UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA

Case No.: 0:21-md-02994-RAR

In re:

MEDNAX SERVICES, INC.,
CUSTOMER DATA SECURITY BREACH LITIGATION
_____/

This Document Relates to All Actions

PLAINTIFFS' RESPONSE IN OPPOSITION TO MEDNAX INC.; MEDNAX SERVICES, INC.; PEDIATRIX MEDIAL GROUP; AND PEDIATRIX MEDIAL GROUP OF KANSAS, P.C.'S MOTION FOR SUMMARY JUDGMENT AND MEMORANDUM OF LAW IN SUPPORT

TABLE OF CONTENTS

I. INTRODUCTION 1

II. STANDARD OF REVIEW 1

III. ARGUMENT 2

a. Plaintiffs Have Set Forth Sufficient Facts to Support Article III Standing. 2

1. The Eleventh Circuit's Decision in *Green-Cooper v. Brinker International, Inc.* Does Not Affect This Court's Prior Holding that Actual Misuse or Access of Data is Sufficient to Satisfy Article III's Injury-in-Fact Requirement. 3

2. Plaintiffs Have Demonstrated Actual Misuse of Their Data That is Fairly Traceable to the Data Breach. 4

i. Plaintiffs' Social Security Numbers Were Found on the Dark Web. 4

ii. Plaintiffs Have Produced Evidence of Spam Emails, Text Messages, and Phone Calls, as well as Evidence of Other Misuse of PII and PHI. 6

3. Plaintiffs Have Demonstrated Actual Access of Their PII/PHI Resulting in a Substantial Risk of Future Harm. 7

4. Plaintiffs Have Satisfied the Standard Set Forth in *TransUnion, LLC v. Ramirez* to Support Their Claim for Damages. 7

i. Plaintiffs Have Suffered Emotional Damages. 8

ii. Plaintiffs Have Taken Reasonable Mitigating Measures to Protect Themselves Against Future Harm 8

iii. Plaintiffs Have Suffered a Diminution in Value of Their PII and PHI. 9

iv. Plaintiffs Have Suffered a Loss of Privacy 10

b. The Facts Show that Defendants Violated State Statutory Laws. 10

1. Evidence exists that Mednax violated the Maryland Consumer Protection Act 10

2. Plaintiff Larsen Has Established A Genuine Issue of Material Fact as to His Arizona Consumer Fraud Act Claim. 13

3. Plaintiff Rumely Has Established that Genuine Issues of Material Fact Exist as to His California Consumer Records Act Claim.....14

5. Plaintiff Jay Has Established that Genuine Issues of Material Fact Exist as to Her WCPA Claim.....17

6. There are Genuine Issues of Facts as to Whether Mednax Violated the Florida Deceptive and Unfair Trade Practices Act. 19

c. There are Genuine Issues of Material Fact as to Plaintiffs' Negligence Claims. 20

1. Plaintiffs' Negligence Claims Are Governed by Florida Law.....20

2. Mednax Had a Duty to Protect Plaintiffs' PII/PHI. 22

3. Plaintiffs' Claims Are Not Barred by the Economic Loss Rule. 23

4. Plaintiffs Have More Than a Scintilla of Evidence to Establish Damages. 24

i. Evidence that Plaintiffs' PII/PHI was Improperly Disclosed and Is Being Sold on the Dark Web. 24

ii. Plaintiffs' Mitigation of Costs and Damages.....25

5. There Exists a Genuine Issue of Material Fact as to Causation.....26

6. Conclusion.....26

IV. CONCLUSION 27

TABLE OF AUTHORITIES

CASES

Allen v. Bank of Am., N.A.
933 F. Supp. 2d 716 (D. Md. 2013) 11

Alpert v. Nationstar Mortg. LLC
No. 15-cv-1164, 2019 WL 1200541 (W.D. Wash. Mar. 14, 2019) 18

Anderson v. Liberty Lobby, Inc.
477 U.S. 242 (1986) 1–2, 16

Ayers v. Ocwen Loan Servicing, LLC
129 F. Supp. 3d 249 (D. Md. 2015) 10–11

Baldwin v. Nat'l W. Life Ins. Co.
No. 2:21-CV-04066-WJE, 2021 WL 4206736 (W.D. Mo. Sept. 15, 2021) 21

