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

KASHARI DAVIS, individually and on behalf of all similarly situated persons, Plaintiff, v. MEDNAX SERVICES, INC., Defendant.	)	Case No. _____ [On Removal from the Circuit Court of the Seventeenth Judicial Circuit in and for Broward County, Case No. CACE-21-000625]

MEDNAX SERVICES, INC.'S NOTICE OF REMOVAL

PLEASE TAKE NOTICE that, pursuant to 28 U.S.C. §§ 1332(d), 1441(a), 1446, and 1453, Defendant Mednax Services, Inc. ("Mednax") hereby removes the above-captioned action, *Kashari Davis v. Mednax Services, Inc.*, Case No. CACE-21-000625 (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. Mednax 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 and where the amount in controversy for the putative class members in the aggregate exceeds the sum or value of $5,000,000, 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. 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 January 11, 2021, Plaintiff Kashari Davis ("Plaintiff") filed the State Court Action, individually and on behalf of all persons she claims 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 Mednax 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 process, pleadings, and orders filed 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, Plaintiff and the members of the putative class she purports to represent are persons whose personally identifiable information ("PII") was allegedly compromised in a phishing attack perpetrated by a criminal third-party actor against certain Microsoft Office 360-hosted Mednax business e-mail accounts. *See generally* Compl.

5. The Complaint alleges seven counts for: (1) negligence; (2) negligence per se; (3) breach of implied contract; (4) unjust enrichment; (5) breach of confidence; (6) violation of the Florida Deceptive and Unfair Trade Practices Act ("FDUTPA"), Fla. Stat. § 501.201 *et seq.*; and (7) violation of the North Carolina Unfair and Deceptive Trade Practices Act ("UDTPA"), N.C. Gen. Stat. § 75-1.1 *et seq*.

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 Plaintiff's 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. Mednax was served with a copy of the Summons and Complaint on January 15, 2021. This Notice has been filed within thirty (30) days after Mednax 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 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 Classes Contain At Least 100 Members in the Aggregate

9. Plaintiff purports to bring claims on behalf of a putative class of individuals she defines as: "All persons MEDNAX identified as being among those individuals impacted by the

Data Breach, including all who were sent a notice of the Data Breach." Compl. ¶ 116 (the "Nationwide Putative Class"). Plaintiff also purports to bring claims on behalf of a subclass of individuals defined as: "All persons residing in the State of North Carolina MEDNAX identified as being among those individuals impacted by the Data Breach, including all who were sent a notice of the Data Breach." *Id.* This subclass is a subset of the Nationwide Putative Class.

10. Plaintiff alleges that the Nationwide Putative Class includes approximately 1,290,670 people. Compl. ¶ 117. Therefore, CAFA's 100-person requirement is satisfied. *See Kelly v. State Farm Mut. Auto. Ins. Co.*, No. 5:10-cv-194-Oc-32GRJ, 2010 U.S. Dist. LEXIS 145840, at *9-10 (M.D. Fla. Sept. 23, 2010) (concluding that "CAFA's 100 person requirement" is satisfied because "Plaintiffs have alleged in the First Amended Class Complaint that it is believed the class contains more than 1,000 persons").

Minimal Diversity Exists

11. 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.

12. Plaintiff alleges that she is a citizen of North Carolina. Compl. ¶ 15.

13. Mednax is a corporation organized under the laws of Florida, with its principal place of business located at 1301 Concord Terrace, Sunrise, Florida 33323. Thus, Mednax is a citizen of Florida. *See* 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 . . .").

14. Because at least one member of the putative class, namely Plaintiff, is a citizen of North Carolina, and Mednax is a citizen of Florida, CAFA's minimal diversity requirement is met.

No Defendant Is a Governmental Entity

15. Mednax, the only Defendant, is a for-profit corporation. Accordingly, no defendant is a state, state official, or other governmental entity.

The Amount in Controversy Exceeds $5,000,000, Exclusive of Interest and Costs[1]

16. A notice of removal "need include only a plausible allegation that the amount in controversy exceeds the jurisdictional threshold." *Dart Cherokee Basin Operating Co., LLC v. Owens*, 547 U.S. 81, 89 (2014); *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." (alterations, internal quotation marks, and citation omitted)).

17. Based upon Plaintiff's allegations and theories, the amount in controversy exceeds $5,000,000 in the aggregate for the putative class, exclusive of interest and costs. These same allegations have spawned three overlapping class actions filed in federal district courts arising out of the same data security incident that gives rise to Plaintiff's claims here. The plaintiffs in those cases expressly allege that the amount in controversy exceeds $5,000,000. *See* Class Action Complaint, No. 21-cv-611, *Bean v. Mednax, Inc. et al.*, Dkt. No. 1 ¶ 25 (S.D. Fla. Jan. 18, 2021),

[1] Though Mednax disputes that Plaintiff is entitled to bring this action, vehemently denies liability, and contends that Plaintiff and the members of the putative class can recover nothing under the claims in the Complaint, for purposes of removal only, Plaintiff's allegations and the relief sought by Plaintiff 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).

a true and correct copy of which is attached as **Exhibit D** to this Notice; [2] Class Action Complaint, No. 21-cv-152, *Rumely v. Mednax, Inc.*, Dkt. No. 1 ¶ 36 (S.D. Cal. Jan. 27, 2021), a true and correct copy of which is attached as **Exhibit E** to this Notice; Class Action Complaint, No. 21-cv-20375, *Cohen v. Mednax Services, Inc.*, Dkt. No. 1 ¶ 13 (S.D. Fla. Jan. 28, 2021), a true and correct copy of which is attached as **Exhibit F** to this Notice. The same is true here.

18. Given the number of putative class members alleged in Plaintiff's Complaint, potential damages need only reach $3.88 per class member to exceed the jurisdictional minimum. This requirement is easily satisfied given the broad relief Plaintiff seeks. The Complaint seeks "compensatory and consequential damages" the members of the putative class purportedly suffered as a result of the phishing attack. Compl. ¶ 140. Among other things, Plaintiff seeks to recover "out-of-pocket expenses . . . incurred to remedy or mitigate the effects of the" phishing attack, including costs incurred for "[p]urchasing credit monitoring and identity theft protection." Compl. ¶ 112; *see also id.* ¶ 210 (alleging that "[a]s a direct and proximate result of Defendant's conduct, Plaintiff and the other members of the Class have been harmed and have suffered damages including, but not limited to . . . out-of-pocket expenses associated with procuring identity protection and restoration services").

19. The advertised monthly rates of credit monitoring services provided by the three national credit-reporting bureaus range from $14.95 to $19.95 per month at Equifax, $24.95 per month at TransUnion, and from $9.99 per month to $29.99 per month at Experian. *See* **Exhibit G**, which are true and correct copies of screenshots from the websites of the three national credit-reporting bureaus as of February 2021. Based on Plaintiff's assertion of class-wide damages based on the purchase of identity protection and restoration services, even applying the lowest advertised

[2] Plaintiff voluntarily dismissed this action without prejudice on February 2, 2021.

rate among any of the three national credit-reporting bureaus of $9.99 per month, the Complaint places over $12,800,000 in controversy based on a request for reimbursement for one month of identity protection and restoration services alone. The Complaint asserts that "Plaintiff and Class Members must vigilantly monitor their financial and medical accounts for many years to come," and thus suggests that they will continue to incur the costs of credit monitoring and identity theft protection (for which they seek recovery in the Complaint) for far more than just one month, bringing the amount in controversy even higher than set forth above. *See* Compl. ¶ 91.

20. While CAFA's amount in controversy threshold is easily satisfied based on the request for reimbursement for credit monitoring costs 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:

- **Other categories of out-of-pocket expenses**, including "late fees and declined payment fees imposed as a result of failed automatic payments that were tied to compromised cards that had to be cancelled," Compl. ¶ 112(j), and "costs associated with placing freezes on credit reports." *Id.* ¶ 198. These out-of-pocket expenses further increase the amount in controversy.
- **"[R]easonable attorneys' fees"** for an alleged violation of the Florida Deceptive and Unfair Trade Practices Act, Fla. Stat. § 501.201 *et seq.* *See Cohen v. Office Depot, Inc.*, 204. F.3d 1069, 1079 (11th Cir. 2000) (holding that attorneys' fees awarded under Florida Deceptive and Unfair Trade Practices Act are properly included in amount in controversy). While it is impossible to say with certainty at this stage what attorneys' fees will be reasonably expended by Plaintiff's counsel in this matter, Plaintiffs' lawyers routinely seek fees of over $1,000,000 in data breach class actions. For example, in the Wendy's

consumer data breach class action, Mr. Yanchunis asserted that an attorneys' fee of $1,020,000 was reasonable. *See* Dkt. No. 153, *Torres v. Wendy's Int'l, LLC*, No. 16-cv-210 (M.D. Fla. Feb. 14, 2019).

- **Disgorgement of proceeds** Mednax allegedly unjustly received from the members of the putative class. *See Compl.* ¶ 187; *Lorenzo v. MillerCoors LLC*, No. 16-20851-CV-KING, 2016 U.S. Dist. LEXIS 193195, at *4 (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 CAFA's jurisdictional threshold is satisfied. *S. Fla. Wellness v. Allstate Ins. Co.*, 745 F.3d 1312, 1316 (11th Cir. 2014).

21. 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

22. None of the exceptions to CAFA jurisdiction applies 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 Mednax's burden to demonstrate that any exception to CAFA does not apply.

CONCLUSION

23. 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 Mednax; (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.

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

25. Mednax reserves the right to amend this Notice of Removal.

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

Dated: February 12, 2021

Respectfully submitted,

s/ Martin B. Goldberg
Martin B. Goldberg
Florida Bar No. 827029
Jonathan E. Feuer
Florida Bar No. 68752
LASH & GOLDBERG LLP
Miami Tower
100 SE 2nd Street, Suite 1200
Miami, FL 33131-2158
Phone: (305) 347-4040
Fax: (305) 347-3050
mgoldberg@lashgoldberg.com
jfeuer@lashgoldberg.com

Kristine McAlister Brown
Florida Bar No. 443640
Gavin Reinke (*to be admitted pro hac vice*)
ALSTON & BIRD LLP
1201 West Peachtree Street
Atlanta, GA 30309
Phone: (404) 881-7000
Fax: (404) 881-7777
kristy.brown@alston.com
gavin.reinke@alston.com

JS 44 (Rev. 10/20) FLSD Revised 10/14/2020

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

Kashari Davis

DEFENDANTS

Mednax Services, Inc.

