/personal/ (last visited Jul. 14, 2022); Experian, https://www.experian.com/consumer-products/compare-identity-theft-products.html (last visited Jul. 14, 2022); TransUnion, https://www.transunion.com/hp202112A (last visited Jul. 14, 2022). Plaintiffs' claim for identity theft protective services alone puts more than $5 million, exclusive of interest and costs, at stake.

23. Numerous courts have considered the cost of identity theft protection and credit monitoring in evaluating CAFA jurisdiction in data breach cases. *See, e.g.*, *Porras*, 2016 WL 4051265, at *3 (C.D. Cal. July 25, 2016) (including cost of providing credit monitoring services in evaluating amount in controversy and assuming cost of $15.95 per month per putative class member); *Fielder v. Penn Station Inc.*, No. 1:12-cv-2166, 2013 WL 1869618, at *2 (N.D. Ohio May 3, 2013) (finding CAFA amount in controversy requirement satisfied in light of class size and cost of credit monitoring services); *McLoughlin v. People's United Bank, Inc.*, 586 F. Supp. 2d 70, 73 (D. Conn. 2008) (same).

[3] 1,000,000 (putative class members) multiplied by $1.01 (dollars per year) multiplied by 5 (years) equals $5,050,000 dollars. That amount would of course increase if it were assumed that the identity theft protective services cost more than $1.01 per year. In *Porras*, for example, a district court used a **monthly** rate of $15.95. *Porras v. Sprouts Farmers Mkt., LLC*, No. EDCV 16-1005 JGB (KKx), 2016 WL 4051265, at *3 (C.D. Cal. July 25, 2016).

24. While CAFA's amount in controversy threshold is easily satisfied based on the damages sought for identity theft protection services alone, the Complaint requests other forms of relief that also must be considered in the amount in controversy and that further demonstrate that CAFA's jurisdictional threshold is satisfied, including:

- **Disgorgement of proceeds** Tenet allegedly unjustly received from the members of the putative class. *See* Compl. ¶ 156(b); *Lorenzo v. MillerCoors LLC*, No. 16-20851-CV-KING, 2016 WL 9632955, at *2 (S.D. Fla. Jul. 21, 2016) (including "the monies for which Plaintiff seeks disgorgement" in assessing whether CAFA's $5 million amount in controversy was satisfied).
- **Declaratory and injunctive relief.** The value to the class of the requested relief must also be included in assessing the amount in controversy and is further evidence that CAFA's jurisdictional threshold is satisfied. *S. Fla. Wellness v. Allstate Ins. Co.*, 745 F.3d at 1316.

25. In sum, the Complaint places in controversy at least $5,000,000, and CAFA's jurisdictional threshold is satisfied.

The Exceptions to CAFA Do Not Apply

26. None of the exceptions to CAFA jurisdiction apply here. *See* 28 U.S.C. §§ 1332(d)(3-4). In any event, the burden to prove the applicability of an exception to jurisdiction under CAFA rests with the party opposing removal. *Breuer v. Jim's Concrete of Brevard, Inc.*, 538 U.S. 691, 698 (2003) (finding that once a defendant establishes removal is proper, "the burden is on a plaintiff to find an express exception"). Accordingly, it is not Tenet's burden to demonstrate that no exception to CAFA applies.

CONCLUSION

27. In conclusion, removal is appropriate under CAFA because (1) the proposed class contains at least 100 members; (2) at least one member of the proposed class is a citizen of a state different than Tenet; (3) the aggregate amount in controversy exceeds $5,000,000, exclusive of interest and costs; and (4) the procedural requirements for removal under 28 U.S.C. § 1446 have been met.

28. Accordingly, federal subject matter jurisdiction over this action exists.

29. Tenet reserves the right to amend this Notice of Removal.

WHEREFORE, Tenet removes the Action from the Circuit Court of the Seventeenth Judicial Circuit in and for Broward County, to this Court.

Dated: July 15, 2022

Respectfully submitted,

/s/ Kristine McAlister Brown

Kristine McAlister Brown
Florida Bar No. 443640
ALSTON & BIRD LLP
1201 West Peachtree Street
Atlanta, GA 30309
Phone: (404) 881-7000
Fax: (404) 881-7777
kristy.brown@alston.com

EXHIBIT A

Wolters Kluwer

CT Corporation
Service of Process Notification
06/15/2022
CT Log Number 541755908

Service of Process Transmittal Summary

TO: Olga Barnes
TENET HEALTHCARE CORPORATION
14201 NORTH DALLAS PARKWAY
DALLAS, TX 75254

RE: **Process Served in Florida**

FOR: Tenet Healthcare Corporation (Domestic State: NV)

ENCLOSED ARE COPIES OF LEGAL PROCESS RECEIVED BY THE STATUTORY AGENT OF THE ABOVE COMPANY AS FOLLOWS:

TITLE OF ACTION:	ROB BREWSTER and ANITA GOFFMAN, on behalf of themselves and all others similarly situated vs. TENET HEALTHCARE CORPORATION
DOCUMENT(S) SERVED:	Summons, Complaint, Exhibit(s)
COURT/AGENCY:	Broward County Circuit Court, FL Case # CACE22008510
NATURE OF ACTION:	04/26/2022
PROCESS SERVED ON:	C T Corporation System, Plantation, FL
DATE/METHOD OF SERVICE:	By Process Server on 06/15/2022 at 03:12
JURISDICTION SERVED:	Florida
APPEARANCE OR ANSWER DUE:	Within 20 days after service of this Summons upon you, exclusive of the day of service
ATTORNEY(S)/SENDER(S):	Patrick A. Barthle Morgan & Morgan Complex Litigation Group 201 N. Franklin Street, 7th Floor Tampa, FL 33602 813-223-5505
ACTION ITEMS:	CT has retained the current log, Retain Date: 06/15/2022, Expected Purge Date: 06/20/2022 Image SOP Email Notification, Olga Barnes olga.barnes@tenethealth.com Email Notification, Jennifer Cossa jennifer.cossa@tenethealth.com
REGISTERED AGENT CONTACT:	C T Corporation System 1200 South Pine Island Road Plantation, FL 33324 877-564-7529 MajorAccountTeam2@wolterskluwer.com

The information contained in this Transmittal is provided by CT for quick reference only. It does not constitute a legal opinion, and should not otherwise be relied on, as to the nature of action, the amount of damages, the answer date, or any other

information contained in the included documents. The recipient(s) of this form is responsible for reviewing and interpreting the included documents and taking appropriate action, including consulting with its legal and other advisors as necessary. CT disclaims all liability for the information contained in this form, including for any omissions or inaccuracies that may be contained therein.

Wolters Kluwer

PROCESS SERVER DELIVERY DETAILS

Date: Wed, Jun 15, 2022
Server Name: Eric Deal

Entity Served	Tenet Healthcare Corporation
Case Number	CACE-22-008510 Division: 03
Jurisdiction	FL

Inserts		

Case Number: CACE-22-008510 Division: 03
Filing # 151298203 E-Filed 06/10/2022 05:23:40 PM

IN THE CIRCUIT COURT FOR THE SEVENTEENTH JUDICIAL CIRCUIT IN AND FOR BROWARD COUNTY, FLORIDA

ROB BREWSTER and ANITA GOFFMAN,

on behalf of themselves and all others similarly situated,

Plaintiffs,

vs.

TENET HEALTHCARE CORPORATION, d/b/a TENET

Defendant.

Case No.:

DEMAND FOR JURY TRIAL

Date: 6-15-22 Time: 1:00 PM

Eric Deal S.P.S. 336

SUMMONS

THE STATE OF FLORIDA:

To all and singular Sheriffs of said state:

YOU ARE HEREBY COMMANDED to serve this Summons and a copy of the Complaint, in the above-styled cause upon the Defendant:

Tenet Healthcare Corporation
c/o Registered Agent
C T CORPORATION SYSTEM
1200 SOUTH PINE ISLAND RD.
PLANTATION, FL 33324

Each Defendant is hereby required to serve written defenses to said Complaint or Petition on:

Patrick A. Barthle, Esquire
Morgan & Morgan Complex Litigation Group
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602

(813) 223-5505 // FAX: (813) 223-5402
E-Mail: pbarthle@forthepeople.com
jcabezas@forthepeople.com

within *twenty (20) days* after service of this Summons upon you, exclusive of the day of service, and to file the original of said written defenses with the Clerk of said Court either before service on Plaintiff's attorney or immediately thereafter. If you fail to do so, a default will be entered against you for the relief demanded in the Complaint or Petition.

"If you are a person with a disability who needs any accommodation in order to participate in this proceeding, you are entitled, at no cost to you, to the provision of certain assistance. Please contact the ADA Coordinator, Room 20140, 201 S.E. Sixth Street, Fort Lauderdale, Florida 33301, 954-831-7721 at least 7 days before your scheduled court appearance, or immediately upon receiving this notification if the time before the scheduled appearance is less than 7 days. If you have a hearing or voice disability you can contact the court through the Florida Relay Service by calling 711."

WITNESS my hand and the seal of this Court on this the _____ day of JUN 13 2022 2022.

CLERK OF THE CIRCUIT COURT

By: _____
as Deputy Clerk

CLERK OF CIRCUIT & COUNTY COURT IN GOD WE TRUST FLORIDA

BRENDA D. FORMAN

Filing # 151298203 E-Filed 06/10/2022 05:23:40 PM

IN THE CIRCUIT COURT FOR THE SEVENTEENTH JUDICIAL CIRCUIT IN AND FOR BROWARD COUNTY, FLORIDA

ROB BREWSTER and ANITA GOFFMAN, on behalf of themselves and all others similarly situated, Plaintiffs, vs. TENET HEALTHCARE CORPORATION, d/b/a TENET Defendant.	Case No.: **CLASS ACTION COMPLAINT** DEMAND FOR JURY TRIAL

Plaintiffs Rob Brewster and Anita Goffman, individually and on behalf of a putative class of all other similarly situated persons ("Class Members" or the "Class"), file this Complaint against Defendant Tenet Healthcare Corporation (hereinafter Defendant or "Tenet") and would respectfully show as follows:

I. INTRODUCTION

1. Plaintiffs bring this class action against Defendant for its failure to properly secure and safeguard the sensitive personally identifiable information (PII) and protected health information (PHI) of individuals, including but not limited to current and former patients and/or employees, whose PII and PHI it stored on its internal systems. Plaintiffs allege that Defendant failed to comply with industry standards to protect information systems that contain PII and PHI

and, as a result, Defendant's systems containing patient PII and PHI and electronic health records ("EHR") experienced unauthorized access and activity. Plaintiff seek, among other things, orders requiring Defendant to fully and accurately disclose the nature of the information that has been compromised, to adopt reasonably sufficient security practices and safeguards to prevent incidents like the disclosure in the future, to destroy information no longer necessary to retain for purposes for which the information was first obtained from Class Members, and to provide a sum of money sufficient to provide to Plaintiffs and Class Members identity theft protective services for their respective lifetimes as Plaintiffs and Class Members will be at an increased risk of identity theft due to the conduct of Tenet as described herein.

2. Tenet is one of the largest for-profit health systems in the United States.[1] In 2021, Tenet reported $19.45 billion ($19,485,000,000) in revenue.[2] Tenet operates "an expansive network across the country, with 60 hospitals and approximately 550 other healthcare facilities."[3]

3. In 2021 alone, Tenet had over 8.5 million "patient encounters."[4] In relation to these patient encounters, Defendant collects and retains the PII and PHI of its current and former patients. In the ordinary course of these services, individuals such as Plaintiffs are regularly required to provide their PII and PHI to Defendant directly.

4. According to public reporting, on or about April 20, 2022, hospitals connected to Tenet's IT systems began experiencing outages of their information technology systems,

---

[1] 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/.