(b) County of Residence of First Listed Plaintiff Mecklenburg County, NC
(EXCEPT IN U.S. PLAINTIFF CASES)

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

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

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

Morgan & Morgan, 201 N. Franklin St., Tampa, FL, 813-223-5505

Attorneys *(If Known)*

Lash & Goldberg, 100 SE 2 St, Ste 1200, Miami, FL, 305-347-4040

(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)
- ☐ 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: Hon. Jose E. Martinez **DOCKET NUMBER:** 1:21-cv-20375-JEM

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, Negligence Per Se, 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 Febiacry 12, 2021

SIGNATURE OF ATTORNEY OF RECORD

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

EXHIBIT A

CT Corporation

Service of Process Transmittal

01/15/2021
CT Log Number 538893157

TO: Stacia Cunningham
Mednax Services, Inc.
1301 Concord Ter
Sunrise, FL 33323-2843

RE: **Process Served in Florida**

FOR: Mednax Services, Inc. (Domestic State: FL)

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

TITLE OF ACTION:	KASHARI DAVIS, INDIVIDUALLY AND ON BEHALF OF ALL SIMILARLY SITUATED PERSONS, Pltf. vs. MEDNAX SERVICES, INC., Dft.
DOCUMENT(S) SERVED:	-
COURT/AGENCY:	None Specified Case # CACE21000625
ON WHOM PROCESS WAS SERVED:	C T Corporation System, Plantation, FL
DATE AND HOUR OF SERVICE:	By Process Server on 01/15/2021 at 11:21
JURISDICTION SERVED :	Florida
APPEARANCE OR ANSWER DUE:	None Specified
ATTORNEY(S) / SENDER(S):	None Specified
ACTION ITEMS:	CT has retained the current log, Retain Date: 01/15/2021, Expected Purge Date: 01/20/2021 Image SOP Email Notification, Stacia Cunningham stacia_cunningham@mednax.com Email Notification, Risk Management risk_management@mednax.com
REGISTERED AGENT ADDRESS:	C T Corporation System 1200 South Pine Island Road Plantation, FL 33324 866-401-8252 EastTeam2@wolterskluwer.com

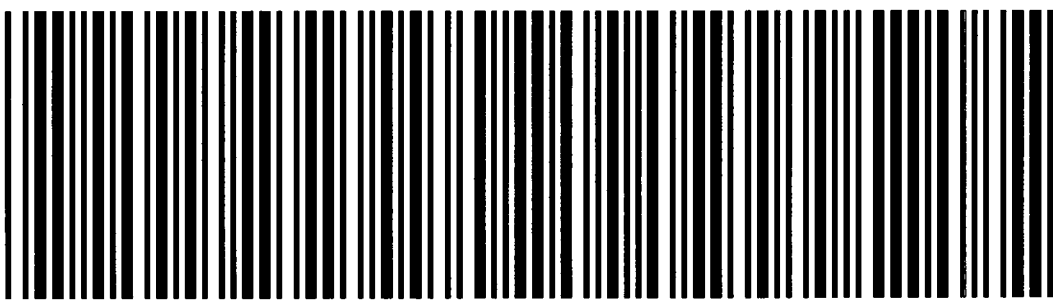
Wolters Kluwer

PROCESS SERVER DELIVERY DETAILS

Date: Fri, Jan 15, 2021

Server Name: Drop Service

Entity Served	MEDNAX SERVICES, INC.
Agent Name	CT CORPORATION SYSTEM
Case Number	CACE21000625
Jurisdiction	FL



Case Number: CACE-21-000625 Division: 04
Filing # 119386047 E-Filed 01/11/2021 12:28:21 PM

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

KASHARI DAVIS, individually and on behalf of all similarly situated persons,

Plaintiff,

v.

MEDNAX SERVICES, INC.,

Defendant.

Civil Action No. _____

CLASS REPRESENTATION

Jury Trial Demanded

Date 1/15/21 Time 11059
Initials _____ ID # 109

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:

MEDNAX SERVICES, INC.,
c/o REGISTERED AGENT
CT CORPORATION SYSTEM
1200 SOUTH PINE ISLAND ROAD
PLANTATION, FL 33324

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

John Yanchunis, Esquire
Morgan & Morgan Complex Litigation Group
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
(813) 223-5505 // FAX: (813) 223-5402
E-Mail: jyanchunis@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. Contact Diana Sobel, 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 are hearing or voice impaired, call 711."

WITNESS my hand and the seal of this Court on this the _____ day of _____, 2021.

JAN 12 2021

CLERK OF THE CIRCUIT COURT

By: _____
as Deputy Clerk
BRENDA D. FORMAN

IMPORTANTE

Usted ha sido demandado legalmente. Tiene veinte (20) dias, contados a partir del recibo de esta notificacion; para contestar la demanda adjunta, por escrito, y presentarla ante este tribunal. Una llamada telefonica no lo protegera; si usted desea que el tribunal considere su defensa, debe presentar su repuesta por escrito, incluyendo el numero del caso y los numbres de las partes interesadas en dicho caso. Si usted no contesta la demanda a tiempo, pudiese perder el caso y podria ser despojado de sus ingresos y propiedades, o privado de sus derechos, sin previo aviso del tribunal. Existen otros requisitos legales. Si lo desea, puede usted consultar a un abogado immediatamente. Si no conoce a un abogado, puede llamar a una de las oficinas de asistencia legal que aparecen en la guia telefonica.

Si desea responder a la demanda por su centa, al mismo tiempo en que presenta su respuesta ante el tribunal, debera usted inviar por correo o entregar una copia de su respuesta a la persona denuminada abajo como "Plaintiff/Plaintiff's Attorney." (Demandate o Abogado del Demanadante).

"De acuerdo con el Acto o' Decreto de los Americanos con Impedimentos Inhabilitados, personas en necesidad del servicio especial para particpar en estee procedimiento deberan, dentro de un tiempo razonable, antes de cualquier procedimiento, ponerse en un tiempo razonable, antes de cualquier procedimiento, ponerse en contacto con la oficina Administrativa de la Corte, Telefono (TDD) 1-800-955-8771 o (V) 1-800-955-8770, via Florida Relay System."

IMPORTANT

Des poursuites judiciaries ont ete entreprises contre vous. Vous avez 20 jours consecutifs a partir de la date de l'assignation de cet'te citation pour deposer une response ecrite a la plainte ci-jointe aupres de ce Tribunal. Un simple coup de telephone est insuffisant pour vous proteger' vous etes oblige de deposer votre reponse ecrite, avec mention du numero de dossier ci-dessus et du nom des parties nommees ici, si vous souhaitez que le Tribunal entende votre cause. Si vous ne deposez' pas votre reponse ecrite dans le relai requis, vous risquez de perdre la cause ainsi que votre salaire, votre argent, et vos biens peuvent etre saisis par la suite, sans aucun preavis ulterieur du Tribunal. Il y a d'autres obligations juridiques et vous pouvez requerir les services immediats d'un avocat. Si vous ne connaissez pas d'avocat, vous pourriez telephoner a un service de reference d'avocats ou a. un bureau d'assistance juridique (figurant a l'annuaire de telephones).

Si vous choisissez de deposer vous-meme une response ecrite, il vous faudra egalement, en meme temps que cette formalite, faire parvenir ou expedier une copie au carbone ou une photocopie de votre reponse ecrite au "Plaintiff/Plaintiff's Attorney" (Plaignant ou a son avocat) nomme ci-dessous.

En accordance avec la Loi des "Americans With Disabilities". Les personnes en besoin d'une accomodation speciale pour participer a ces procedures doivent, dans un temps raisonable, avant

d'entreprendre aucune autre demarche, contracter l'office administrative de la Court situe au le telephone ou Telefono (TDD) 1-800-955-8771 ou (V) 1-800-955-8770, via Florida Relay System."

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

Filing # 119386047 E-Filed 01/11/2021 12:28:21 PM

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

KASHARI DAVIS, individually and on behalf of all similarly situated persons,

Plaintiff,

v.

MEDNAX SERVICES, INC.,

Defendant.

Civil Action No. _____

CLASS REPRESENTATION

Jury Trial Demanded

CLASS ACTION COMPLAINT

Plaintiff KASHARI DAVIS ("Plaintiff"), individually and on behalf of all others similarly situated, brings this action against Defendant MEDNAX SERVICES, INC. ("MEDNAX" or "Defendant"), a Florida corporation, to obtain damages, restitution, and injunctive relief for the Class, as defined below, from Defendant. Plaintiff makes the following allegations upon information and belief, except as to her own actions, the investigation of her counsel, and the facts that are a matter of public record:

NATURE OF THE ACTION

1. This class action arises out of the recent targeted cyberattack and data breach ("Data Breach") at MEDNAX, a national health-care network that offers clinical care services, revenue cycle management, and patient engagement. As a result of the Data Breach, Plaintiff and approximately 1,290,670 Class Members suffered ascertainable losses in the form of the loss of the benefit of their bargain, out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the attack.

2. In addition, Plaintiff's and Class Members' sensitive personal information—which was entrusted to Defendant for safe keeping —was compromised and unlawfully accessed due to the Data Breach.

3. Information compromised in the Data Breach includes (1) patient contact information (such as patient names, dates of birth, guarantor names, addresses, and email addresses); (2) Social Security numbers, driver's license numbers, government identification numbers, and/or financial account numbers; (3) health insurance information (payor name, payor contract dates, policy information including type and deductible amount, and subscriber, Medicare, and Medicaid numbers); (4) medical and/or treatment information (dates of services, locations, services requested or procedures performed, diagnosis, prescription information, physician names, and Medical Record Numbers); and (5) billing and claims information (invoices, submitted claims and appeals, and patient account identifiers used by providers) and other protected health information as defined by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), and additional personally identifiable information ("PII") and protected health information ("PHI") that Defendant collected and maintained (collectively the "Private Information").

4. Plaintiff brings this class action lawsuit to address Defendant's inadequate safeguarding of Class Members' Private Information that it collected and maintained, and for failing to provide timely and adequate notice to Plaintiff and Class Members that their information had been subject to the unauthorized access of an unknown third party and precisely what specific type of information was accessed.

5. Defendant maintained the Private Information in a reckless manner.

6. In particular, the Private Information was maintained on Defendant's computer

network in a condition vulnerable to cyberattacks, such as the phishing attack that obtained Defendant's employees' credentials and access to Defendant's network.

7. Upon information and belief, the mechanism of the cyberattack and potential for improper disclosure of Plaintiff's and Class Members' Private Information was a known risk to Defendant, and thus Defendant was on notice that failing to take steps necessary to secure the Private Information from those risks left that property in a dangerous condition.

8. In addition, Defendant and its employees failed to properly monitor the computer network and systems that housed the Private Information. Had Defendant properly monitored its property, it would have discovered the intrusion sooner.

9. Plaintiff's and Class Members' identities are now at increased risk of identity theft because of Defendant's negligent conduct since the Private Information that Defendant collected and maintained is now in the hands of data thieves.

10. Armed with the Private Information accessed in the Data Breach, data thieves can commit a variety of crimes including, e.g., opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' names to obtain medical services, using Class Members' health information to target other phishing and hacking intrusions based on their individual health needs, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

11. As a result of the Data Breach, Plaintiff and Class Members have been exposed to a heightened and imminent risk of fraud and identity theft. Plaintiff and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft.

12. Plaintiff and Class Members may also incur out of pocket costs for, e.g., purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

13. Plaintiff seeks to remedy these harms on behalf of herself and all similarly situated individuals whose Private Information was accessed during the Data Breach.

14. Plaintiff seeks remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, and injunctive relief including improvements to MEDNAX's data security systems, future annual audits, and adequate credit monitoring services funded by Defendant.

PARTIES

15. Plaintiff Kashari Davis is, and at all times mentioned herein was, an individual citizen of the State of North Carolina residing in the City of Charlotte. Plaintiff is a patient who received health care services from Defendant's affiliated physician practice groups. Plaintiff was sent and received a "Notice of Data Security Event" letter dated December 16, 2020, a copy of which is attached hereto as Exhibit A.

16. Defendant MEDNAX is a healthcare services provider with its principal place of business at 1301 Concord Terrace, Sunrise, FL 33323.

JURISDICTION AND VENUE

17. The Court has subject matter jurisdiction over Plaintiff's 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.

18. Venue is proper in Broward County pursuant to Florida Stat. § 47.011 and § 47.051 because Defendant MEDNAX is headquartered and does business in this County, the cause of

action accrued in this county, and MEDNAX has an office for the transaction of its customary business in this county.

19. The Court has personal jurisdiction over Defendant because under Florida Stat. § 48.193, Defendant personally or through its agents operated, conducted, engaged in, or carried on a business or business venture in Florida and/or had offices in Florida committed tortious acts in Florida, and because Defendant engaged in significant business activity within Florida.

DEFENDANT'S BUSINESS

20. Defendant MEDNAX is a national healthcare services partner and provider offering newborn, anesthesia, maternal-fetal, radiology and teleradiology, pediatric cardiology, and other pediatric subspecialty care services in 39 states and Puerto Rico.[1]

21. In addition, Defendant operates a consulting services branch that provides administrative services and solutions to optimize performance, resources and capacity within hospitals and healthcare providers.[2]

22. In 2019, MEDNAX reported revenues of over $3.5 billion and had 4,327 physicians within its network.[3]

23. In the ordinary course of receiving treatment and health care services from MEDNAX, patients are required to provide sensitive personal and private information such as:

- Names;
- Dates of birth;
- Social Security numbers;

---

[1] *2019 Annual Report*, Mednax Health Solutions Partner (2019), at 3. Available at https://mednax.gcs-web.com/static-files/79b9289b-61f7-41a9-9394-81b99c902169 (last visited Jan. 4, 2021).
[2] *Id* at 7.
[3] *Id* at Selected Highlights.

- Driver's license numbers;
- Tribal identification numbers;
- Financial account information;
- Payment card information;
- Medical histories;
- Treatment information;
- Medication or prescription information;
- Beneficiary information;
- Provider information;
- Address, phone number, and email address, and;
- Health insurance information.

24. On information and belief, MEDNAX and its affiliated partners ("Agents") provide each of their customers with a HIPAA compliant Notice of its Privacy Practices (the "Privacy Notice") in respect to how they handle customers' sensitive information.[4]

25. The Privacy Notice provides, in relevant part, the following:

> I. WHO WE ARE
> This Notice of Privacy Practices ("Notice") describes the privacy practices of MEDNAX Services, Inc., and its affiliated entities, its physicians, nurses and other personnel ("we" or "us"). It applies to services furnished to you at all of the offices where we provide services.
>
> II. OUR PRIVACY OBLIGATIONS
>
> **We are required by law to maintain the privacy of your health information** ("Protected Health Information" or "PHI") and to provide you with this Notice of our legal duties and privacy practices

[4] *See Notice of Privacy Practices*, Mednax, https://www.mednax.com/notice-of-privacy-practices/ (last visited Jan. 5, 2021).

> with respect to your PHI. **We are also obligated to notify you following a breach of unsecured PHI.** When we use or disclose your PHI, we are required to abide by the terms of this Notice (or other notice in effect at the time of the use or disclosure).

Id. (emphasis added).

26. Thus, because of the highly sensitive and personal nature of the information MEDNAX acquires and stores with respect to its patients, MEDNAX promises in its Privacy Notice to, among other things, maintain the privacy of patients' health information.[5]

27. As a condition of receiving medical care and treatment at Defendant's Agents' facilities, Defendant requires that its patients entrust it with highly sensitive personal information.

28. By obtaining, collecting, using, and deriving a benefit from Plaintiff' and Class Members' Private Information, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' Private Information from disclosure.

29. Plaintiff and the Class Members have taken reasonable steps to maintain the confidentiality of their Private Information.

30. Plaintiff and the Class Members relied on Defendant to keep their Private Information confidential and securely maintained, to use this information for business and health purposes only, and to make only authorized disclosures of this information.

THE CYBERATTACK AND DATA BREACH

31. On or around June 19, 2020, MEDNAX became aware of suspicious activity related to "certain Microsoft Office 360-hosted MEDNAX business email accounts[.]"[6]

---

[5] *Id.*

[6] See https://oag.ca.gov/system/files/Attachment%20-%20CA%20Individual%20Notice%20Letters.pdf (last visited Jan 5, 2021).

32. MEDNAX launched an investigation into this suspicious activity and determined that certain employees improperly opened or handled email or email attachments that were part of a phishing scheme.

33. Upon information and belief, the phishing cyberattack was targeted at Defendant, due to its status as a healthcare entity that collects, creates, and maintains both PII and PHI.

34. Upon information and belief, the targeted phishing cyberattack was expressly designed to gain access to private and confidential data, including (among other things) the PII and PHI of patients like Plaintiff and the Class Members.

35. Because of this targeted phishing attack, data thieves were able to gain access to the employees' email accounts and subsequently access the protected Private Information of many MEDNAX clients and patients.

36. Further, MEDNAX's investigation also uncovered that the unauthorized intrusion and access occurred between June 17, 2020 and June 22, 2020.[7]

37. The email accounts and messages contained therein affected by this incident contained some combination of the following information: patient names, dates of birth, contact information, healthcare and medical information, insurance information, social security numbers, driver's license numbers, government identification numbers and/or financial account numbers.

38. The Private Information contained in the emails was not encrypted.

39. Plaintiff's Private Information was accessed and stolen in the Data Breach. Plaintiff further believes her stolen Private Information was subsequently sold on the Dark Web.

40. Unsurprisingly, MEDNAX could not rule out that Private Information was viewed

[7] *Id.*

or accessed in the Data Breach.[8]

41. MEDNAX informed impacted customers that they should take steps to "monitor and protect" their personal information, as well as that of their children.[9]

42. Further, MEDNAX offered impacted customers twelve months of identity monitoring services through Kroll.

43. The offer of identity monitoring services is an acknowledgment by MEDNAX that the impacted customers are subject to an imminent threat of identity theft.

44. Despite discovering the Data Breach in June 2020 and acknowledging that data thieves likely accessed Plaintiff's and the Class Members' Private Information, MEDNAX did not begin to notify affected patients until December 16, 2020, nearly six months later.

45. MEDNAX had obligations created by HIPAA, contract, industry standards, common law, and representations made to Plaintiff and Class Members to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

46. Plaintiff and Class Members provided their Private Information to MEDNAX and/or its Agents with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

47. MEDNAX's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in the healthcare industry preceding the date of the breach.

48. In light of recent high profile data breaches at other healthcare partner and provider

[8] *Id.*
[9] *Id.*

companies, including, American Medical Collection Agency (25 million patients, March 2019), University of Washington Medicine (974,000 patients, December 2018), Florida Orthopedic Institute (640,000 patients, July 2020), Wolverine Solutions Group (600,000 patients, September 2018), Oregon Department of Human Services (645,000 patients, March 2019), Elite Emergency Physicians (550,000 patients, June 2020), Magellan Health (365,000 patients, April 2020), and BJC Health System (286,876 patients, March 2020), MEDNAX knew or should have known that its electronic records would be targeted by cybercriminals

49. Indeed, cyberattacks have become so notorious that the Federal Bureau of Investigation and U.S. Secret Service have issued a warning to potential targets, so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive to ransomware criminals . . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[10]

50. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in MEDNAX's industry, including Defendant.

51. Phishing attacks of the type that the unauthorized persons used to gain access to Defendant's employee email accounts are among the oldest, most common, and well-known form of cyberattacks.