[2] https://www.wsj.com/market-data/quotes/THC/company-people (last visited May 11, 2022).

[3] *Tenet Healthcare 2022 Proxy Statement*, at 7, *available at* https://s23.q4cdn.com/674051945/files/doc_financials/2022/q1/Tenet-Healthcare-2022-Proxy-Statement.pdf (last visited May 11, 2022).

[4] *Id.*

including network and telecom services.[5] The interruptions at Tenet-owned hospitals continued through at least April 26, 2022.[6]

5. On April 26, 2022, Tenet posted a statement "Tenet Reports Cybersecurity Incident" ("Website Notice") announcing a "cybersecurity incident" involving unauthorized activity on its network that began the prior week (the "Cybersecurity Incident").[7]

6. In the Website Notice, Tenet states it "immediately suspended user access to impacted information technology applications, executed extensive cybersecurity protection protocols, and quickly took steps to restrict further unauthorized activity."[8]

7. In its Website Notice, Tenet confirmed the Cybersecurity Incident and that information technology applications were subject to unauthorized access and activity.[9] However, the Website Notice provides scant other information, including precisely whether, how much, and what types of information was accessed and/or copied, the exact causes of the Cybersecurity Incident, and how long these unauthorized third parties had access to the hospital systems containing the PII and PHI of Plaintiffs and Class Members.

8. This is not Defendant's first experience with unauthorized activity and/or exposure of sensitive information – Tenet has twice reported exposures of confidential patient data that included PII and PHI.[10] Plaintiffs and Class Members demand security to protect

---

[5] Dave Bohman, *Timeline gives insight into cybersecurity breach at West Palm Beach hospital,* WPTV WEST PALM BEACH, INVESTIGATIONS (Apr. 26, 2022) https://www.wptv.com/news/local-news/investigations/timeline-gives-insight-into-cybersecurity-breach-at-west-palm-beach-hospital

[6] Jessica Davis, *Tenet Health investigating cybersecurity incident, IT outage*, SCMAGAZINE (Apr. 26, 2022), https://www.scmagazine.com/analysis/cybercrime/tenet-health-investigating-cybersecurity-incident-it-outage (last visited May 11, 2022).

[7] Exhibit 1 ("Website Notice").

[8] *Id.*

[9] *Id.*

[10] Steve Adler, *Data Privacy Breach to Cost Tenet Healthcare up to $32.5 Million*, HIPPA JOURNAL (Oct. 23, 2014), https://www.hipaajournal.com/data-privacy-breach-cost-tenet-healthcare-32-5-million/; Jaikumar Vijayan, *Tenet Healthcare Warns 37,000 Patients of Data Compromise*, COMPUTERWORLD (Feb. 21, 2008), https://www.computerworld.com/article/2537390/tenet-healthcare-warns-37-000-patients-of-data-compromise.html.

themselves from any possible further exposure of their PII and PHI by Defendant.

9. Defendant has a posted "Notice of Privacy Practices," last modified and effective March 1, 2021, wherein it acknowledges its privacy obligations and acknowledges that Tenet is also "required to notify you if there is a breach or impermissible access, use or disclosure of your medical information."[11]

10. Defendant's Notice of Privacy Practices lists certain circumstances wherein the PII and PHI of its patients may be shared without prior consent, none of which are applicable here.

11. The healthcare sector is a favored target by cybercriminals, yet recent studies, including one by the Massachusetts Institute of Technology, found hospitals lagged behind other businesses in safeguarding their computer systems.[12] 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."[13]

12. This case involves just such a breach of a computer system by an unknown third-party, and, accordingly, is 93 % likely to have resulted in the unauthorized access, disclosure, and/or acquisition of the PII and PHI of Plaintiffs and Class Members to unknown third-parties. As a result of Defendant's failure to implement and follow basic security procedures, the PII and PHI of Plaintiffs and Class Members was more likely than not accessed, disclosed, and/or acquired and is now in the hands of criminals. Plaintiffs and Class Members now and will forever face a substantial increased risk of identity theft. Consequently, Plaintiffs and Class Members have had to spend, and will continue to spend, significant time and money in the future to protect

[11] Exhibit 2 ("Notice of Privacy Practices"), p. 1.
[12] 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/.
[13] 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.

themselves due to Tenet's failures.

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

14. By obtaining, collecting, using, and deriving a benefit from the PII and PHI of Plaintiffs 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.

15. Defendant's internal systems contain millions of individuals' detailed medical records, PHI, and PII. Defendant admits that the Cybersecurity Incident involved unauthorized access and activity on their internal systems.[14]

16. Time is of the essence when highly sensitive PII and PHI is subject to unauthorized access and/or acquisition. The actually or potentially disclosed, accessed, and/or acquired PII and PHI of Plaintiffs and Class Members can be sold on the dark web. Hackers can access and then offer for sale the unencrypted, unredacted PII and PHI to criminals. Plaintiffs and Class Members now face a lifetime risk of identity theft, which is heightened here by unauthorized access, disclosure, and/or activity by cybercriminals on computer systems containing millions of Social Security numbers and/or specific, sensitive medical information.

17. The Cybersecurity Incident occurred due to Defendant's negligent and/or careless acts and omissions and the failure to protect the PII and PHI of Plaintiffs and Class Members. Defendant has not yet provided notice of the Cybersecurity Incident to Plaintiffs and Class Members and still maintains as secret the specific vulnerabilities and root causes of the

[14] Ex. 1.

Cybersecurity Incident. Plaintiffs and Class Members also remain unaware of precisely what information was accessed and subject to unauthorized activity and for how long.

18. Plaintiffs brings this action on behalf of all persons whose PII and PHI was compromised as a result of Defendant's failure to adequately protect the PII and PHI of Plaintiffs and Class Members and failure to warn Plaintiffs and Class Members of Defendant's inadequate information security practices. Defendant's conduct amounts to negligence and violates state statutes.

19. Plaintiffs and Class Members have suffered injury as a result of Defendant's conduct. These injuries include: (i) lost or diminished value of PII and PHI; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII and PHI; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Cybersecurity Incident, including but not limited to lost time; and, significantly (iv) the present, continuing, and certainly increased risk to their PII and PHI, which: (a) may remain unencrypted and available for unauthorized third-parties to access and abuse; and (b) 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 and PHI; and (v) nominal damages.

20. Plaintiffs 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

21. Plaintiff Rob Brewster is an individual residing in Palm Beach County, Florida and is a Citizen of the State of Florida.

22. Plaintiff Anita Goffman is an individual residing in Palm Beach County and is a Citizen of the State of Florida.

23. Defendant Tenet Healthcare Corporation ("Tenet") is a Texas-based corporation that is registered to do business in Florida,[15] owns and operates over 80 healthcare facilities in Florida, including Good Samaritan Hospital, and does substantial business in Florida.[16] Defendant Tenet may be served with process in Florida by serving its registered agent at C T Corporation System, 1200 South Pine Island Rd, Plantation, FL 33324.[17]

III. JURISDICTION AND VENUE

24. The Court has subject matter jurisdiction over Plaintiffs' claims under Florida Stat. § 26.012 and § 86.011. This Court has jurisdiction over this dispute because this complaint seeks damages in excess of $30,000.00 dollars, exclusive of interest and attorneys' fees.

25. The Court has personal jurisdiction over Defendant under Florida Stat. § 48.193, because Defendant personally or through its agents operated, conducted, engaged in, or carried on a business or business venture in Florida; had offices in Florida; committed tortious acts in Florida; and breached a contract in Florida by failing to perform acts required by the contract to be performed in Florida.

26. Venue is proper in Broward County pursuant to Florida Stat. § 47.011 and § 47.051 because Defendant is a foreign corporation doing business in Florida whose agent is

---

[15] *Application by Foreign Corporation to Transact Business in Florida* (Dec. 12, 2002), *available at* http://search.sunbiz.org/Inquiry/CorporationSearch/ConvertTiffToPDF?storagePath=COR1%5C2003%5C0317%5C40680894.Tif&documentNumber=F03000001277.

[16] Defendant's parent corporation is headquartered at 1445 Ross Ave, Suite 1400, Dallas, TX 75202. NIACS Profile Page, *Tenet Healthcare Corporation*, https://www.naics.com/company-profile-page/?co=4836 (last visited May 12, 2022). Defendant owns and operates many subsidiary corporations and/or is the majority shareholder in numerous corporations based in Florida that are subject to the allegations in this complaint. Tenet Health, *Locations*, https://www.tenethealth.com/locations (last visited May 12, 2022).

[17] http://search.sunbiz.org/Inquiry/CorporationSearch/GetDocument?aggregateId=domp-p01000035382-9e6cc920-7d90-437d-a3aa-ad0d7c3fb6b4&transactionId=p01000035382-7293949c-ee19-4df4-ab46-0cc2c63bc147&formatType=PDF

located in Broward County, the events giving rise to the causes of action alleged in this complaint accrued in Broward County, and Defendant has an office for the transaction of its customary business in Broward County.

IV. FACTUAL ALLEGATIONS

A. Background

27. Tenet is one of the largest for-profit health systems in the United States.[18] Tenet operates "an expansive network across the country, with 60 hospitals and approximately 550 other healthcare facilities."[19]

28. Tenet operates eighty (80) facilities and hospitals throughout Florida.[20] In 2001, Tenet acquired Good Samaritan Hospital and St. Mary's Medical Center.[21]

29. Tenet is a publicly traded company and, in 2021, Tenet reported $19.45 billion ($19,485,000,000) in revenue.[22]

30. In 2021 alone, Tenet had over 8.5 million "patient encounters."[23]

31. In relation to these patient encounters, Defendant collects and retains the PII and PHI of its current and former patients.

32. In the ordinary course of these services, individuals such as Plaintiffs are regularly required to provide their PII and PHI to Defendant directly.

---

[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] *Tenet Healthcare 2022 Proxy Statement*, at 7, *available at* https://s23.q4cdn.com/674051945/files/doc_financials/2022/q1/Tenet-Healthcare-2022-Proxy-Statement.pdf (last visited May 11, 2022).

[20] Tenet Health, Locations, https://www.tenethealth.com/locations (last visited May 12, 2022).

[21] Stacey Singer, *St. Mary's Good Sam Being Sold to Tenet*, SOUTH FLORIDA SUN SENTINEL (Mar. 23, 2001), *available at* https://www.sun-sentinel.com/news/fl-xpm-2001-03-23-0103230237-story.html (last visited June 1, 2022)

[22] Tenet Healthcare Company Market Data, WALL ST. J., https://www.wsj.com/market-data/quotes/THC/company-people (last visited May 11, 2022).

[23] *Id.*

33. Plaintiffs and Class Members are Defendant's current and former patients and/or employees who provided their sensitive personal information to Defendant as a condition of receiving healthcare services and/or employment.

34. Plaintiffs and the Class Members entrusted this sensitive and confidential information to this highly sophisticated and well-funded Defendant to store and manage. Importantly, many pieces of the information provided to Tenet—such as Social Security Numbers—are static, do not change, and can be used to commit myriad financial crimes.

35. Defendant's Information Privacy and Security policy states that Tenet respects the privacy of every patient's medical information, as well as the rights patients have with respect to their medical information.[24]

36. Further, Defendant has a posted "Notice of Privacy Practices," last modified and effective March 1, 2021, wherein it acknowledges its privacy obligations and acknowledges that Tenet is also "required to notify you if there is a breach or impermissible access, use or disclosure of your medical information."[25]

37. Defendant's Notice of Privacy Practices lists certain circumstances wherein the PII and PHI of its patients may be accessed, subjected to disclosure, or shared without prior consent, none of which are applicable here.