52. According to Verizon, over 90% of all cybersecurity attacks that result in a data breach start with a phishing attack.[11]

53. "Phishing is a cyber-attack that uses disguised email as a weapon. The goal is to

[10] *FBI, Secret Service Warn of Targeted*, Law360 (Nov. 18, 2019), https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware (last visited Jan. 5, 2021).
[11] *Verizon Says Phishing Drives 90% of Cybersecurity Breaches*, Graphus (Jan. 21, 2020), https://www.graphus.ai/verizon-says-phishing-still-drives-90-of-cybersecurity-breaches/ (last visited Jan. 5, 2021).

trick the email recipient into believing that the message is something they want or need — a request from their bank, for instance, or a note from someone in their company — and to click a link or download an attachment."[12] The fake link will typically mimic a familiar website and require the input of credentials. Once inputted, the credentials are then used to gain unauthorized access into a system. "It's one of the oldest types of cyber-attacks, dating back to the 1990s" and one that every organization with an internet presence is aware.[13] It remains the "simplest kind of cyberattack and, at the same time, the most dangerous and effective."[14]

54. Phishing attacks are generally preventable with the implementation of a variety of proactive measures such as purchasing and using some sort of commonly available anti-malware security software (such as the ubiquitous Malwarebites). Most cybersecurity tools have the ability to detect when a link or an attachment is not what it seems.[15]

55. Other proactive measures include sandboxing inbound e-mail (*i.e.*, an automated process that segregates e-mail with attachments and links to an isolated test environment, or a "sandbox," wherein a suspicious file or URL may be executed safely), inspecting and analyzing web traffic, penetration testing (which can be used to test an organization's security policy, its adherence to compliance requirements, its employees' security awareness and the organization's ability to identify and respond to security incidents), and employee education, just to name some of the well-known tools and techniques to prevent phishing attacks.

---

[12] Josh Fruhlinger, *What is Phishing? How This Cyber-Attack Works and How to Prevent It*, CSO Online (Sept. 4, 2020), https://www.csoonline.com/article/2117843/what-is-phishing-how-this-cyber-attack-works-and-how-to-prevent-it.html (last visited Jan. 5, 2021).
[13] *Id.*
[14] *What is Phishing?*, Malwarebytes, https://www.malwarebytes.com/phishing/ (last visited Jan. 5, 2021).
[15] *Id.*

Defendant Fails to Comply with FTC Guidelines

56. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

57. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[16] The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[17]

58. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

59. The FTC has brought enforcement actions against businesses for failing to protect

[16] *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016). Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Jan. 5, 2021).
[17] *Id.*

customer data adequately and reasonably, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

60. These FTC enforcement actions include actions against healthcare providers like Defendant. *See, e.g., In the Matter of Labmd, Inc., A Corp*, 2016-2 Trade Cas. (CCH) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) ("[T]he Commission concludes that LabMD's data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.")

61. Defendant failed to properly implement basic data security practices. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to patient PII and PHI constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

62. Defendant was at all times fully aware of its obligation to protect the PII and PHI of its patients. Defendant was also aware of the significant repercussions that would result from its failure to do so.

Defendant Fails to Comply with Industry Standards

63. As shown above, experts studying cyber security routinely identify healthcare providers as being particularly vulnerable to cyberattacks because of the value of the PII and PHI which they collect and maintain.

64. Several best practices have been identified that a minimum should be implemented by healthcare providers like Defendant, including but not limited to: educating all employees;

strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data; and limiting which employees can access sensitive data.

65. A number of industry and national best practices have been published and should be used as a go-to resource when developing an institution's cybersecurity standards. The Center for Internet Security (CIS) released its Critical Security Controls, and all healthcare institutions are strongly advised to follow these actions. The CIS Benchmarks are the overwhelming option of choice for auditors worldwide when advising organizations on the adoption of a secure build standard for any governance and security initiative, including PCI DSS, HIPAA, NIST 800-53, SOX, FISMA, ISO/IEC 27002, Graham Leach Bliley and ITIL.[18]

66. Other best cybersecurity practices that are standard in the healthcare industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.

67. Upon information and belief, Defendant failed to meet the minimum standards of the following cybersecurity frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are established standards in reasonable cybersecurity readiness.

[18] *See CIS Benchmarks FAQ*, Center for Internet Security, https://www.cisecurity.org/cis-benchmarks/cis-benchmarks-faq/ (last visited Jan. 5, 2021).

Defendant's Conduct Violates HIPAA and Evidences Its Insufficient Data Security

68. HIPAA requires covered entities to protect against reasonably anticipated threats to the security of sensitive patient health information.

69. Covered entities must implement safeguards to ensure the confidentiality, integrity, and availability of PHI. Safeguards must include physical, technical, and administrative components.

70. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§ 1301, *et seq*. These provisions require, among other things, that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling PII like the data MEDNAX left unguarded. The HHS subsequently promulgated multiple regulations under authority of the Administrative Simplification provisions of HIPAA. These rules include 45 C.F.R. § 164.306(a)(1-4); 45 C.F.R. § 164.312(a)(1); 45 C.F.R. § 164.308(a)(1)(i); 45 C.F.R. § 164.308(a)(1)(ii)(D), and 45 C.F.R. § 164.530(b).

71. Phishing attacks are also considered a breach under the HIPAA Rules because there is an access of PHI not permitted under the HIPAA Privacy Rule:

> A breach under the HIPAA Rules is defined as, "...the acquisition, access, use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of the PHI." *See* 45 C.F.R. 164.40[19]

72. MEDNAX's Data Breach resulted from a combination of insufficiencies that demonstrate they failed to comply with safeguards mandated by HIPAA regulations.

DEFENDANT'S BREACH

73. MEDNAX breached its obligations to Plaintiff and Class Members and/or was

[19] *See* https://onlinelibrary.wiley.com/doi/full/10.1111/1475-6773.13203 (last visited July 12, 2020).

otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and data. MEDNAX's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. Failing to adequately protect patients' Private Information;

c. Failing to properly monitor its own data security systems for existing intrusions;

d. Failing to ensure that its vendors with access to its computer systems and data employed reasonable security procedures;

e. Failing to train its employees in the proper handling of emails containing PII and PHI;

f. Failing to ensure the confidentiality and integrity of electronic PHI it created, received, maintained, and/or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

g. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

h. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. § 164.308(a)(1)(i);

i. Failing to implement procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);

j. Failing to protect against reasonably anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);

k. Failing to protect against reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);

l. Failing to ensure compliance with HIPAA security standard rules by its workforces in violation of 45 C.F.R. § 164.306(a)(4);

m. Failing to train all members of its workforces effectively on the policies and procedures regarding PHI as necessary and appropriate for the members of its workforces to carry out their functions and to maintain security of PHI, in violation of 45 C.F.R. § 164.530(b);

n. Failing to render the electronic PHI it maintained unusable, unreadable, or indecipherable to unauthorized individuals, as it had not encrypted the electronic PHI as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key" (45 CFR § 164.304's definition of "encryption");

o. Failing to comply with FTC guidelines for cybersecurity, in violation of Section 5 of the FTC Act, and;

p. Failing to adhere to industry standards for cybersecurity.

74. As the result of computer systems in dire need of security upgrading, inadequate procedures for handling emails containing viruses or other malignant computer code, and employees who opened files containing the virus or malignant code that perpetrated the

cyberattack, MEDNAX negligently and unlawfully failed to safeguard Plaintiff's and Class Members' Private Information.

75. Accordingly, as outlined below, Plaintiff and Class Members now face an increased risk of fraud and identity theft. In addition, Plaintiff and the Class Members also lost the benefit of the bargain they made with MEDNAX.

Cyberattacks and Data Breaches Put Consumers at an Increased Risk of Fraud and Identity Theft

76. Cyberattacks and data breaches at medical facilities like MEDNAX are especially problematic because of the increased risk of fraud and identity theft.

77. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[20]

78. That is because any victim of a data breach is exposed to serious ramifications regardless of the nature of the data. Indeed, the reason criminals steal personally identifiable information is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims and take over victims' identities in order to engage in illegal financial transactions under the victims' names. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity, or otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such

[20] *See* U.S. Gov. Accounting Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (2007). Available at https://www.gao.gov/new.items/d07737.pdf (last visited Jan. 5, 2021).

as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

79. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[21]

80. Identity thieves use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

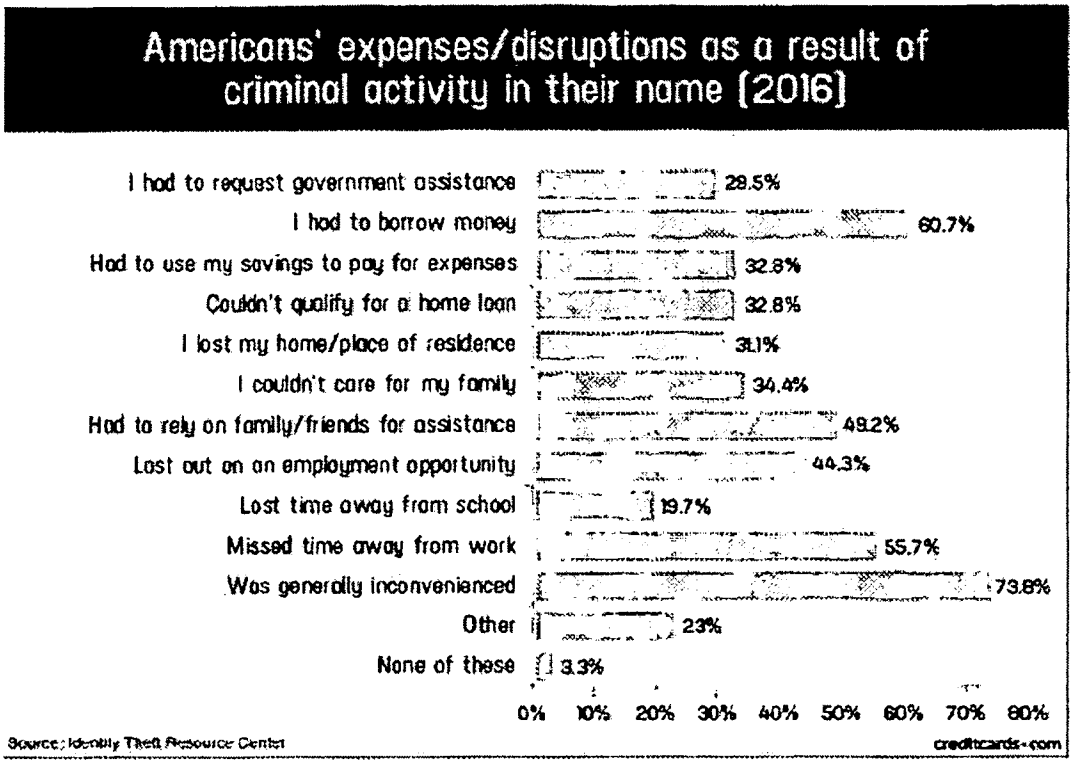
81. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

82. A study by Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information:[22]

---

[21] *See IdentityTheft.gov*, Federal Trade Commission, https://www.identitytheft.gov/Steps (last visited January 5, 2021).

[22] *See* Jason Steele, *Credit Card and ID Theft Statistics*, CreditCards.com (Oct. 23, 2020)



83. Moreover, theft of Private Information is also gravely serious. PII/PHI is a valuable property right.[23]

84. Its value is axiomatic, considering the value of "big data" in corporate America and the fact that the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

85. Theft of PHI, in particular, is gravely serious: "[a] thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance

https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php.

[23] *See, e.g.*, John T. Soma, et al. *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

provider, or get other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."[24]

86. Drug manufacturers, medical device manufacturers, pharmacies, hospitals and other healthcare service providers often purchase PII/PHI on the black market for the purpose of target marketing their products and services to the physical maladies of the data breach victims themselves. Insurance companies purchase and use wrongfully disclosed PHI to adjust their insureds' medical insurance premiums.

87. It must also be noted there may be a substantial time lag – measured in years -- between when harm occurs and when it is discovered, and also between when Private Information and/or financial information is stolen and when it is used.

88. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

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

See GAO Report, at p. 29.

89. Private Information is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

90. There is a strong probability that entire batches of stolen information have been dumped on the black market and are yet to be dumped on the black market, meaning Plaintiff and

[24] *See* Federal Trade Commission, *Medical Identity Theft*, http://www.consumer.ftc.gov/articles/0171-medical-identity-theft (last visited Jan. 5, 2021).

Class Members are at an increased risk of fraud and identity theft for many years into the future.

91. Thus, Plaintiff and Class Members must vigilantly monitor their financial and medical accounts for many years to come.

92. Sensitive Private Information can sell for as much as $363 per record according to the Infosec Institute.[25] PII is particularly valuable because criminals can use it to target victims with frauds and scams. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.

93. For example, the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines.[26] Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security Numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity.[27] Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

94. Moreover, it is not an 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. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of

[25] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/.
[26] *Identity Theft and Your Social Security Number*, Social Security Administration (2018) at 1. Available at https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Jan. 5, 2021).
[27] *Id* at 4.

that old bad information is quickly inherited into the new Social Security number."[28]

95. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."[29]

96. Medical information is especially valuable to identity thieves.

97. According to account monitoring company LogDog, coveted Social Security numbers were selling on the dark web for just $1 in 2016 – the same as a Facebook account.[30] That pales in comparison with the asking price for medical data, which was selling for $50 and up.[31]

98. Because of the value of its collected and stored data, the medical industry has experienced disproportionally higher numbers of data theft events than other industries.

99. For this reason, MEDNAX knew or should have known about these dangers and strengthened its data and email handling systems accordingly. MEDNAX was put on notice of the substantial and foreseeable risk of harm from a data breach, yet it failed to properly prepare for that risk.

Plaintiff's and Class Members' Damages

100. To date, Defendant has done absolutely nothing to provide Plaintiff and the Class

---

[28] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft.

[29] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, Computer World (Feb. 6, 2015), http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html.

[30] *See* Omri Toppol, *Email Security: How You Are Doing It Wrong & Paying Too Much*, LogDog (Feb. 14, 2016), https://getlogdog.com/blogdog/email-security-you-are-doing-it-wrong/.

[31] Lisa Vaas, *Ransomware Attacks Paralyze, and Sometimes Crush, Hospitals*, Naked Security (Oct. 3, 2019), https://nakedsecurity.sophos.com/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals/#content.

Members with relief for the damages they have suffered as a result of the Cyber-Attack and Data Breach. The identity monitoring offered by MEDNAX is wholly inadequate as the services are only offered for 12 months and it places the burden squarely on Plaintiff and Class Members by requiring them to expend time signing up for that service, as opposed to automatically enrolling all victims of this cybercrime.

101. Plaintiff and Class Members have been damaged by the compromise of their Private Information in the Data Breach.

102. After the Data Breach occurred, Plaintiff Davis received a substantial amount of scam phone calls which appeared to be placed with the intent to obtain personal information to commit identity theft by way of a social engineering attack.

103. Plaintiff's PII and PHI was compromised as a direct and proximate result of the Data Breach.

104. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft.

105. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been forced to expend time dealing with the effects of the Data Breach.

106. Plaintiff and Class Members face substantial risk of out-of-pocket fraud losses such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

107. Plaintiff and Class Members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their Private Information as potential fraudsters could use that information to target such schemes more effectively to Plaintiff and Class

Members.

108. Plaintiff and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

109. Plaintiff and Class Members also suffered a loss of value of their Private Information when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in related cases.

110. Plaintiff and Class Members were also damaged via benefit-of-the-bargain damages. Plaintiff and Class Members overpaid for a service that was intended to be accompanied by adequate data security but was not. Part of the price Plaintiff and Class Members paid to Defendant was intended to be used by Defendant to fund adequate security of MEDNAX's computer property and protect Plaintiff's and Class Members' Private Information. Thus, Plaintiff and the Class Members did not get what they paid for.

111. Plaintiff and Class Members have spent and will continue to spend significant amounts of time to monitor their financial and medical accounts and records for misuse. Indeed, Defendant's own notice of data breach provides instructions to Plaintiff and Class Members about all the time that they will need to spend monitor their own accounts, or to establish a "security freeze" on their credit report.[32]

112. Plaintiff and Class Members have suffered or will suffer actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the

[32] *See Notice of Data Security Event*, MEDNAX (Dec. 16, 2020), https://oag.ca.gov/system/files/Attachment%20-%20CA%20Individual%20Notice%20Letters.pdf.

Data Breach relating to:

a. Finding fraudulent charges;

b. Canceling and reissuing credit and debit cards;

c. Purchasing credit monitoring and identity theft prevention;

d. Addressing their inability to withdraw funds linked to compromised accounts;

e. Taking trips to banks and waiting in line to obtain funds held in limited accounts;

f. Placing "freezes" and "alerts" with credit reporting agencies;

g. Spending time on the phone with or at a financial institution to dispute fraudulent charges;

h. Contacting financial institutions and closing or modifying financial accounts;

i. Resetting automatic billing and payment instructions from compromised credit and debit cards to new ones;

j. Paying late fees and declined payment fees imposed as a result of failed automatic payments that were tied to compromised cards that had to be cancelled, and;

k. Closely reviewing and monitoring Social Security Number, medical insurance accounts, bank accounts, and credit reports for unauthorized activity for years to come.

113. Moreover, Plaintiff and Class Members have an interest in ensuring that their Private Information, which is believed to remain in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing personal and financial information is not accessible online, that access to such data is password-protected, and that such data is properly encrypted.

114. Further, as a result of MEDNAX's conduct, Plaintiff and Class Members are forced to live with the anxiety that their Private Information—which contains the most intimate details about a person's life, including what ailments they suffer, whether physical or mental—may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

115. As a direct and proximate result of MEDNAX's actions and inactions, Plaintiff and Class Members have suffered a loss of privacy and are at an imminent and increased risk of future harm.

CLASS REPRESENTATION ALLEGATIONS

116. Pursuant to Florida Rule of Civil Procedure 1.220, Plaintiff seeks certification of the following classes of persons defined as follows:

> **National Class:** All persons MEDNAX identified as being among those individuals impacted by the Data Breach, including all who were sent a notice of the Data Breach.
>
> **North Carolina Sub-Class:** All persons residing in the State of North Carolina MEDNAX identified as being among those individuals impacted by the Data Breach, including all who were sent a notice of the Data Breach.

Excluded from the Classes are any judges presiding over this matter and court personnel assigned to this case.

117. **Numerosity**: The Class Members are so numerous that joinder of all members is impracticable. Though the exact number and identities of Class Members are unknown at this time, the Classes reportedly include approximately 1,290,670 people. The identities of Class Members are ascertainable through MEDNAX's records, Class Members' records, publication notice, self-identification, and other means.

118. **Commonality**. There are questions of law and fact common to the Classes, which

predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether MEDNAX unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' Private Information;

b. Whether MEDNAX failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Cyber-Attack and Data Breach;

c. Whether MEDNAX's data security systems prior to and during the Cyber-Attack and Data Breach complied with applicable data security laws and regulations, *e.g.*, HIPAA;

d. Whether MEDNAX's data security systems prior to and during the Data Breach were consistent with industry standards;

e. Whether MEDNAX owed a duty to Class Members to safeguard their Private Information;

f. Whether MEDNAX breached its duty to Class Members to safeguard their Private Information;

g. Whether computer hackers obtained Class Members' Private Information in the Data Breach;

h. Whether MEDNAX knew or should have known that its data security systems and monitoring processes were deficient;

i. Whether MEDNAX owed a duty to provide Plaintiff and Class Members notice of this Data Breach, and whether Defendant breached that duty to provide timely notice;

j. Whether Plaintiff and Class Members suffered legally cognizable damages as a result of MEDNAX's misconduct;

k. Whether MEDNAX's conduct was negligent;

l. Whether MEDNAX's conduct violated federal law;

m. Whether MEDNAX's conduct violated state law;

n. Whether Plaintiff and Class Members are entitled to damages, civil penalties, nominal damages, and/or injunctive relief.

119. Common sources of evidence may also be used to demonstrate MEDNAX's unlawful conduct on a class-wide basis, including, but not limited to, documents and testimony about its data and cybersecurity measures (or lack thereof); testing and other methods that can prove MEDNAX's data and cybersecurity systems have been or remain inadequate; documents and testimony about the source, cause, and extent of the Data Breach; and documents and testimony about any remedial efforts undertaken as a result of the Data Breach.

120. **Typicality**. Plaintiff's claims are typical of the claims of the respective Class she seeks to represent, in that the named Plaintiff and all members of the proposed Class have suffered similar injuries as a result of the same practices alleged herein. Plaintiff has no interests adverse to the interests of the other members of the Class.

121. **Adequacy of Representation**. Plaintiff will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiff's Counsel is competent and experienced in litigating Class actions, including data privacy litigation of this kind.

122. The Class also satisfies the criteria for certification under Florida Rule of Civil Procedure 1.220(b). Among other things, Plaintiff avers that the prosecution of separate actions by the individual members of the proposed Class would create a risk of inconsistent or varying

adjudication which would establish incompatible standards of conduct for MEDNAX; that the prosecution of separate actions by individual class members would create a risk of adjudications with respect to them which would, as a practical matter, be dispositive of the interests of other class members not parties to the adjudications, or substantially impair or impede their ability to protect their interests; that MEDNAX has acted or refused to act on grounds that apply generally to the proposed Class, thereby making final injunctive relief or declaratory relief described herein appropriate with respect to the proposed Class as a whole; that questions of law or fact common to the Class predominate over any questions affecting only individual members and that class action treatment is superior to other available methods for the fair and efficient adjudication of the controversy which is the subject of this action. Plaintiff further states that the interests of judicial economy will be served by concentrating litigation concerning these claims in this Court, and that the management of the Class will not be difficult.