38. Defendant, in its Notice of Privacy Practices, acknowledges its obligation to keep PHI and PII confidential and securely maintained. Further, because of its two previous data security breaches that resulted in exposures of confidential patient data that included PII and PHI,

[24] *Tenet Health*, Information Privacy and Security Administration, https://www.tenethealth.com/about/ethics-compliance (under Information Privacy and Security tab, EC.PS.02.00 Patient Information Privacy Policy), *available at* https://tenet.policytech.com/dotNet/documents/?docid=94234&anonymous=true (last visited May 12, 2022).

[25] Ex. 2.

Defendant is aware of the steep consequences of insufficient cybersecurity.[26] Plaintiffs and Class Members demand security to protect themselves from any possible further exposure of their PII and PHI by Defendant.

39. 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.[27] Indeed, just days before Tenet's networks crashed on April 20, 2022, HHS's cybersecurity arm issued yet another warning about increased cyberattacks that urged vigilance with respect to data security.[28]

40. Plaintiffs and Class Members relied on this sophisticated Defendant to keep their PII confidential and securely maintained, to use this information for authorized and appropriate purposes only, and to make only authorized disclosures of this information. Plaintiffs and Class Members demand security to safeguard their PII and PHI.

41. Defendant had a duty to adopt reasonable measures to protect the PII and PHI of Plaintiffs and Class Members from involuntary disclosure to third parties.

B. The Cybersecurity Incident

42. According to public reporting, on or about April 20, 2022, hospitals owned by

---

[26] Steve Adler, *Data Privacy Breach to Cost Tenet Healthcare up to $32.5 Million*, HIPPA JOURNAL (Oct. 23, 2014) https://www.hipaajournal.com/data-privacy-breach-cost-tenet-healthcare-32-5-million/; Jaikumar Vijayan, *Tenet Healthcare Warns 37,000 Patients of Data Compromise*, COMPUTERWORLD (Feb. 21, 2008), https://www.computerworld.com/article/2537390/tenet-healthcare-warns-37-000-patients-of-data-compromise.html.

[27] 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/.

[28] *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.").

Tenet and connected to Tenet's IT systems began experiencing outages of their information technology systems, including network and telecom services.[29]

43. Upon information and belief, hospitals throughout the country connected to Tenet's Dallas-based IT network were affected. For example, in Massachusetts, hospitals owned by Tenet reported to city services that the hospital was experiencing a "code black."[30] In Florida, employees at hospitals owned by Tenet reported significant outages that forced staff to divert patients, use only patient-reported medical records, use only paper to record-keep and chart for patients, and/or make necessary phone calls outside of the hospital. [31]

44. Specifically, according to local news reporting, on or about April 20, 2022, Tenet's employees were instructed to "log off and turn off" all computers and that no electronic systems were to be used, even if they "appeared to be working."[32] At that point, EMTs began diverting patients to other medical centers.[33] Further, medical staff reported that they were relying on paper records and physically leaving the hospital to use phones.[34]

45. The interruptions at some Tenet-owned hospitals continued through April 26, 2022.[35]

---

[29] Dave Bohman, *Timeline gives insight into cybersecurity breach at West Palm Beach hospital,* WPTV WEST PALM BEACH, INVESTIGATIONS (Apr. 26, 2022), https://www.wptv.com/news/local-news/investigations/timeline-gives-insight-into-cybersecurity-breach-at-west-palm-beach-hospital (last visited May 15, 2022).

[30] "According to a MetroWest Medical Center staffer, who wished to remain anonymous, when a code black is called it means the hospital can not handle anymore patients and the patients currently in the ER could be a risk." FRAMINGHAM SOURCE, *UPDATED: MetroWest Medical Center Turned Away Ambulances & Patients Earlier Today* (Apr. 20, 2022), https://framinghamsource.com/index.php/2022/04/20/updated-metrowest-medical-center-turned-away-ambulances-patients-earlier-today/ (last visited May 11, 2022).

[31] Dave Bohman, *Timeline gives insight into cybersecurity breach at West Palm Beach hospital,* WPTV WEST PALM BEACH, INVESTIGATIONS (Apr. 26, 2022) https://www.wptv.com/news/local-news/investigations/timeline-gives-insight-into-cybersecurity-breach-at-west-palm-beach-hospital (last visited May 15, 2022).

[32] *Id.*

[33] *Id.*

[34] Naomi Diaz, *Tenet reports cybersecurity incident took down 2 Florida hospitals*, BECKER HOSPITAL REVIEW (Apr. 25, 2022), https://www.beckershospitalreview.com/cybersecurity/tenet-reports-it-problems-at-2-florida-hospitals.html.

[35] Jessica Davis, *Tenet Health investigating cybersecurity incident, IT outage*, SCMAGAZINE (Apr. 26, 2022), https://www.scmagazine.com/analysis/cybercrime/tenet-health-investigating-cybersecurity-incident-it-outage.

46. On April 26, 2022, Tenet posted a statement "Tenet Reports Cybersecurity Incident" ("Website Notice") announcing a "cybersecurity incident" involving unauthorized activity on its network that began the prior week.[36] Upon discovering the cybersecurity incident, Tenet states it "immediately suspended user access to impacted information technology applications, executed extensive cybersecurity protection protocols, and quickly took steps to restrict further unauthorized activity."[37]

47. In its Website Notice, Tenet confirmed the Cybersecurity Incident and that information technology applications were subject to unauthorized activity.[38] However, the Website Notice provides scant other information, including precisely whether, how much, and what types of information was accessed and/or copied, the exact causes of the Cybersecurity Incident, and how long these unauthorized third parties had access to the hospital systems containing the PII and PHI of Plaintiffs and Class Members. Indeed, efforts by reporters to determine whether patient and employee information was compromised went unanswered by Defendant.[39]

48. Defendant claims that upon detecting the unauthorized activity, it "quickly took steps to restrict further unauthorized activity." Further, Defendant states that, as of April 26, 2022 "efforts to restore impacted information technology operations continue to make important progress" and Tenant was "taking additional measures to protect patient, employee and other data,

---

[36] Ex. 1.
[37] *Id.*
[38] *Id.*
[39] *See, e.g.*, Dave Bohman, *Timeline gives insight into cybersecurity breach at West Palm Beach hospital,* WPTV WEST PALM BEACH, INVESTIGATIONS (Apr. 26, 2022) https://www.wptv.com/news/local-news/investigations/timeline-gives-insight-into-cybersecurity-breach-at-west-palm-beach-hospital ("WPTV called the number and emailed the address Tenet Health Systems listed in its news release to ask them if patient and employee information was compromised. However, they did not respond."); 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/ ("Both the company and [its spokesperson] Friedberg declined to say how the security breach occurred or detail the impacts it had on hospital operations. They didn't say whether any patient records were compromised.").

as appropriate, in response to this incident."[40] However, the details of the root cause of the Cybersecurity Incident, the vulnerabilities exploited, and the adequacy of any remedial measures undertaken to ensure a breach does not occur again have not been shared with regulators or Plaintiffs and Class Members, who retain a vested interest in ensuring that their information remains protected.

49. The PII and PHI of Plaintiffs and Class Members may end up for sale on the dark web, or simply fall into the hands of companies that will use the detailed PII and PHI for targeted marketing without the approval of Plaintiffs and Class Members.

50. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive information it maintained and stored belonging Plaintiffs and Class Members, resulting in the unauthorized access, disclosure, and/or acquisition of PII and PHI.

C. Defendant Acquires, Collects, and Stores the PII and PHI of Plaintiffs and Class Members

51. Defendant acquired, collected, and stored the PII and PHI of Plaintiffs and Class Members.

52. As a condition of obtaining healthcare services from Defendant, individuals entrusted Defendant with highly confidential PII and PHI. By obtaining, collecting, and storing the PII and PHI of Plaintiffs and Class Members, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting the PII and PHI from disclosure.

53. Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality of their PII and PHI and implicitly relied on Defendant to keep their PII and PHI confidential and securely maintained, to use this information for authorized purposes only, and to

[40] Ex 2.

make only authorized disclosures of this information.

D. Securing PII/PHI and Preventing Breaches

54. Defendant could have prevented this Cybersecurity Incident by properly securing the files and file servers containing the PII and PHI of Plaintiffs and Class Members. Alternatively, Defendant could have destroyed the data, especially outdated information.

55. Defendant's negligence in safeguarding the PII of Plaintiffs and Class Members is exacerbated by the repeated warnings and alerts directed to protecting and securing this sensitive data.

56. Despite the prevalence of public announcements of data breach and data security compromises, as detailed above, Defendant failed to take appropriate steps to protect the PII and PHI of Plaintiffs and Class Members from being compromised.

57. In the context of data breaches, healthcare is "by far the most affected industry sector."[41] 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 and PHI.[42] 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*."[43]

58. Tenable found that the damages are particularly acute in the context of breaches at hospital systems, "[b]ecause such systems can include multiple facilities spread across a number of campuses, the impact of [those healthcare system breaches] is exponentially worse than if they

[41] 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

[42] *See id.*

[43] 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.

had occurred in an individual, standalone facility such as a single hospital."[44]

59. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[45] 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."[46]

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

E. Value of Personal Identifiable Information

61. The PII 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.[47] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[48] Criminals can also purchase access to entire

---

[44] Samantha Schwartz, *55% of healthcare breaches feature ransomware:* report, CYBERSECURITYDIVE (Mar. 10, 2021) https://www.cybersecuritydive.com/news/ransomware-data-breach-healthcare-cost-tenable/596451/ (citing 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).

[45] 17 C.F.R. § 248.201 (2013).

[46] *Id.*

[47] *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 May 12, 2022).

[48] *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 May 12, 2022).

company data breaches from $900 to $4,500.[49]

62. 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 may be 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.[50]

63. 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.

64. 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

---

[49] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last visited May 12, 2022).

[50] 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 May 12, 2022).

into the new Social Security number."[51]

65. Based on the foregoing, the information potentially compromised in the Cybersecurity Incident is 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 potentially compromised in this Cybersecurity Incident is impossible to "close" and difficult, if not impossible, to change—name and Social Security number.

66. 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 in price on the black market."[52]

67. 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.

68. The PII and PHI of Plaintiffs and Class Members was potentially accessed by, disclosed to, and/or acquired by hackers to engage in identity theft or and or to sell it to other criminals who will purchase the PII and PHI for that purpose. The fraudulent activity resulting from the Cybersecurity Incident may not come to light for years.

69. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII and PHI 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

[51] 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 May 12, 2022).

[52] 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 May 12, 2022).

> 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.[53]

F. Defendant's Conduct Violates Florida's Privacy and Data Security Laws

70. The Florida Information Protection Act of 2014, Fla. Stat. § 501.171, *et seq.* ("FIPA") is "one of the broadest and most encompassing data security breach laws in the nation," and imposes a statutory requirement upon covered entities, such as Defendant, to safeguard Floridians' personal information, to report a breach to the state attorney general, and to comply with other affirmative obligations.[54] One such obligation is to provide notice of a breach of cybersecurity to affected individuals within 30 days of an incident. As of the date of filing of this complaint, Defendant has not yet provided individuals with such sufficient notice.

71. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII and PHI of Plaintiffs and Class Members, including Social Security numbers, and of the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiffs and Class Members as a result of a breach. As another element of damages. Plaintiffs and Class Members seek a sum of money sufficient to provide to Plaintiffs and Class Members identity theft protective services for their respective lifetimes.

72. Moreover, Defendant put the burden squarely on Plaintiffs and Class Members to

---

[53] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* https://www.gao.gov/assets/gao-07-737.pdf (last visited May 12, 2022).