123. Plaintiff and other members of the Class have suffered injury, harm, and damages as a result of MEDNAX's unlawful and wrongful conduct. Absent a class action, MEDNAX will continue to maintain Class Members' Personal Information that could be subject to future breaches due to lax or non-existent cybersecurity measures, and such unlawful and improper conduct should not go remedied. Absent a class action, the members of the Class will not be able to effectively litigate these claims and will suffer further harm and losses, as MEDNAX will be allowed to continue such conduct with impunity and benefit from its unlawful conduct.

124. MEDNAX has acted on grounds that apply generally to the Classes as a whole, so that Class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

125. Certification is appropriate 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 MEDNAX owed a legal duty to Plaintiff and the Classes to exercise due care in collecting, storing, and safeguarding their Private Information;

b. Whether MEDNAX's security measures to protect their data systems were reasonable in light of best practices recommended by data security experts;

c. Whether MEDNAX's failure to institute adequate protective security measures amounted to negligence;

d. Whether MEDNAX failed to take commercially reasonable steps to safeguard consumer Private Information; and

e. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the data breach.

126. Finally, all members of the proposed Classes are readily ascertainable. MEDNAX has access to Class Members' names and addresses affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by MEDNAX.

CLAIMS FOR RELIEF

COUNT I
NEGLIGENCE
(On Behalf of Plaintiff and the Classes)

127. Plaintiff repeats and re-alleges each and every factual allegation contained in paragraphs 1-126 as if fully set forth herein. Plaintiff brings this claim individually and on behalf of the Class Members.

128. In order to receive medical treatments and services, MEDNAX and/or its Agents

required Plaintiff and Class Members to submit non-public Private Information, such as PII and PHI.

129. Plaintiff and Class Members entrusted their Private Information to MEDNAX and/or its Agents with the understanding that MEDNAX would safeguard their information.

130. By collecting and storing this data in its computer property, and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and safeguard its computer property—and Class Members' Private Information held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which they could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

131. Defendant owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the Private Information.

132. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and its client patients, which is recognized by laws and regulations including but not limited to HIPAA, as well as common law. Defendant was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from a data breach.

133. Defendant's duty to use reasonable security measures under HIPAA required Defendant to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to

protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1).

134. Some or all of the medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

135. In addition, Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

136. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential Private Information.

137. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;

b. Failing to adequately monitor the security of its networks and systems;

c. Failure to periodically ensure that its network system had plans in place to maintain reasonable data security safeguards;

d. Failing to adequately train its employees to recognize and contain phishing attacks;

e. Allowing unauthorized access to Class Members' Private Information;

f. Failing to detect in a timely manner that Class Members' Private Information had been compromised;

g. Failing to timely notify Class Members about the Cyber-Attack regarding what type of Private Information had been compromised so that they could take appropriate steps to mitigate the potential for identity theft and other damages; and

h. Failing to have mitigation and back-up plans in place in the event of a cyber-attack and data breach.

138. It was foreseeable that Defendant's failure to use reasonable measures to protect Class Members' Private Information would result in injury to Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the medical industry.

139. It was therefore foreseeable that the failure to adequately safeguard Class Members' Private Information would result in one or more types of injuries to Class Members.

140. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Cyber-Attack and data breach.

141. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit and identity monitoring to all Class Members.

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

142. Plaintiff realleges paragraphs 1–126 of this Complaint as if fully set forth herein. Plaintiff brings this claim on behalf of the Classes set forth above.

143. 71. Pursuant to HIPAA (42 U.S.C. § 1302d et seq.), the FTCA, and Florida law

(Fla. Stat. § 456.057 and § 501.171), MEDNAX was required by law to maintain adequate and reasonable data and cybersecurity measures to maintain the security and privacy of Plaintiff's and Class Members' Personal Information.

144. Plaintiff and Class Members are within the class of persons that the HIPAA was intended to protect.

145. The harm that occurred as a result of the Data Breach is the type of harm that HIPAA was intended to guard against. The Federal Health and Human Services' Office for Civil Rights ("OCR") has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures relating to protected health information, caused the same harm as that suffered by Plaintiffs and the Class.

146. Plaintiffs and Class Members are within the class of persons that the FTCA was intended to protect.

147. The harm that occurred as a result of the Data Breach is the type of harm the FTCA was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and the Class.

148. MEDNAX breached its duties by failing to employ industry standard data and cybersecurity measures to gain compliance with those laws, including, but not limited to, proper segregation, access controls, password protection, encryption, intrusion detection, secure destruction of unnecessary data, and penetration testing.

149. It was reasonably foreseeable, particularly given the growing number of data breaches of health information, that the failure to reasonably protect and secure Plaintiff's and Class Members' Personal Information in compliance with applicable laws would result in an

unauthorized third-party gaining access to MEDNAX's email accounts, networks, and computers that stored or contained Plaintiff's and Class Members' Personal Information.

150. Plaintiff's and Class Members' Personal Information constitutes personal property that was stolen due to MEDNAX'S negligence, resulting in harm, injury and damages to Plaintiff and Class Members.

151. MEDNAX's conduct in violation of applicable laws directly and proximately caused the unauthorized access and disclosure of Plaintiff's and Class Members' unencrypted Personal Information and Plaintiff and Class Members have suffered and will continue to suffer damages as a result of MEDNAX'S conduct. Plaintiff and Class Members seek damages and other relief as a result of MEDNAX's negligence.

COUNT III
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and the Classes)

152. Plaintiff re-alleges and incorporates by reference Paragraphs 1-126 above as if fully set forth herein.

153. Through their course of conduct, Defendant, Plaintiff, and Class Members entered into implied contracts for the provision of medical care and treatment, as well as implied contracts for Defendant to implement data security adequate to safeguard and protect the privacy of Plaintiff's and Class Members' Private Information.

154. Specifically, Plaintiff entered into a valid and enforceable implied contract with Defendant when she first went for medical care and treatment at one of Defendant's Agents' facilities.

155. The valid and enforceable implied contracts to provide medical health care services that Plaintiff and Class Members entered into with Defendant and/or its Agents include the promise

to protect non-public Private Information given to Defendant or that Defendant creates on its own from disclosure.

156. When Plaintiff and Class Members provided their Private Information to Defendant and/or its Agents in exchange for medical services, they entered into implied contracts with Defendant pursuant to which Defendant agreed to reasonably protect such information.

157. Defendant and/or its agents solicited and invited Class Members to provide their Private Information as part of Defendant's regular business practices. Plaintiff and Class Members accepted Defendant's offers and provided their Private Information to Defendant.

158. In entering into such implied contracts, Plaintiff and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations, including HIPAA, and were consistent with industry standards.

159. Class Members who paid money to Defendant reasonably believed and expected that Defendant would use part of those funds to obtain adequate data security. Defendant failed to do so.

160. Under the implied contracts, Defendant and/or its Agents promised and were obligated to: (a) provide healthcare to Plaintiff and Class Members; and (b) protect Plaintiff's and the Class Members' PII/PHI: (i) provided to obtain such health care; and/or (ii) created as a result of providing such health care. In exchange, Plaintiff and Members of the Class agreed to pay money for these services, and to turn over their Private Information.

161. Both the provision of medical services healthcare and the protection of Plaintiff's and Class Members' Private Information were material aspects of these implied contracts.

162. The implied contracts for the provision of medical services – contracts that include the contractual obligations to maintain the privacy of Plaintiff's and Class Members' Private

Information—are also acknowledged, memorialized, and embodied in multiple documents, including (among other documents) Defendant's Privacy Notice.

163. Defendant's express representations, including, but not limited to the express representations found in its Privacy Notice, memorializes and embodies the implied contractual obligation requiring Defendant to implement data security adequate to safeguard and protect the privacy of Plaintiff's and Class Members' Private Information.

164. Consumers of healthcare value their privacy, the privacy of their dependents, and the ability to keep their Private Information associated with obtaining healthcare private. To customers such as Plaintiff and Class Members, healthcare that does not adhere to industry standard data security protocols to protect Private Information is fundamentally less useful and less valuable than healthcare that adheres to industry-standard data security. Plaintiff and Class Members would not have entrusted their Private Information to Defendant and/or its Agents and entered into these implied contracts with Defendant without an understanding that their Private Information would be safeguarded and protected or entrusted their Private Information to Defendant in the absence of its implied promise to monitor its computer systems and networks to ensure that it adopted reasonable data security measures.

165. A meeting of the minds occurred, as Plaintiff and Members of the Class agreed to and did provide their Private Information to Defendant and/or its Agents, and paid for the provided healthcare in exchange for, amongst other things, both the provision of health care and medical services and the protection of their Private Information.

166. Plaintiff and Class Members performed their obligations under the contract when they paid for their health care services and provided their Private Information.

167. Defendant materially breached its contractual obligation to protect the non-public

Private Information Defendant gathered when the sensitive information was accessed by unauthorized personnel as part of the Cyber-Attack and Data Breach.

168. Defendant materially breached the terms of the implied contracts, including, but not limited to, the terms stated in the relevant Privacy Notice. Defendant did not maintain the privacy of Plaintiff's and Class Members' Private Information as evidenced by its notifications of the Data Breach to Plaintiff and approximately 1,290,670 Class Members. Specifically, Defendant did not comply with industry standards, standards of conduct embodied in statutes like HIPAA and Section 5 of the FTCA, or otherwise protect Plaintiff's and the Class Members' Private Information, as set forth above.

169. The Cyber-Attack and Data Breach was a reasonably foreseeable consequence of Defendant's actions in breach of these contracts.

170. As a result of Defendant's failure to fulfill the data security protections promised in these contracts, Plaintiff and Members of the Class did not receive the full benefit of the bargain, and instead received health care and other medical services that were of a diminished value to that described in the contracts. Plaintiff and Class Members therefore were damaged in an amount at least equal to the difference in the value of the healthcare with data security protection they paid for and the health care they received.

171. Had Defendant disclosed that its security was inadequate or that it did not adhere to industry-standard security measures, neither the Plaintiff, the Class Members, nor any reasonable person would have purchased healthcare from Defendant and/or its affiliated healthcare providers.

172. As a direct and proximate result of the Cyber-Attack/Data Breach, Plaintiff and Class Members have been harmed and have suffered, and will continue to suffer, actual damages

and injuries, including without limitation the release and disclosure of their Private Information, the loss of control of their Private Information, the imminent risk of suffering additional damages in the future, disruption of their medical care and treatment, out-of-pocket expenses, and the loss of the benefit of the bargain they had struck with Defendant.

173. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Cyber-Attack/Data Breach.

174. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, *e.g.*, (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit and identity monitoring to all Class Members.

COUNT IV
UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Classes)

175. Plaintiff re-alleges and incorporates by reference Paragraphs 1-126 above as if fully set forth herein.

176. This count is plead in the alternative to the breach of contract counts above.

177. Plaintiff and Class Members conferred a monetary benefit on Defendant. Specifically, they purchased goods and services from Defendant and/or its Agents and in so doing provided Defendant with their Private Information. In exchange, Plaintiff and Class Members should have received from Defendant the goods and services that were the subject of the transaction and have their Private Information protected with adequate data security.

178. Defendant knew that Plaintiff and Class Members conferred a benefit which Defendant accepted. Defendant profited from these transactions and used the Private Information of Plaintiff and Class Members for business purposes.

179. The amount Plaintiff and Class Members paid for goods and services were used, in part, to pay for use of Defendant's network and the administrative costs of data management and security.

180. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiff and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

181. Defendant failed to secure Plaintiff's and Class Members' Private Information and, therefore, did not provide full compensation for the benefit Plaintiff and Class Members provided.

182. Defendant acquired the Private Information through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

183. If Plaintiff and Class Members knew that Defendant had not reasonably secured their Private Information, they would not have agreed to Defendant's services.

184. Plaintiff and Class Members have no adequate remedy at law.

185. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (a) actual identity theft; (b) the loss of the opportunity of how their Private Information is used; (c) the compromise, publication, and/or theft of their Private Information; (d) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private Information; (e) lost opportunity costs associated with efforts expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (f) the continued risk to their Private Information, which remains in

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

186. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

187. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiff and Class Members overpaid for Defendant's services.

COUNT V
BREACH OF CONFIDENCE
(On Behalf of Plaintiff and the Classes)

188. Plaintiff re-alleges and incorporates by reference Paragraphs 1-126 above as if fully set forth herein.

189. At all times during Plaintiff's and Class Members' interactions with Defendant and/or its Agents, Defendant was fully aware of the confidential and sensitive nature of Plaintiff's and Class Members' Private Information.

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

191. Plaintiff and Class Members provided their Private Information to Defendant

and/or its Agents with the explicit and implicit understandings that Defendant would protect and not permit the Private Information to be disseminated to any unauthorized parties.

192. Plaintiff and Class Members also provided their Private Information to Defendant and/or its Agents with the explicit and implicit understandings that Defendant would take precautions to protect such Private Information from unauthorized disclosure.

193. Defendant voluntarily received in confidence Plaintiff's and Class Members' Private Information with the understanding that the Private Information would not be disclosed or disseminated to the public or any unauthorized third parties.

194. Due to Defendant's failure to prevent, detect, or avoid the Data Breach from occurring by, inter alia, following industry standard information security practices to secure Plaintiff's and Class Members' Private Information, Plaintiff's and Class Members' Private Information was disclosed and misappropriated to unauthorized third parties beyond Plaintiff's and Class Members' confidence, and without their express permission.

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

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

197. The injury and harm Plaintiff and Class Members suffered was the reasonably foreseeable result of Defendant's unauthorized disclosure of Plaintiff' and Class Members'

Private Information.

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

199. As a direct and proximate result of Defendant's breach of confidence, Plaintiff and Class Members have suffered and will continue to suffer injury and/or harm.

COUNT VI
VIOLATION OF THE FLORIDA DECEPTIVE AND UNFAIR TRADE PRACTICES ACT ("FDUTPA") FLA. STAT. § 501.201 ET SEQ.
(On Behalf of Plaintiff and the National Class)

200. Plaintiff re-alleges and incorporates by reference Paragraphs 1-126 above as if fully set forth herein.

201. FDUTPA prohibits "unfair methods of competition, unconscionable acts or practices, and unfair or deceptive acts or practices in the conduct of any trade or commerce." Fla.

Stat.§ 501.204.

202. Defendant engaged in the conduct alleged in this Complaint through transactions in and involving trade and commerce. Mainly, the Phishing Attack and Data Breach occurred through the use of the internet, an instrumentality of interstate commerce.

203. While engaged in trade or commerce, Defendant has violated FDUTPA, including, among other things, by:

a. Failing to implement and maintain appropriate and reasonable security procedures and practices to safeguard and protect the Private Information of Defendant's client patients from unauthorized access and disclosure;

b. Failing to disclose that its computer systems and data security practices were inadequate to safeguard and protect the Private Information of Defendant's client patients from being compromised, stolen, lost, or misused; and

c. Failing to disclose the Data Breach to Defendant's client patients in a timely and accurate manner in violation of Fla. Stat. § 501.171.

204. Defendant knew or should have known that the MEDNAX computer systems and data security practices were inadequate to safeguard Class Members' Private Information entrusted to it, and that risk of a data breach or theft was highly likely.

205. Defendant should have disclosed this information because Defendant was in a superior position to know the true facts related to the defective data security.

206. Defendant's failures constitute false and misleading representations, which have the capacity, tendency, and effect of deceiving or misleading consumers (including Plaintiff and Class Members) regarding the security of MEDNAX's network and aggregation of Private

Information.

207. The representations upon which impacted individuals (including Plaintiff and Class Members) relied were material representations (e.g., as to Defendant's adequate protection of Private Information), and consumers (including Plaintiff and Class Members) relied on those representations to their detriment.

208. Defendant's actions constitute unconscionable, deceptive, or unfair acts or practices because, as alleged herein, Defendant engaged in immoral, unethical, oppressive, and unscrupulous activities that are and were substantially injurious to Defendant's client patients.

209. In committing the acts alleged above, Defendant engaged in unconscionable, deceptive, and unfair acts and practices acts by omitting, failing to disclose, or inadequately disclosing to Defendant's client patients that it did not follow industry best practices for the collection, use, and storage of Private Information.

210. As a direct and proximate result of Defendant's conduct, Plaintiff and other Members of the Class have been harmed and have suffered damages including, but not limited to: damages arising from attempted identity theft and fraud; out-of-pocket expenses associated with procuring identity protection and restoration services; increased risk of future identity theft and fraud, and the costs associated therewith; and time spent monitoring, addressing and correcting the current and future consequences of the Data Breach.

211. As a direct and proximate result of Defendant's unconscionable, unfair, and deceptive acts and omissions, Plaintiff's and Class Members' Private Information was disclosed to third parties without authorization, causing and will continue to cause Plaintiff and Class Members damages. Accordingly, Plaintiff and Class Members are entitled to recover actual damages, an order providing declaratory and injunctive relief, and reasonable attorneys' fees and

costs, to the extent permitted by law.

COUNT VII
VIOLATION OF THE NORTH CAROLINA UNFAIR AND DECEPTIVE TRADE PRACTICES ACT ("UDTPA") N.C. GEN. STAT. § 75-1.1 ET SEQ.
(On Behalf of Plaintiff and the North Carolina Sub-Class)

213. Plaintiff re-alleges and incorporates by reference Paragraphs 1-126 above as if fully set forth herein.

214. UDTPA declares unlawful "unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce[.]" N.C. Gen. Stat.§ 75-1.1(a).

215. Defendant engaged in the conduct alleged in this Complaint through transactions in and involving commerce. Mainly, the Phishing Attack and Data Breach occurred through the use of the internet, an instrumentality of interstate commerce.

216. While engaged in commerce, Defendant has violated UDTPA, including, among other things, by:

a. Failing to implement and maintain appropriate and reasonable security procedures and practices to safeguard and protect the Private Information of Defendant's client patients from unauthorized access and disclosure;
b. Failing to disclose that its computer systems and data security practices were inadequate to safeguard and protect the Private Information of Defendant's client patients from being compromised, stolen, lost, or misused; and
c. Failing to disclose the Data Breach to Defendant's client patients without unreasonable delay in violation of N.C. Gen. Stat. § 75-65(a).

217. Defendant knew or should have known that the MEDNAX computer systems and data security practices were inadequate to safeguard North Carolina Class Members' Private Information entrusted to it, and that risk of a data breach or theft was highly likely.

218. Defendant should have disclosed this information because Defendant was in a superior position to know the true facts related to the defective data security.

219. Defendant's failures constitute false and misleading representations, which have the capacity, tendency, and effect of deceiving or misleading consumers (including Plaintiff and North Carolina Class Members) regarding the security of MEDNAX's network and aggregation of Private Information.

220. The representations upon which impacted individuals (including Plaintiff and North Carolina Class Members) relied were material representations (e.g., as to Defendant's adequate protection of Private Information), and consumers (including Plaintiff and North Carolina Class Members) relied on those representations to their detriment.

221. Defendant's actions constitute deceptive and unfair acts or practices because, as alleged herein, Defendant engaged in immoral, unethical, oppressive, and unscrupulous activities that are and were substantially injurious to Defendant's client patients.

222. In committing the acts alleged above, Defendant engaged in deceptive and unfair acts and practices acts by omitting, failing to disclose, or inadequately disclosing to Defendant's client patients that it did not follow industry best practices for the collection, use, and storage of Private Information.

223. As a direct and proximate result of Defendant's conduct, Plaintiff and other Members of the Class have been harmed and have suffered damages including, but not limited to: damages arising from attempted identity theft and fraud; out-of-pocket expenses associated with

procuring identity protection and restoration services; increased risk of future identity theft and fraud, and the costs associated therewith; and time spent monitoring, addressing and correcting the current and future consequences of the Data Breach.