[54] Though FIPA does not provide individuals with a private right of action, it serves as evidence for the standard of care with which Defendant more than likely failed to comply. Florida Information Protection Act of 2014, Fla. Stat. § 501.171, *et seq.*; *see also* Joseph Lazzarotti, *New Florida Data Security and Breach Law Effective July 1*, JACKSONLEWIS (June 26, 2014), *available at* https://www.jacksonlewis.com/resources-publication/new-florida-data-security-and-breach-law-effective-july-1 (last visited May 31, 2022).

investigate the Cybersecurity Incident, among other steps Plaintiffs 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.[55]

73. 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;[56] leisure time is defined as time not occupied with work or chores and is "the time equivalent of 'disposable income.'"[57] Usually, this time can be spent at the option and choice of the consumer, however, having heard of the Cybersecurity Incident – whether through news reporting or from Defendant's press release – these 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.

74. Plaintiffs 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.

75. Plaintiffs and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII and PHI.

---

[55] 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 May 23, 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 May 23, 2022) (finding that on average, private-sector workers make $1,253 per 40-hour work week.).

[56] *See* James Wallman, *How Successful People Spend Leisure Time*, CNBC (Nov. 6, 2019), *available at* https://www.cnbc.com/2019/11/06/how-successful-people-spend-leisure-time-james-wallman.html (last visited May 23, 2022).

[57] *Id.*

76. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on its file servers, amounting to potentially tens of millions of individuals' detailed, personal information and thus, the significant number of individuals who would be harmed by the exposure of the data.

77. To date, Defendant has offered no recourse for affected individuals and has not provided any resources to protect Plaintiffs or Class Members from further injury.

78. The injuries to Plaintiffs and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the PII and PHI of Plaintiffs and Class Members.

79. Plaintiffs seek, among other things, orders requiring Defendant to fully and accurately disclose the nature of the information that has been compromised, to adopt reasonably sufficient security practices and safeguards to prevent incidents like the disclosure in the future, to destroy information no longer necessary to retain for purposes for which the information was first obtained from Class Members, and to provide a sum of money sufficient to provide Plaintiff and Class Members identity theft protective services for their respective lifetimes, as Plaintiff and Class Members will be at an increased risk of identity theft due to the conduct of Tenet as described herein.

G. Plaintiff Rob Brewster's Experience

80. Plaintiff Rob Brewster is a patient of one of Tenet's hospitals, Good Samaritan Medical Center. Plaintiff Brewster last visited Good Samaritan Medical Center on or about April 5, 2022, approximately two weeks before the Cybersecurity Incident began

81. As a condition of that relationship, Plaintiff Brewster was required to provide and entrust his PII, including his name and Social Security number, to Defendant.

82. At the time of the Cybersecurity Incident, Defendant retained, among other personal information, the PII and PHI of Plaintiff and other individuals in its internal, administrative system.

83. As a result of the Cybersecurity Incident notice, Plaintiff spent time dealing with the consequences of the Cybersecurity Incident, which includes time spent verifying the legitimacy of the Cybersecurity Incident and self-monitoring his accounts. Plaintiff has spent many hours of his time attempting to rectify the consequences of the Cybersecurity Incident. This time has been lost forever and cannot be recaptured.

84. Additionally, Plaintiff is very careful about sharing his sensitive PII. He has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

85. Plaintiff stores any documents containing his sensitive PII or PHI in a safe and secure location or destroys the documents. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

86. Plaintiff suffered actual injury in the form of damages to and diminution in the value of his PII and PHI — a form of intangible property that Plaintiff entrusted to Defendant for the purpose of receiving healthcare services, which was potentially compromised in and as a result of the Cybersecurity Incident.

87. Plaintiff suffered lost time, annoyance, interference, and inconvenience as a result of the Cybersecurity Incident and has anxiety and increased concerns for the loss of his privacy. Plaintiff has taken time to freeze his credit, contact his bank, relevant credit bureaus, and his credit card providers to alert them of this incident. This is time that cannot be recovered.

88. Plaintiff has suffered injury arising from the present and continuing risk of fraud, identity theft, and misuse resulting from his PII and PHI, especially his Social Security number in

combination with his name, potentially being placed in the hands of unauthorized third parties and possibly criminals.

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

H. Plaintiff Anita Goffman's Experience

90. Plaintiff Anita Goffman is a patient of St. Mary's Medical Center. Plaintiff Goffman is also a former employee of Tenet. Plaintiff Goffman retired from her position at Tenet in approximately 1990.

91. Plaintiff Goffman first visited St. Mary's Medical Center on or about December 24, 2021, and has returned twice a for treatment. To pay for Defendant's services, Plaintiff used her Visa credit card at least ten times to pay for her appointment.

92. As a condition of her relationship with Defendant, Plaintiff Goffman was also required to provide and entrust her PII, including her name and Social Security number, to Defendant.

93. At the time of the Cybersecurity Incident, Defendant retained, among other personal information, including Plaintiff Goffman's Visa credit card information, along with the PII and PHI of Plaintiff and other individuals in its internal, administrative system.

94. On or about May 26, 2022, after hearing of the Cybersecurity Incident, Plaintiff was notified of potential fraudulent charges on her Visa credit card. After checking her statement, she found several unauthorized and fraudulent charges at various retailers totaling over $600. As a result, Plaintiff spent time dealing with the consequences of the Cybersecurity Incident, which includes time spent verifying the legitimacy of the Cybersecurity Incident and self-monitoring

her accounts, contacting her bank and credit card company to attempt to deal with the fraudulent charges, and contacting her service providers to update her credit card information. Plaintiff has spent many hours of her time attempting to rectify the consequences of the Cybersecurity Incident. This time has been lost forever and cannot be recaptured.

95. Additionally, Plaintiff is very careful about sharing her sensitive PII. She has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

96. Plaintiff stores any documents containing her sensitive PII or PHI in a safe and secure location or destroys the documents. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

97. Plaintiff suffered identity theft in the form of fraudulent charges on her Visa credit card shortly after the Cybersecurity Incident. Further, Plaintiff suffered additional actual injury in the form of damages to and diminution in the value of her PII and PHI — a form of intangible property that Plaintiff entrusted to Defendant for the purpose of receiving healthcare services, which was also potentially compromised in and as a result of the Cybersecurity Incident.

98. Plaintiff suffered lost time, annoyance, interference, and inconvenience as a result of the Cybersecurity Incident and has anxiety and increased concerns for the loss of her privacy. On top of the time spent dealing with the fraudulent charges, Plaintiff has taken time to freeze her credit, contact her bank, relevant credit bureaus, and her credit card providers to alert them of this incident. This is additional time that cannot be recovered.

99. In addition to the fraudulent charges Plaintiff suffered as a result of her PII being placed in the hands of unauthorized individuals, Plaintiff has suffered additional injury arising from present and continuing risk of fraud, identity theft, and misuse resulting from her PII and PHI, especially her Social Security number in combination with her name, potentially also being placed

in the hands of unauthorized third parties and possibly criminals.

100. Plaintiff has a continuing interest in ensuring that her PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

V. CLASS ALLEGATIONS

101. Plaintiffs bring this nationwide class action on behalf of themselves and on behalf of all others similarly situated pursuant to Rule 1.220(b)(2), (b)(3), and (d)(4) of the Florida Rules of Civil Procedure, and seek certification of a Class defined as follows:

> **All individuals residing in the United States whose information was accessed, viewed, copied, and/or acquired during the Cybersecurity Incident reported by Tenet on or about April 26, 2022.**

102. Excluded from the Class 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 and staff members.

103. Plaintiffs hereby reserve the right to amend or modify the class definitions with greater specificity or division after having had an opportunity to conduct discovery.

104. Numerosity, Fla. R. Civ. P. 1.220(a)(1): The Nationwide Class (the "Class") is so numerous that joinder of all members is impracticable. Based upon the "millions" of patient

encounters at Defendant's health system every year and the nature of Defendant's business, it is more likely that there are millions of individuals whose PII and PHI may have been improperly accessed in the Cybersecurity Incident. In any event the exact numbers of members in the Class can be ascertained through Defendant's records.

105. Commonality, Fla. R. Civ. P. 1.220(a)(2) and (b)(3): Questions of law and fact common to the Class exist and predominate over any questions affecting only individual Class Members. These include:

a. Whether Plaintiffs' and Class Members' PII and/or PHI has been compromised;

b. Whether and to what extent Defendant had a duty to protect the PII and PHI of Plaintiffs and Class Members;

c. Whether Defendant had duties not to disclose the PII and PHI of Plaintiffs and Class Members to unauthorized third parties;

d. Whether Defendant had a duty not to use the PII and PHI of Plaintiffs and Class Members for non-authorized purposes;

e. Whether Defendant failed to adequately safeguard the PII and PHI of Plaintiffs and Class Members;

f. Whether and when Defendant actually learned of the Cybersecurity Incident;

g. Whether Defendant adequately, promptly, and accurately informed Plaintiffs and Class Members that their PII and PHI had been compromised;

h. Whether Defendant violated the law by failing to promptly notify

Plaintiffs and Class Members that their PII and PHI had been compromised;

i. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Cybersecurity Incident;

j. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Cybersecurity Incident to occur;

k. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII and PHI of Plaintiffs and Class Members;

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

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

n. Whether Plaintiffs and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Cybersecurity Incident.

106. Typicality, Fla. R. Civ. P. 1.220(a)(3): Plaintiffs' claims are typical of those of other Class Members because all had their PII and PHI potentially compromised as a result of the Cybersecurity Incident, due to Defendant's misfeasance.

107. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect

to the Class as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiffs' challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiffs.

108. Adequacy, Fla. R. Civ. P.1.220(a)(4): Plaintiffs will fairly and adequately represent and protect the interests of the Class Members in that they have no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiffs seek no relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages they have suffered are typical of other Class Members. Plaintiffs have retained counsel experienced in complex class action litigation, and Plaintiffs intend to prosecute this action vigorously.

109. Superiority and Manageability, Fla. R. Civ. P. 1.220(b)(3): Class litigation is an appropriate method for fair and efficient adjudication of the claims involved here. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

110. The nature of this action and the nature of laws available to Plaintiffs and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiffs and Class Members for the wrongs alleged because Defendant would

necessarily gain an unconscionable advantage since it would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiffs was exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the causes of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

111. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

112. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

113. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the PII and PHI of Class Members and Defendant may continue to act unlawfully as set forth in this Complaint.

114. Further, Defendant has acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under Rule 1.220(b)(2) of the Florida Rules of Civil Procedure.

115. Likewise, particular issues under Rule 1.220(d)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues

include, but are not limited to:

a. Whether the PII and PHI of Plaintiffs and Class Members was compromised in the Cybersecurity Incident;

b. Whether Defendant owed a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII and PHI;

c. Whether Defendant breached a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII and PHI;

d. Whether Defendant failed to comply with their own policies and applicable laws, regulations, and industry standards relating to data security;

e. Whether a contract existed between Defendant on the one hand, and Plaintiffs and Class Members on the other, and the terms of that contract;

f. Whether Defendant breached the contract;

g. Whether an implied contract existed between Defendant on the one hand, and Plaintiffs and Class Members on the other, and the terms of that implied contract;

h. Whether Defendant breached the implied contract;

i. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information at issue in the Cybersecurity Incident;

j. Whether Defendant engaged in unfair, unlawful, or deceptive practices

by failing to safeguard the PII and PHI of Plaintiffs and Class Members; and,

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

116. Finally, all members of the proposed Classes are readily ascertainable as they are all individuals who provided their PII and PHI to Tenet or subsidiaries of Tenet. Class Members can be identified, and their contact information ascertained for the purpose of providing notice to the Class based upon private records (including but not limited to Defendant's records) and declarations.

VI. CAUSES OF ACTION

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

117. Plaintiffs repeat, reallege, and incorporate by reference the allegations contained in paragraphs 1 through 116 as if fully set forth herein.

118. Defendant collected, stored, and maintained the PII and PHI of Plaintiffs and Class Members on its internal information systems.