224. As a direct and proximate result of Defendant's unfair and deceptive acts and omissions, Plaintiff's and Class Members' Private Information was disclosed to third parties without authorization, causing and will continue to cause Plaintiff and Class Members damages. Accordingly, Plaintiff and Class Members are entitled to recover actual damages, an order providing declaratory and injunctive relief, and reasonable attorneys' fees and costs, to the extent permitted by law.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on her own and behalf of all others similarly situated, prays for relief as follows:

A. For an Order certifying this case as a class action pursuant to Florida Rule of Civil Procedure 1.220, appointing Plaintiff as Class Representatives, and the undersigned as Class Counsel;

B. Awarding monetary and actual damages, including at a minimum, nominal damages, and/or restitution, as appropriate;

C. Awarding declaratory and injunctive relief as permitted by law or equity to assure that the Class has an effective remedy, including enjoining MEDNAX from continuing the unlawful practices as set forth above;

D. Prejudgment interest to the extent allowed by the law;

E. Awarding all costs, experts' fees and attorneys' fees, expenses and costs of prosecuting this action; and

F. Such other and further relief as the Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands a trial by jury of all claims so triable.

DATED: January 11, 2021

Respectfully submitted,

MORGAN & MORGAN COMPLEX
LITIGATION GROUP
201 N. Franklin Street, 7th Floor
Tampa, FL 33602
Telephone: (813) 223-5505
Facsimile: (813) 222-2434

/s/ John A. Yanchunis
John A. Yanchunis
Florida Bar Number 324681
Ryan D.Maxey
Florida Bar Number 59283
Email: jyanchunis@forthepeople.com
Email: rmaxey@forthepeople.com

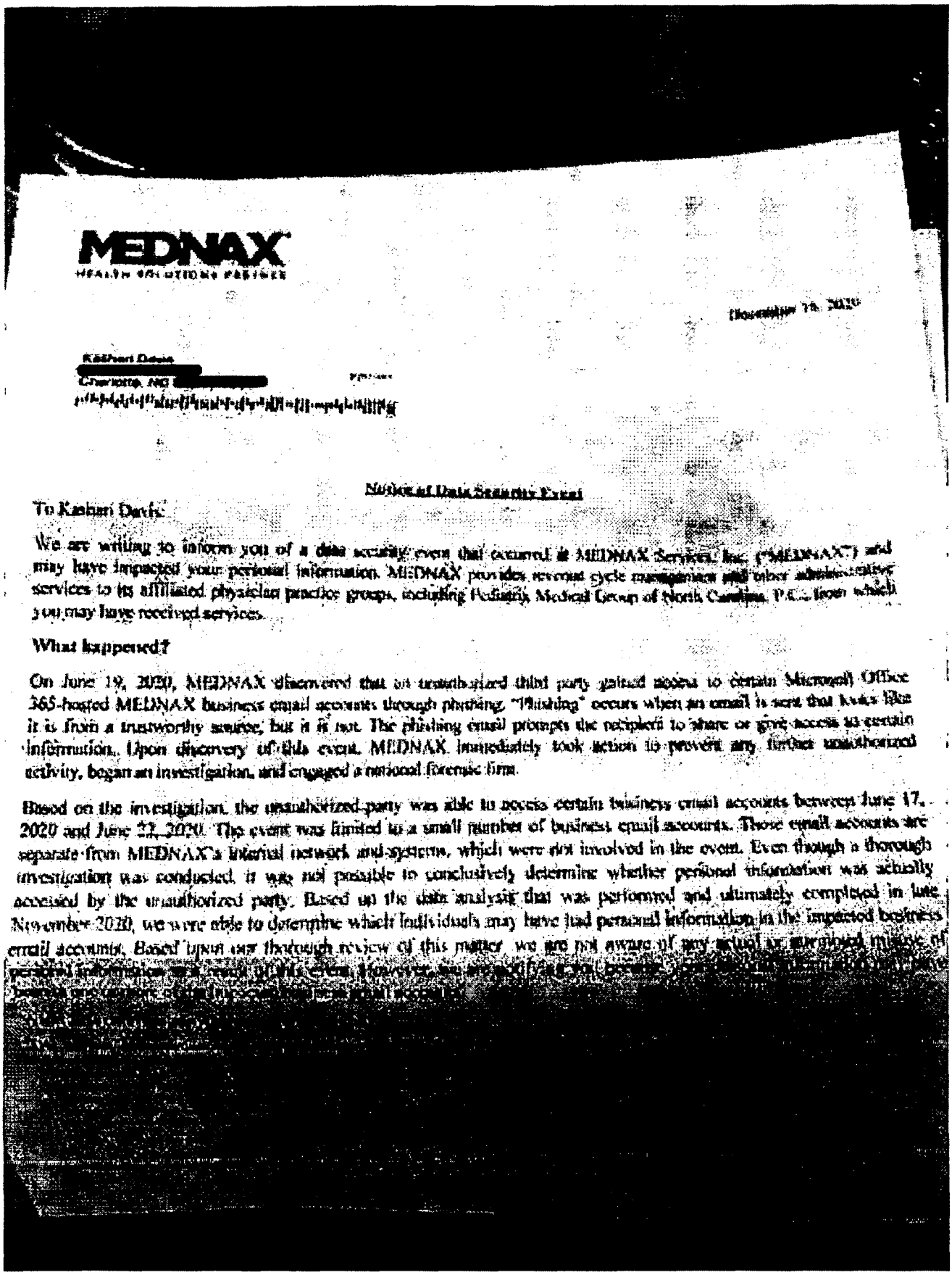
Gary E. Mason*
David K. Lietz*
MASON LIETZ & KLINGER LLP
5301 Wisconsin Avenue, NW
Suite 305
Washington, DC 20016
Tel: (202) 429-2290
gmason@masonllp.com
dlietz@masonllp.com

Gary M. Klinger*
MASON LIETZ & KLINGER LLP
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Tel: (202) 429-2290
gklinger@masonllp.com

**pro hac vice to be filed*

Attorneys for Plaintiff and the Proposed Class

EXHIBIT A



MEDNAX
HEALTH SOLUTIONS PARTNER

[redacted]

Notice of Data Security Event

To Kashuri Davis:

We are writing to inform you of a data security event that occurred at MEDNAX Services, Inc. ("MEDNAX") and may have impacted your personal information. MEDNAX provides revenue cycle management and other administrative services to its affiliated physician practice groups, including Pediatrix Medical Group of North Carolina, P.A., from which you may have received services.

What happened?

On June 19, 2020, MEDNAX discovered that an unauthorized third party gained access to certain Microsoft Office 365-hosted MEDNAX business email accounts through phishing. "Phishing" occurs when an email is sent that looks like it is from a trustworthy source, but it is not. The phishing email prompts the recipient to share or give access to certain information. Upon discovery of this event, MEDNAX immediately took action to prevent any further unauthorized activity, began an investigation, and engaged a national forensic firm.

Based on the investigation, the unauthorized party was able to access certain business email accounts between June 17, 2020 and June 23, 2020. The event was limited to a small number of business email accounts. Those email accounts are separate from MEDNAX's internal network and systems, which were not involved in the event. Even though a thorough investigation was conducted, it was not possible to conclusively determine whether personal information was actually accessed by the unauthorized party. Based on the data analysis that was performed and ultimately completed in late November 2020, we were able to determine which individuals may have had personal information in the impacted business email accounts. Based upon our thorough review of this matter, we are not aware of any actual or attempted misuse of personal information as a result of this event. However, we are notifying you because your personal information was present in the impacted business email accounts.

Reference Guide

Review Your Account Statements

Carefully review statements sent to you from providers as well as from your insurance company to ensure that all account activity is valid. Report any questionable charges promptly to the provider's billing office, or for insurance statements, to your insurance company.

Provide Any Updated Personal Information to Your Health Care Provider

Your health care provider's office may ask to see a photo ID to verify your identity. Please bring a photo ID with you to every appointment if possible. Your provider's office may also ask you to confirm your date of birth, address, telephone, and other pertinent information so that they can make sure that all of your information is up to date. Please be sure and tell your provider's office when there are any changes to your information. Carefully reviewing this information with your provider's office at each visit can help to avoid problems and to address them quickly should there be any discrepancies.

Order Your Free Credit Report

To order your free annual credit report, visit www.annualcreditreport.com, call toll-free at [illegible], or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's ("FTC") website at [illegible] and mail it to Annual Credit Report Request Service, P.O. Box [illegible], Atlanta, GA [illegible]. The three credit bureaus provide free annual credit reports only through the website, toll-free number or request form.

Upon receiving your credit report, review it carefully. Look for accounts you did not open. Look in the "inquiries" section for names of creditors from whom you have not requested credit. Some companies bill under names other than their store or commercial names; the credit bureau will be able to tell if this is the case. Look in the "personal information" section for any inaccuracies in information (such as home address and Social Security Number).

If you see anything you do not understand, call the credit bureau at the telephone number on the report. Errors may be a warning sign of possible identity theft. You should notify the credit bureaus of any inaccuracies in your report, whether due to error or fraud, as soon as possible so the information can be investigated and, if found to be in error, corrected. If there are accounts or charges you did not authorize, immediately notify the appropriate credit bureau by telephone and in writing. Information that cannot be explained should also be reported to your local police or sheriff's office because it may signal criminal activity.

Contact the U.S. Federal Trade Commission

If you detect any unauthorized transactions in any of your financial accounts, promptly notify the appropriate payment card company or financial institution. If you detect any incidents of identity theft or fraud, promptly report the matter to your local law enforcement authorities, state Attorney General and the FTC.

You can contact the FTC to learn more about how to protect yourself from becoming a victim of identity theft by using the contact information below:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-IDTHEFT (438-4338)
www.ftc.gov/idtheft

Place a Fraud Alert on Your Credit File

To protect yourself from possible identity theft, consider placing a fraud alert on your credit file. A fraud alert helps protect against the possibility of an identity thief opening new credit accounts in your name. When a credit grantor checks the credit history of someone applying for credit, the credit grantor gets a notice that the applicant may be the victim of identity theft. The alert notifies the credit grantor to take steps to verify the identity of the applicant. You can place a fraud alert on your credit report by calling any one of the toll-free fraud numbers provided below. You will reach an automated telephone system that allows flagging of your file with a fraud alert at all three credit bureaus.

Equifax	P.O. Box 105069 Atlanta, Georgia 30348	800-525-6285	www.equifax.com
Experian	P.O. Box 2002 Allen, Texas 75013	888-397-3742	www.experian.com
TransUnion	P.O. Box 2000 Chester, PA 19016	800-680-7289	www.transunion.com