119. Defendant owed Plaintiffs and Class Members a duty of reasonable care to preserve and protect the confidentiality of the personal information that it collected. This duty included, among other obligations, maintaining and testing its security systems and computer networks and the security systems and computer networks of its vendors, using up-to-date and secure versions of software, and taking other reasonable security measures to safeguard and adequately secure the personal information of Plaintiffs and Class Members from unauthorized access and use.

120. Defendant also had a duty to exercise appropriate clearinghouse practices to remove former patient and/or employee PII and PHI it was no longer required to retain pursuant to regulations.

121. Defendant also had a duty to have procedures in place to detect and prevent the improper access and misuse of the PII and PHI of Plaintiffs and Class Members.

122. Defendant's duty to use reasonable security measures arose as a result of the special relationship that existed between Defendant and Plaintiffs and Class Members. That special relationship arose because Plaintiffs and Class Members entrusted Defendant with their confidential PII and PHI, a necessary part of receiving healthcare services from Defendant.

123. Defendant was subject to an "independent duty," untethered to any contract between Defendant and Plaintiffs or Class Members.

124. Defendant breached these duties and Plaintiffs and Class Members were the foreseeable victims of Defendant's inadequate cybersecurity. The natural and probable consequence of Defendant's failing to adequately secure its information networks was the hacking of Plaintiffs' and Class Members' personal information.

125. Defendant knew or should have known that Plaintiffs' and Class Members' personal information was an attractive target for cyber thieves, particularly in light of data breaches that Defendant and other entities experienced and repeated government warnings about the increased threat level. The harm to Plaintiffs and Class Members from exposure of their highly confidential personal facts was reasonably foreseeable to Defendant.

126. Defendant's own conduct created a foreseeable risk of harm to Plaintiffs and the Class Members. Defendant's misconduct included, but was not limited to, its failure to take the steps and opportunities to prevent the Cybersecurity Incident as set forth herein. Defendant's

misconduct also included its decisions not to comply with industry standards for the safekeeping of the PII and PHI of Plaintiffs and the Class Members. Defendant knew or should have known that data breaches such as the Cybersecurity Incident result in exposure of sensitive information in an overwhelming percentage of instances.

127. Plaintiffs and Class Members had no ability to protect their PII and PHI that was in, and remains in, Defendant's possession.

128. Defendant had the ability to sufficiently guard against data breaches by implementing adequate measures to protect its systems.

129. Defendant breached its duty to exercise reasonable care in protecting Plaintiffs' and Class Members' confidential personal information by failing to implement and maintain adequate security measures to safeguard the information, failing to monitor its systems and files to identify suspicious activity, and allowing unauthorized access to the information.

130. There is a close connection between Defendant's failure to employ reasonable security protections for its patients' personal information and the injuries suffered by Plaintiffs and Class Members. When individuals' sensitive personal information is stolen, they face a heightened risk of identity theft and need to: (1) purchase identity protection, monitoring, and recovery services; (2) flag asset, credit, and tax accounts for fraud, including by reporting the theft of their Social Security numbers to financial institutions, credit agencies, and the IRS; (3) purchase or otherwise obtain credit reports; (4) monitor credit, financial, utility, explanation of benefits, and other account statements on a monthly basis for unrecognized credit inquiries and charges; (5) place and renew credit fraud alerts on a quarterly basis; (6) contest fraudulent charges and other forms of identity theft; (7) repair damage to credit and financial accounts; and (8) take other steps to protect themselves and attempt to avoid or recover from identity theft and fraud.

131. Defendant's failure to comply with industry standards and state regulations further evidences Defendant's negligence in failing to exercise reasonable care in safeguarding and protecting the PII and PHI of Plaintiffs and Class Members.

132. Defendant, through its actions and/or omissions, unlawfully breached its duty to adequately and timely disclose to Plaintiffs and Class Members the existence and scope of the Cybersecurity Incident.

133. But for Defendant's wrongful and negligent breach of duties owed to Plaintiffs and Class Members, the PII and PHI of Plaintiffs and Class Members would not have been compromised.

134. The policy of preventing future harm necessitates the finding that Defendant had an independent duty in tort to protect this data and thereby avoid reasonably foreseeable harm to Plaintiffs and the Class Members, particularly given the extremely sensitive data entrusted to Defendant.

135. As a direct and proximate result of Defendant's negligence, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their PII and PHI is used; (iii) the compromise, publication, and/or theft of their PII and PHI; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII and PHI; (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 Cybersecurity 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 and PHI, 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 PII and PHI of Plaintiffs and Class Members; 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 and PHI compromised as a result of the Cybersecurity Incident for the remainder of the lives of Plaintiffs and Class Members.

136. As a direct and proximate result of Defendant's negligence, Plaintiffs and Class Members 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.

137. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiffs and Class Members have suffered and will suffer the continued risks of exposure of their PII and PHI, 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 PII and PHI in its continued possession.

138. As a direct and proximate result of Defendant's negligence, Plaintiffs and Class Members are entitled to and demand actual, consequential, and nominal damages.

COUNT II
Breach of Express Contract
(On Behalf of Plaintiffs and the Nationwide Class)

139. Plaintiffs repeat, reallege, and incorporate by reference the allegations contained in paragraphs 1 through 116 as if fully set forth herein.

140. Defendant entered into contracts with Plaintiffs and Class Members for healthcare services, among other things. As a condition of that relationship, Plaintiffs and Class Members entrusted personal and sensitive information to Defendant, which gave rise to a duty to safeguard

that information.

141. These contracts included, in part, promises regarding Defendant's commitment to the security of patient privacy. Defendant's Notice of Privacy Practices acknowledges that individuals who provide sensitive information to Defendant, including patients and employees, have a right to privacy and confidentiality in the PII and PHI Tenet collects.[58] Further, it lists limited circumstances wherein the PII and PHI of its patients may be shared without prior consent, none of which are applicable here. Thus, in contracting for healthcare services and/or employment, Defendant promised to safeguard the PII and PHI of Plaintiffs and Class Members.

142. Defendant's contracts with its patients and/or employees, among other things, expressly promised to take reasonable measures to safeguard and protect such information for the benefit of Plaintiffs and Class Members.

143. Plaintiffs and Class Members would not have entrusted such sensitive personal and medical information to Defendant in the absence of Defendant's promise to adequately safeguard the data.

144. Defendant breached the contracts it entered into by failing to provide reasonable data security measures.

145. As a direct and proximate result of Defendant's above-described breach of contract with its patients, Plaintiffs and Class Members have suffered (and will continue to suffer) 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 illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and

[58] Ex. 2.

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.

146. As a direct and proximate result of Defendant's above-described breach of contract, Plaintiffs and Class Members are entitled to recover actual, consequential, and nominal damages.

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

147. Plaintiffs repeat, reallege, and incorporate by reference the allegations contained in paragraphs 1 through 116 as if fully set forth herein.

148. As a condition of obtaining healthcare services and/or employment from Defendant, Plaintiffs and Class Members were obligated to provide their PII and PHI to Defendant.

149. In so doing, Plaintiffs and Class Members 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 Plaintiffs and Class Members if their data had been breached and compromised or stolen.

150. Plaintiffs and Class Members fully performed their obligations under the contracts with Defendant.

151. Plaintiffs and Class Members entered into the contracts with the reasonable expectation that Defendant's data and cyber security practices and policies were reasonable and consistent with industry standards. Plaintiffs and Class Members believed that Defendant would use part of the monies paid to Defendant to fund adequate and reasonable data and cyber security practices, as Defendant represented it would in its Notice of Privacy Practices.

152. Plaintiffs and Class Members would not have provided and entrusted their sensitive

and confidential information to Defendant in the absence of the contract or implied terms between them and Defendant. The safeguarding of the PII and PHI of Plaintiffs and Class Members was critical to realize the intent of the parties.

153. Defendant breached the implied contracts it made with Plaintiffs and Class Members by failing to safeguard and protect their personal information, resulting in the unauthorized access, acquisition, and/or disclosure of Plaintiffs and Class Members' PII and PHI during the Cybersecurity Incident.

154. As a direct and proximate result of Defendant's above-described breach of contract, Plaintiffs and Class Members have suffered (and will continue to suffer) 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 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.

155. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiffs and Class Members are entitled to recover actual, consequential, and nominal damages

VII. REQUEST FOR RELIEF

156. As a result of the foregoing, Plaintiffs, individually and on behalf of all other ClassMembers proposed in this Complaint, respectfully request that the Court enter judgment in their favor and against Defendants as follows:

a. For an order certifying the Class and appointing Plaintiffs as representatives of the Class and appointing the undersigned as Class Counsel;

b. For all recoverable compensatory, statutory, nominal, and other damages sustained by Plaintiffs and the Class, including disgorgement, unjust enrichment and all other relief under applicable laws;

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

d. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and the Class, 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

state or local laws;

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

iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII and PHI of Plaintiffs and the Class;

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 Plaintiffs and the Class;

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 members of the Class 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;

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

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

g. For prejudgment interest on all amounts awarded; and

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

JURY DEMAND

Plaintiffs hereby demand a jury trial on all issues so triable.

Dated: June 10, 2022 Respectfully submitted,

/s/ Patrick A. Barthle
Patrick A. Barthle II
Fla. Bar. No. 99286
MORGAN & MORGAN COMPLEX LITIGATION GROUP
201 N. Franklin St.,
7th Floor Tampa, FL 33602
PBarthle@ForThePeople.com
P: (813) 229-4023
F: (813) 222-4708

Attorney for Plaintiffs and the Proposed Class

Exhibit 1

Tenet Reports Cybersecurity Incident

April 26, 2022

DALLAS--(BUSINESS WIRE)-- Tenet Healthcare Corporation (NYSE: THC) experienced a cybersecurity incident last week. The Company immediately suspended user access to impacted information technology applications, executed extensive cybersecurity protection protocols, and quickly took steps to restrict further unauthorized activity.

Efforts to restore impacted information technology operations continue to make important progress. While there was temporary disruption to a subset of acute care operations, the Company's hospitals remained operational and continued to deliver patient care safely and effectively, utilizing well-established back-up processes. At this time, critical applications have largely been restored and the subset of impacted facilities has begun to resume normal operations.

In parallel, the Company immediately launched an investigation of the incident, which is currently ongoing. The Company is taking additional measures to protect patient, employee and other data, as appropriate, in response to this incident.

Tenet is grateful to its physicians, nurses and staff for their dedication to safely care for patients as the Company works to resolve this matter.

Forward-Looking Statements

This communication includes forward-looking statements within the meaning of the Private Securities Litigation Reform Act of 1995. All statements other than statements of historical fact are forward-looking statements. These forward-looking statements are generally identified by the words "anticipate," "believe," "estimate," "expect," "intend," "may," "could" or similar expressions. Forward-looking statements are based on current expectations and assumptions, which are subject to risks and uncertainties that may cause actual results to differ materially from the forward-looking statements. These risks and uncertainties include those

mediarelations@tenethealth.com

Source: Tenet Healthcare Corporation

VIEW ALL PRESS RELEASES

Email Alerts

Your email address

Sign Up

☐ Press Releases ☐ Events ☐ Presentations ☐ SEC Filings

Exhibit 2

NOTICE OF PRIVACY PRACTICES

THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.

Who Presents this Notice

The references to "Facility" and "Health Professionals" in this notice refer to the members of the Tenet Healthcare Affiliated Covered Entity. An Affiliated Covered Entity (ACE) is a group of organizations under common ownership or control who designate themselves as a single Affiliated Covered Entity for purposes of compliance with the Health Insurance Portability and Accountability Act ("HIPAA"). The Facility, its employees, workforce members and members of the ACE who are involved in providing and coordinating health care are all bound to follow the terms of this Notice of Privacy Practices ("Notice"). The members of the ACE will share PHI with each other for the treatment, payment and health care operations of the ACE and as permitted by HIPAA and this Notice. For a complete list of the members of the ACE, please contact the Privacy & Security Compliance Office.

Privacy Obligations

Each Facility is required by law to maintain the privacy of your health information ("Protected Health Information" or "PHI") and to provide you with this Notice of legal duties and privacy practices with respect to your Protected Health Information. The Facility uses computerized systems that may subject your Protected Health Information to electronic disclosure for purposes of treatment, payment and/or health care operations as described below. When the Facility uses or discloses your Protected Health Information, we are required to abide by the terms of this Notice (or other notice in effect at the time of the use or disclosure).

Notifications

The Facility is required by law to protect the privacy of your medical information, distribute this Notice of Privacy Practices to you, and follow the terms of this Notice. The Facility is also required to notify you if there is a breach or impermissible access, use or disclosure of your medical information.

Permissible Uses and Disclosures Without Your Written Authorization

In certain situations your written authorization must be obtained in order to use and/or disclose your PHI. However, the Facility and Health Professionals do not need any type of authorization from you for the following uses and disclosures:

Uses and Disclosures for Treatment, Payment and Health Care Operations. Your PHI may be used and disclosed to treat you, obtain payment for services provided to you and conduct "health care operations" as detailed below:

Treatment. Your PHI may be used and disclosed to provide treatment and other services to you--for example, to diagnose and treat your injury or illness. In addition, you may be contacted to provide you appointment reminders or information about treatment alternatives or other health-related benefits and services that may be of interest to you. Your PHI may also be disclosed to other providers involved in your treatment. For example, a doctor treating you for a broken leg may need to know if you have diabetes because if you do, this may impact your recovery.

Payment. Your PHI may be used and disclosed to obtain payment for services provided to you--for example, disclosures to claim and obtain payment from your health insurer, HMO, or other company that arranges or pays the cost of some or all of your health care ("Your Payor") to verify that Your Payor will pay for health care. The physician who reads your x-ray may need to bill you or your Payor for reading of your x-ray therefore your billing information may be shared with the physician who read your x-ray.

Health Care Operations. Your PHI may be used and disclosed for health care operations, which include internal administration and planning and various activities that improve the quality and cost effectiveness of the care delivered to you. For example, PHI may be used to evaluate the quality and competence of physicians, nurses and other health care workers. PHI may be disclosed to the Privacy & Security Compliance Office in order to resolve any complaints you may have and ensure that you have a comfortable visit. Your PHI may be provided to various governmental or accreditation entities such as the Joint Commission on Accreditation of Healthcare Organizations to maintain our license and accreditation. In addition, PHI may be shared with business associates who perform treatment, payment and health care operations services on behalf of the Facility and Health Professionals.

Additionally, your PHI may be used or disclosed for the purpose of allowing students, residents, nurses, physicians and others who are interested in healthcare, pursuing careers in the medical field or desire an opportunity for an educational experience to tour, shadow employees and/or physician faculty members or engage in a clinical Practicum.

Health Information Organizations. Your PHI may be used and disclosed with other health care providers or other health care entities for treatment, payment and health care operations purposes, as permitted by law, through a Health Information Organization. A list of Health Information Organizations in which this facility participates may be obtained upon request or found on our website at www.tenethealth.com. For example, information about your past medical care and current medical conditions and medications can be available to other primary care physicians if they participate in the Health Information Organization. Exchange of health information can provide faster access, better coordination of care and assist providers and public health officials in making more informed treatment decisions. You may opt out of the Health Information Organization and prevent providers from being able to search for your information through the exchange. You may opt out and prevent your medical information from being searched through the Health Information Organization by completing and submitting an Opt-Out Form to registration.

Use or Disclosure for Directory of Individuals in the Facility. Facility may include your name, location in the Facility, general health condition and religious affiliation in a patient directory without obtaining your authorization *unless* you object to inclusion in the directory. Information in the directory may be disclosed to anyone who asks for you by name. Your religious affiliation may be given to a member of the clergy, such as a priest or minister, even if they do not ask for you by name. If you do

not wish to be included in the facility directory, you will be given an opportunity to object at the time of admission.

Disclosure to Relatives, Close Friends and Other Caregivers. Your PHI may be disclosed to a family member, other relative, a close personal friend or any other person identified by you who is involved in your health care or helps pay for your care. If you are not present, or the opportunity to agree or object to a use or disclosure cannot practicably be provided because of your incapacity or an emergency circumstance, the Facility and/or Health Professionals may exercise professional judgment to determine whether a disclosure is in your best interests. If information is disclosed to a family member, other relative or a close personal friend, the Facility and/or Health Professionals would disclose only information believed to be directly relevant to the person's involvement with your health care or payment related to your health care. Your PHI also may be disclosed in order to notify (or assist in notifying) such persons of your location or general condition.

Public Health Activities. Your PHI may be disclosed for the following public health activities: (1) to report health information to public health authorities for the purpose of preventing or controlling disease, injury or disability; (2) to report child abuse and neglect to public health authorities or other government authorities authorized by law to receive such reports; (3) to report information about products and services under the jurisdiction of the U.S. Food and Drug Administration; (4) to alert a person who may have been exposed to a communicable disease or may otherwise be at risk of contracting or spreading a disease or condition; and (5) to report information to your employer as required under laws addressing work-related illnesses and injuries or workplace medical surveillance.

Victims of Abuse, Neglect or Domestic Violence. Your PHI may be disclosed to a governmental authority, including a social service or protective services agency, authorized by law to receive reports of such abuse, neglect, or domestic violence if there is a reasonable belief that you are a victim of abuse, neglect or domestic violence.

Health Oversight Activities. Your PHI may be disclosed to a health oversight agency that oversees the health care system and is charged with responsibility for ensuring compliance with the rules of government health programs such as Medicare or Medicaid.

Judicial and Administrative Proceedings. Your PHI may be disclosed in the course of a judicial or administrative proceeding in response to a legal order or other lawful process.

Law Enforcement Officials. Your PHI may be disclosed to the police or other law enforcement officials as required or permitted by law or in compliance with a court order or a grand jury or administrative subpoena. For example, your PHI may be disclosed to identify or locate a suspect, fugitive, material witness, or missing person or to report a crime or criminal conduct at the facility.

Correctional Institution. You PHI may be disclosed to a correctional institution if you are an inmate in a correctional institution and if the correctional institution or law enforcement authority makes certain requests to us.

Organ and Tissue Procurement. Your PHI may be disclosed to organizations that facilitate organ, eye or tissue procurement, banking or transplantation.

Research. Your PHI may be used or disclosed without your consent or authorization if an Institutional Review Board approves a waiver of authorization for disclosure.

Health or Safety. Your PHI may be used or disclosed to prevent or lessen a serious and imminent threat to a person's or the public's health or safety.

U.S. Military. Your PHI may be use or disclosed to U. S. Military Commanders for assuring proper execution of the military mission. Military command authorities receiving protected health information are not covered entities subject to the HIPAA Privacy Rule, but they are subject to the Privacy Act of 1974 and DoD 5400.11-R , "DoD Privacy Program," May 14, 2007.

Other Specialized Government Functions. Your PHI may be disclosed to units of the government with special functions, such as the U.S. Department of State under certain circumstances for example the Secret Service or NSA to protect the country or the President.

Workers' Compensation. Your PHI may be disclosed as authorized by and to the extent necessary to comply with state law relating to workers' compensation or other similar programs.

As Required by Law. Your PHI may be used and disclosed when required to do so by any other law not already referred to in the preceding categories; such as required by the FDA, to monitor the safety of a medical device.

Appointment Reminders. Your PHI may be used to tell or remind you about appointments.

Fundraising. Your PHI may be used to contact you as a part of fundraising efforts, unless you elect not to receive this type of information.

USES AND DISCLOSURES REQUIRING YOUR WRITTEN AUTHORIZATION

Use or Disclosure with Your Authorization. For any purpose other than the ones described above, your PHI may be used or disclosed only when you provide your written authorization on an authorization form ("Your Authorization"). For instance, you will need to execute an authorization form before your PHI can be sent to your life insurance company or to the attorney representing the other party in litigation in which you are involved.

Marketing. Your written authorization ("Your Marketing Authorization") also must be obtained prior to using your PHI to send you any marketing materials. (However, marketing materials can be provided to you in a face-to-face encounter without obtaining Your Marketing Authorization. The Facility and/or Health Professionals are also permitted to give you a promotional gift of nominal value, if they so choose, without obtaining Your Marketing Authorization). The Facility and/or Health Professionals may communicate with you in a face-to-face encounter about products or services relating to your treatment, case management or care coordination, or alternative treatments, therapies, providers or care settings without Your Marketing Authorization.

In addition, the Facility and/or Health Professionals may send you treatment communications, unless you elect not to receive this type of communication, for which the Facility and/or Health Professionals may receive financial remuneration.

Sale of PHI. The Facility and Health Professionals will not disclose your PHI without your authorization in exchange for direct or indirect payment except in limited circumstances permitted by law. These circumstances include public health activities; research; treatment of the individual; sale, transfer, merger or consolidation of the Facility; services provided by a business associate, pursuant to a business associate agreement; providing an individual with a copy of their PHI; and other purposes deemed necessary and appropriate by the U.S. Department of Health and Human Services (HHS).

Uses and Disclosures of Your Highly Confidential Information. In addition, federal and state law require special privacy protections for certain highly confidential information about you ("Highly Confidential Information"), including the subset of your PHI that: (1) is maintained in psychotherapy notes; (2) is about mental illness, mental retardation and developmental disabilities; (3) is about alcohol or drug abuse or addiction; (4) is about HIV/AIDS testing, diagnosis or treatment; (5) is about communicable disease(s), including venereal disease(s); (6) is about genetic testing; (7) is about child abuse and neglect; (8) is about domestic abuse of an adult; or (9) is about sexual assault. In order for your Highly Confidential Information to be disclosed for a purpose other than those permitted by law, your written authorization is required.

YOUR RIGHTS REGARDING YOUR PROTECTED HEALTH INFORMATION

Right to Request Additional Restrictions. You may request restrictions on the use and disclosure of your PHI (1) for treatment, payment and health care operations, (2) to individuals (such as a family member, other relative, close personal friend or any other person identified by you) involved with your care or with payment related to your care, or (3) to notify or assist in the notification of such individuals regarding your location and general condition. While all requests for additional restrictions will be carefully considered, the Facility and Health Professionals are not required to agree to these requested restrictions.

You may also request to restrict disclosures of your PHI to your health plan for payment and healthcare operations purposes (and not for treatment) if the disclosure pertains to a healthcare item or service for which you paid out-of-pocket in full. The Facility and Health Professionals must agree to abide by the restriction to your health plan EXCEPT when the disclosure is required by law.

If you wish to request additional restrictions, please obtain a request form from the Health Information Management Office and submit the completed form to the Health Information Management Office. A written response will be sent to you.

Right to Receive Confidential Communications. You may request, and the Facility and Health Professionals will accommodate, any reasonable written request for you to receive your PHI by alternative means of communication or at alternative locations.

Right to Revoke Your Authorization. You may revoke Your Authorization, Your Marketing Authorization or any written authorization obtained in connection with your PHI, except to the extent that the Facility and/or Health Professionals have taken action in reliance upon it, by delivering a written revocation statement to the Facility Health Information Management Office identified below.

Right to Inspect and Copy Your Health Information. You may request access to your medical record file and billing records maintained by the Facility and Health Professionals in order to inspect and

request copies of the records. Under limited circumstances, you may be denied access to a portion of your records. If you desire access to your records, please obtain a record request form from the Facility Health Information Management Office and submit the completed form to the Facility Health Information Management Office. If you request copies of paper records, you will be charged in accordance with federal and state law. To the extent the request for records includes portions of records which are not in paper form (e.g., x-ray films), you will be charge the reasonable cost of the copies. You also will be charged for the postage costs, if you request that the copies be mailed to you. However, you will not be charged for copies that are requested in order to make or complete an application for a federal or state disability benefits program.

Right to Amend Your Records. You have the right to request that PHI maintained in your medical record file or billing records be amended. If you desire to amend your records, please obtain an amendment request form from the Facility Health Information Management Office and submit the completed form to the Facility Health Information Management Office. Your request will be accommodated unless the Facility and/or Health Professionals believe that the information that would be amended is accurate and complete or other special circumstances apply.

Right to Receive an Accounting of Disclosures. Upon request, you may obtain an accounting of certain disclosures of your PHI made during any period of time prior to the date of your request provided such period does not exceed six years and does not apply to disclosures that occurred prior to April 14, 2003. If you request an accounting more than once during a twelve (12) month period, you will be charged for the accounting statement.

Right to Receive Paper Copy of this Notice. Upon request, you may obtain a paper copy of this Notice, even if you have agreed to receive such notice electronically.

For Further Information or Complaints. If you desire further information about your privacy rights, are concerned that your privacy rights have been violated or disagree with a decision made about access to your PHI, you may contact the Privacy & Security Compliance Office. You may also file written complaints with the Director, Office for Civil Rights of the U.S. Department of Health and Human Services. Upon request, the Privacy & Security Compliance Office will provide you with the correct address for the Director. The Facility and Health Professionals will not retaliate against you if you file a complaint with the Privacy & Security Compliance Office or the Director.

Effective Date and Duration of This Notice

Effective Date. This Notice is effective on March 1, 2021.

Right to Change Terms of this Notice. The terms of this Notice may be changed at any time. If this Notice is changed, the new notice terms may be made effective for all PHI that the Facility and Health Professionals maintain, including any information created or received prior to issuing the new notice. If this Notice is changed, the new notice will be posted in waiting areas around the Facility and on our Internet site at *www.tenethealth.com*. You also may obtain any new notice by contacting the Privacy & Security Compliance Office.

FACILITY CONTACTS:

Privacy & Security Compliance Office

14201 Dallas Parkway

Dallas, Texas 75254

E-mail: PrivacySecurityOffice@tenethealth.com

Ethics Action Line (EAL): 1-800-8-ETHICS

EXHIBIT B

Rob Brewster, et al Plaintiff vs. Tenet Healthcare Corporation Defendant

Broward County Case Number: CACE22008510
State Reporting Number: 062022CA008510AXXXCE
Court Type: Civil
Case Type: Contract and Indebtedness
Incident Date: N/A
Filing Date: 06/10/2022
Court Location: Central Courthouse
Case Status: Pending
Magistrate Id / Name: N/A
Judge ID / Name: 03 McCarthy, Barbara

Party(ies)

Total: 3

Party Type	Party Name	Address	Attorneys / Address ★ Denotes Lead Attorney
Plaintiff	**Brewster, Rob**		★ Barthle, Patrick A, II Retained Bar ID: 99286 Greenberg Traurig PA 625 E Twiggs Street Ste 100 Tampa, FL 33602 **Status: Active**
Plaintiff	**Goffman, Anita**		★ Barthle, Patrick A, II Retained Bar ID: 99286 Greenberg Traurig PA 625 E Twiggs Street Ste 100 Tampa, FL 33602 **Status: Active**
Defendant	**Tenet Healthcare Corporation**		

Disposition(s)

Total: 0

Date	Statistical Closure(s)

Date	Disposition(s)	View	Page(s)

Event(s) & Document(s)

Total: 7

Date	Description	Additional Text	View	Pages
06/22/2022	**Summons Returned Served**	15th day of June, 2022 Party: *Defendant* Tenet Healthcare Corporation		1
06/13/2022	**Clerk's Certificate of Compliance W-2020-73CIV/2020-74-UFC**	none		1
06/10/2022	**Per AOSC20-23 Amd12, Case is determined General**			
06/10/2022	**Civil Cover Sheet**	Amount: $100,001.00		3
06/10/2022	**Civil Cover Sheet**	Amount: $100,001.00		3
06/10/2022	**Complaint (eFiled)**			55
06/10/2022	**eSummons Issuance**			2

Hearing(s)

Total: 0

There is no Disposition information available for this case.

Related Case(s)

Total: 0

There is no related case information available for this case.

EXHIBIT C

FORM 1.997. CIVIL COVER SHEET

The civil cover sheet and the information contained in it neither replace nor supplement the filing and service of pleadings or other documents as required by law. This form must be filed by the plaintiff or petitioner with the Clerk of Court for the purpose of reporting uniform data pursuant to section 25.075, Florida Statutes. (See instructions for completion.)

IN THE CIRCUIT COURT OF THE SEVENTEENTH JUDICIAL CIRCUIT,
IN AND FOR BROWARD COUNTY, FLORIDA

Plaintiff ROB BREWSTER and ANITA GOFFMAN

Case # _____
Judge _____

vs.

Defendant TENET HEALTHCARE CORPORATION, d/b/a TENET

I. AMOUNT OF CLAIM

Please indicate the estimated amount of the claim, rounded to the nearest dollar. The estimated amount of the claim is requested for data collection and clerical processing purposes only. The amount of the claim shall not be used for any other purpose.

- ☐ $8,000 or less
- ☐ $ 8,001 - $30,000
- ☐ $30,001 - $50,000
- ☐ $50,001 - $75,000
- ☐ $75,001 - $100,000
- ☑ over $100,000

II. TYPE OF CASE (If the case fits more than one type of case, select the most definitive category.) If the most descriptive label is a subcategory (is indented under a broader category), place an x on both the main category and subcategory lines.

CIRCUIT CIVIL

- ☐ Condominium
- ☑ Contracts and indebtedness
- ☐ Eminent domain
- ☐ Auto negligence
- ☐ Negligence—other
  - ☐ Business governance
  - ☐ Business torts

- ☐ Environmental/Toxic tort
- ☐ Third party indemnification
- ☐ Construction defect
- ☐ Mass tort
- ☐ Negligent security
- ☐ Nursing home negligence
- ☐ Premises liability—commercial
- ☐ Premises liability—residential

☐ Products liability

☐ Real property/Mortgage foreclosure

- ☐ Commercial foreclosure
- ☐ Homestead residential foreclosure
- ☐ Non-homestead residential foreclosure
- ☐ Other real property actions

☐ Professional malpractice

- ☐ Malpractice—business
- ☐ Malpractice—medical
- ☐ Malpractice—other professional

☐ Other

- ☐ Antitrust/Trade regulation
- ☐ Business transactions
- ☐ Constitutional challenge—statute or ordinance
- ☐ Constitutional challenge—proposed amendment
- ☐ Corporate trusts
- ☐ Discrimination—employment or other
- ☐ Insurance claims
- ☐ Intellectual property
- ☐ Libel/Slander
- ☐ Shareholder derivative action
- ☐ Securities litigation
- ☐ Trade secrets
- ☐ Trust litigation

COUNTY CIVIL

☑ Civil

☐ Real Property/Mortgage foreclosure

☐ Evictions

- ☐ Residential Evictions
- ☐ Non-residential Evictions

☐ Other civil (non-monetary)

III. REMEDIES SOUGHT (check all that apply):

☑ Monetary;
☑ Nonmonetary declaratory or injunctive relief;
☐ Punitive

IV. NUMBER OF CAUSES OF ACTION: [3]

(Specify) Negligence, Breach of Express Contract, Breach of Implied Contract,

V. IS THIS CASE A CLASS ACTION LAWSUIT?

◉ yes
○ no

VI. HAS NOTICE OF ANY KNOWN RELATED CASE BEEN FILED?

◉ no
○ yes If "yes," list all related cases by name, case number, and court.

VII. IS JURY TRIAL DEMANDED IN COMPLAINT?

◉ yes
○ no

I CERTIFY that the information I have provided in this cover sheet is accurate to the best of my knowledge and belief, and that I have read and will comply with the requirements of Florida Rule of Judicial Administration 2.425.

Signature _____ Fla. Bar # 99286
Attorney or party (Bar # if attorney)

Patrick A. Barthle 06/10/22
(type or print name) Date

FORM 1.997. CIVIL COVER SHEET

The civil cover sheet and the information contained in it neither replace nor supplement the filing and service of pleadings or other documents as required by law. This form must be filed by the plaintiff or petitioner with the Clerk of Court for the purpose of reporting uniform data pursuant to section 25.075, Florida Statutes. (See instructions for completion.)

I. CASE STYLE

IN THE CIRCUIT/COUNTY COURT OF THE SEVENTEENTH JUDICIAL CIRCUIT,
IN AND FOR BROWARD COUNTY, FLORIDA

Rob Brewster, Anita Goffman
Plaintiff

Case # _____
Judge _____

vs.
Tenet Healthcare Corporation d/b/a Tenet
Defendant

II. AMOUNT OF CLAIM

Please indicate the estimated amount of the claim, rounded to the nearest dollar. The estimated amount of the claim is requested for data collection and clerical processing purposes only. The amount of the claim shall not be used for any other purpose.

☐ $8,000 or less
☐ $8,001 - $30,000
☐ $30,001- $50,000
☐ $50,001- $75,000
☐ $75,001 - $100,000
☒ over $100,000.00

III. TYPE OF CASE (If the case fits more than one type of case, select the most definitive category.) If the most descriptive label is a subcategory (is indented under a broader category), place an x on both the main category and subcategory lines.

CIRCUIT CIVIL

☐ Condominium
☒ Contracts and indebtedness
☐ Eminent domain
☐ Auto negligence
☐ Negligence—other
- ☐ Business governance
- ☐ Business torts
- ☐ Environmental/Toxic tort
- ☐ Third party indemnification
- ☐ Construction defect
- ☐ Mass tort
- ☐ Negligent security
- ☐ Nursing home negligence
- ☐ Premises liability—commercial
- ☐ Premises liability—residential

☐ Products liability
☐ Real Property/Mortgage foreclosure
- ☐ Commercial foreclosure
- ☐ Homestead residential foreclosure
- ☐ Non-homestead residential foreclosure
- ☐ Other real property actions

☐Professional malpractice
- ☐ Malpractice—business
- ☐ Malpractice—medical
- ☐ Malpractice—other professional

☐ Other
- ☐ Antitrust/Trade regulation
- ☐ Business transactions
- ☐ Constitutional challenge—statute or ordinance
- ☐ Constitutional challenge—proposed amendment
- ☐ Corporate trusts
- ☐ Discrimination—employment or other
- ☐ Insurance claims
- ☐ Intellectual property
- ☐ Libel/Slander
- ☐ Shareholder derivative action
- ☐ Securities litigation
- ☐ Trade secrets
- ☐ Trust litigation

COUNTY CIVIL

☐ Small Claims up to $8,000
☐ Civil
☐ Real property/Mortgage foreclosure

☐ Replevins
☐ Evictions
  ☐ Residential Evictions
  ☐ Non-residential Evictions
☐ Other civil (non-monetary)

COMPLEX BUSINESS COURT

This action is appropriate for assignment to Complex Business Court as delineated and mandated by the Administrative Order. Yes ☒ No ☐

IV. REMEDIES SOUGHT (check all that apply):
☒ Monetary;
☒ Nonmonetary declaratory or injunctive relief;
☐ Punitive

V. NUMBER OF CAUSES OF ACTION: [ ]
(Specify)

3

VI. IS THIS CASE A CLASS ACTION LAWSUIT?
☒ yes
☐ no

VII. HAS NOTICE OF ANY KNOWN RELATED CASE BEEN FILED?
☒ no
☐ yes If "yes," list all related cases by name, case number, and court.

VIII. IS JURY TRIAL DEMANDED IN COMPLAINT?
☒ yes
☐ no

IX. DOES THIS CASE INVOLVE ALLEGATIONS OF SEXUAL ABUSE?
☐ yes
☒ no

I CERTIFY that the information I have provided in this cover sheet is accurate to the best of my knowledge and belief, and that I have read and will comply with the requirements of Florida Rule of Judicial Administration 2.425.

Signature: s/ Patrick A. Barthle II — Fla. Bar # 99286
Attorney or party — (Bar # if attorney)

Patrick A. Barthle II — 06/10/2022
(type or print name) — Date

AP

IN THE CIRCUIT COURT OF THE 17TH JUDICIAL CIRCUIT IN AND FOR BROWARD COUNTY, FLORIDA

Case No: 22-8510

Rob Brewster et al
Plaintiff

Judge Division: 03

VS

Tenet Healthcare corp DBA Tenet
Defendant

FILED
JUN 13 2022
By

CLERK'S CERTIFICATE OF COMPLIANCE

I hereby certify that pursuant to Administrative Order, No. 2020-73Civ/2020-74-UFC: "ADMINISTRATIVE ORDER DIRECTING CLERK OF COURTS WITH REGARD TO DISMISSED CIVIL OR FAMILY CASES",

The Clerk has conducted a search for all previous existing civil cases related to these two parties.

Listed below are all the aforementioned related cases: NOT

Brenda D. Forman
Circuit and County Courts

By: _____
Deputy Clerk

RETURN OF SERVICE

State of Florida **County of Broward** **Circuit Court**

Case Number: CACE-22-8510

Plaintiff:
ROB BREWSTER and ANITA GOFFMAN, ON BEHALF OF THEMSELVES AND ALL OTHERS SIMILARLY SITUATED

IST2022002318

vs.

Defendant:
TENET HEALTHCARE CORPORATION D/B/A TENET

For:
Patrick Barthle, II
Morgan & Morgan, P.A.
201 North Franklin Street
7th Floor
Tampa, FL 33602

Received by Tampa Process, LLC on the 15th day of June, 2022 at 8:30 am to be served on **TENET HEALTHCARE CORPORATION C/O R/A CT CORPORATION SYSTEM, 1200 SOUTH PINE ISLAND ROAD, PLANTATION, FL 33324**.

I, Eric Deal, do hereby affirm that on the **15th day of June, 2022** at **1:00 pm, I:**

CORPORATE: Served the within named corporation/entity TENET HEALTHCARE CORPORATION C/O R/A CT CORPORATION SYSTEM by delivering a true copy of the Summons and Complaint with Exhibit(s) with the date and hour of service endorsed thereon by me to: Monicka Creary as employee of the Registered Agent (Company) for TENET HEALTHCARE CORPORATION at 1200 South Pine Island Road, c/o CT Corporation System, R/A, Plantation, FL 33324 and informed said person of the contents therein, in compliance with state statutes.

Under penalty of perjury, I declare that I have read the foregoing and that the facts stated in it are true and correct, that I am a Sheriff's Appointed process server in the county in which service was effected in accordance with Florida Statutes and I have no interest in the above action.

Eric Deal
SPS 336

Tampa Process, LLC
P.O. Box 271986
Tampa, FL 33688
(813) 964-9159

Our Job Serial Number: IST-2022002318
Ref: 12780481

JS 44 (Rev. 10/20) FLSD Revised 02/12/2021

CIVIL COVER SHEET

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. *(SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)* **NOTICE: Attorneys MUST Indicate All Re-filed Cases Below.**

I. (a) PLAINTIFFS

Rob Brewster and Anita Goffman

(b) County of Residence of First Listed Plaintiff Palm Beach County, FL
(EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys *(Firm Name, Address, and Telephone Number)*

Morgan & Morgan, 201 N. Franklin St., Tampa, FL, 813-229-4023

DEFENDANTS

Tenet Healthcare Corporation, d/b/a Tenet

County of Residence of First Listed Defendant Dallas County, TX
(IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

Attorneys *(If Known)*

Alston & Bird, 1201 W. Peachtree St., Atlanta, GA, 404-881-7000

(d) Check County Where Action Arose: ☐ MIAMI- DADE ☐ MONROE ■ BROWARD ☐ PALM BEACH ☐ MARTIN ☐ ST. LUCIE ☐ INDIAN RIVER ☐ OKEECHOBEE ☐ HIGHLANDS

II. BASIS OF JURISDICTION *(Place an "X" in One Box Only)*

- ☐ 1 U.S. Government Plaintiff
- ☐ 3 Federal Question *(U.S. Government Not a Party)*
- ☐ 2 U.S. Government Defendant
- ☒ 4 Diversity *(Indicate Citizenship of Parties in Item III)*

III. CITIZENSHIP OF PRINCIPAL PARTIES *(Place an "X" in One Box for Plaintiff) and One Box for Defendant)*
(For Diversity Cases Only)

	PTF	DEF		PTF	DEF
Citizen of This State	■ 1	☐ 1	Incorporated *or* Principal Place of Business In This State	☐ 4	☐ 4
Citizen of Another State	☐ 2	☐ 2	Incorporated *and* Principal Place of Business In Another State	☐ 5	■ 5
Citizen or Subject of a Foreign Country	☐ 3	☐ 3	Foreign Nation	☐ 6	☐ 6

IV. NATURE OF SUIT *(Place an "X" in One Box Only)*

Click here for: Nature of Suit Code Descriptions

CONTRACT
- ☐ 110 Insurance
- ☐ 120 Marine
- ☐ 130 Miller Act
- ☐ 140 Negotiable Instrument
- ☐ 150 Recovery of Overpayment & Enforcement of Judgment
- ☐ 151 Medicare Act
- ☐ 152 Recovery of Defaulted Student Loans (Excl. Veterans)
- ☐ 153 Recovery of Overpayment of Veteran's Benefits
- ☐ 160 Stockholders' Suits
- ☐ 190 Other Contract
- ☐ 195 Contract Product Liability
- ☐ 196 Franchise

REAL PROPERTY
- ☐ 210 Land Condemnation
- ☐ 220 Foreclosure
- ☐ 230 Rent Lease & Ejectment
- ☐ 240 Torts to Land
- ☐ 245 Tort Product Liability
- ☐ 290 All Other Real Property

TORTS

PERSONAL INJURY
- ☐ 310 Airplane
- ☐ 315 Airplane Product Liability
- ☐ 320 Assault, Libel & Slander
- ☐ 330 Federal Employers' Liability
- ☐ 340 Marine
- ☐ 345 Marine Product Liability
- ☐ 350 Motor Vehicle
- ☐ 355 Motor Vehicle Product Liability
- ■ 360 Other Personal Injury
- ☐ 362 Personal Injury - Med. Malpractice

PERSONAL INJURY
- ☐ 365 Personal Injury - Product Liability
- ☐ 367 Health Care/ Pharmaceutical Personal Injury Product Liability
- ☐ 368 Asbestos Personal Injury Product Liability

PERSONAL PROPERTY
- ☐ 370 Other Fraud
- ☐ 371 Truth in Lending
- ☐ 380 Other Personal Property Damage
- ☐ 385 Property Damage Product Liability

CIVIL RIGHTS
- ☐ 440 Other Civil Rights
- ☐ 441 Voting
- ☐ 442 Employment
- ☐ 443 Housing/ Accommodations
- ☐ 445 Amer. w/Disabilities - Employment
- ☐ 446 Amer. w/Disabilities - Other
- ☐ 448 Education

PRISONER PETITIONS

Habeas Corpus:
- ☐ 463 Alien Detainee
- ☐ 510 Motions to Vacate Sentence

Other:
- ☐ 530 General
- ☐ 535 Death Penalty
- ☐ 540 Mandamus & Other
- ☐ 550 Civil Rights
- ☐ 555 Prison Condition
- ☐ 560 Civil Detainee – Conditions of Confinement

FORFEITURE/PENALTY
- ☐ 625 Drug Related Seizure of Property 21 USC 881
- ☐ 690 Other

LABOR
- ☐ 710 Fair Labor Standards Act
- ☐ 720 Labor/Mgmt. Relations
- ☐ 740 Railway Labor Act
- ☐ 751 Family and Medical Leave Act
- ☐ 790 Other Labor Litigation
- ☐ 791 Empl. Ret. Inc. Security Act

IMMIGRATION
- ☐ 462 Naturalization Application
- ☐ 465 Other Immigration Actions

BANKRUPTCY
- ☐ 422 Appeal 28 USC 158
- ☐ 423 Withdrawal 28 USC 157

PROPERTY RIGHTS
- ☐ 820 Copyrights
- ☐ 830 Patent
- ☐ 835 Patent – Abbreviated New Drug Application
- ☐ 840 Trademark
- ☐ 880 Defend Trade Secrets Act of 2016

SOCIAL SECURITY
- ☐ 861 HIA (1395ff)
- ☐ 862 Black Lung (923)
- ☐ 863 DIWC/DIWW (405(g))
- ☐ 864 SSID Title XVI
- ☐ 865 RSI (405(g))

FEDERAL TAX SUITS
- ☐ 870 Taxes (U.S. Plaintiff or Defendant)
- ☐ 871 IRS—Third Party 26 USC 7609

OTHER STATUTES
- ☐ 375 False Claims Act
- ☐ 376 Qui Tam (31 USC 3729 (a))
- ☐ 400 State Reapportionment
- ☐ 410 Antitrust
- ☐ 430 Banks and Banking
- ☐ 450 Commerce
- ☐ 460 Deportation
- ☐ 470 Racketeer Influenced and Corrupt Organizations
- ☐ 480 Consumer Credit (15 USC 1681 or 1692)
- ☐ 485 Telephone Consumer Protection Act (TCPA)
- ☐ 490 Cable/Sat TV
- ☐ 850 Securities/Commodities/ Exchange
- ☐ 890 Other Statutory Actions
- ☐ 891 Agricultural Acts
- ☐ 893 Environmental Matters
- ☐ 895 Freedom of Information Act
- ☐ 896 Arbitration
- ☐ 899 Administrative Procedure Act/Review or Appeal of Agency Decision
- ☐ 950 Constitutionality of State Statutes

V. ORIGIN *(Place an "X" in One Box Only)*

☐ 1 Original Proceeding ■ 2 Removed from State Court ☐ 3 Re-filed **(See VI below)** ☐ 4 Reinstated or Reopened ☐ 5 Transferred from another district *(specify)* ☐ 6 Multidistrict Litigation Transfer ☐ 7 Appeal to District Judge from Magistrate Judgment ☐ 8 Multidistrict Litigation – Direct File ☐ 9 Remanded from Appellate Court

VI. RELATED/ RE-FILED CASE(S)

(See instructions): a) Re-filed Case ☐YES ☐NO b) Related Cases ☐YES ■ NO

JUDGE: **DOCKET NUMBER:**

VII. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing and Write a Brief Statement of Cause ***(Do not cite jurisdictional statutes unless diversity)***:
28 U.S.C. Sections 1332, 1441, 1446, 1453 (Negligence, Breach of Express Contract, Breach of Implied Contract)
LENGTH OF TRIAL via 7 days estimated (for both sides to try entire case)

VIII. REQUESTED IN COMPLAINT:

☒ CHECK IF THIS IS A **CLASS ACTION** UNDER F.R.C.P. 23

DEMAND $

CHECK YES only if demanded in complaint:

JURY DEMAND: ■ Yes ☐ No

ABOVE INFORMATION IS TRUE & CORRECT TO THE BEST OF MY KNOWLEDGE

DATE: July 15, 2022

SIGNATURE OF ATTORNEY OF RECORD: Kristine McAlister Brown

FOR OFFICE USE ONLY : RECEIPT # **AMOUNT** IFP JUDGE MAG JUDGE

ClassAction.org