Bannum v. City of Ft. Lauderdale
901 F.2d 989 (11th Cir. 1990) 2

Bank of Am., N.A. v. Jill P. Mitchell Living Trust
822 F. Supp. 2d 505 (D. Md. 2011) 11–12

Buckley v. Santander Consumer USA, Inc.
No. C17-5813 BHS, 2018 WL 1532671 (W.D. Wash. Mar. 29, 2018) 22–23

Burrows v. Purchasing Power, LLC
No. 1:120CV022800-UU, 2012 WL 9391827 (S.D. Fla. Oct. 18, 2012) 19

Carr v. Oklahoma Student Loan Auth.
No. CIV-23-99-R, 2023 WL 6929850 (W.D. Okla. Oct. 19, 2023) 23

Clark v. Bank of America, N.A.
561 F. Supp. 3d 542 (D. Md. 2021) 10

Chavez v. Mercantil Commercebank, N.A.
701 F.3d 896 (11th Cir. 2012) 16

Corona v. Sony Pictures Ent'mt
No. 14-CV-09600 RGK, 2015 WL 3916744 (C.D. Cal. June 15, 2015) 15

Davis v. Williams
451 F.3d 759 (11th Cir. 2006) 2

Deegan v. Windermere Real Estate / Ctr.-Isle, Inc
197 Wash. App. 875, 391 P.3d 582 (2017) 18

Edmondson v. Velvet Lifestyles, LLC
43 F.4th 1153 (11th Cir. 2022) 1

Farmer v. Humana, Inc.
582 F. Supp. 3d 1176 (M.D. Fla. 2022) 19

F.T.C. v. Wyndham Worldwide Corp.
799 F.3d 236 (3d Cir. 2015) 19

Focus on the Family v. Pinellas Suncoast Transit Auth.
344 F.3d 1263 (11th Cir. 2003) 4

Garcia v. City of Fresno
No. 116CV01340LJOSAB, 2017 WL 6383814 (E.D. Cal. Dec. 14, 2017) 16

Garner v. Medicis Pharmaceutical Corp.
2023 WL 6295052 (D. Ariz. Sept. 27, 2023) 13

Gray v. Amazon.com, Inc.
653 F. Supp. 3d 847 (W.D. Wa. 2023) 17

Green-Cooper v. Brinker International, Inc.
73 F. 4th 883 (11th Cir. 2023) 3–4, 20–21

Green v. eBay Inc.
No. CIV.A. 14-1688, 2015 WL 2066531 (E.D. La. May 4, 2015) 25

Griffey v. Magellan Health Inc.
562 F. Supp. 3d 34 (D. Ariz. 2021) 25

Gonzalez-Gonzalez-Jimenez de Ruiz v U.S.
231 F.Supp.2d 1187 (M.D. Fla. 2002) 8

Hutchins v. Frontier Airlines, Inc.
No. 23-CV-80210-ROSENBERG, 2023 WL 7461324 (S.D. Fla. Oct. 13, 2023) 2

Huynh v. Quora, Inc.
508 F. Supp. 3d 633 (N.D. Cal. 2020) 24

In re 21st Century Oncology Customer Data Security Breach Litig.
380 F. Supp. 3d 1243 (M.D. Fla. 2019) 24

In re Anthem, Inc. Data Breach Litig.
327 F.R.D. 299 (N.D. Cal. 2018) 22

In re Banner Health Data Breach Litig.
No. CV-16-02696-PHX-SRB, 2017 WL 6763548 (D. Ariz. Dec. 20, 2017) 22–23

In re Blackbaud, Inc., Customer Data Breach Litig.
567 F. Supp. 3d 667 (D.S.C. 2021) 24

In re Brinker Data Incident Litig.
2020 WL 691848 (M.D. Fla. Jan. 27, 2020) 19

In re Brinker
2021 WL 1405508 (M.D. Fla. Apr. 14, 2021) 22

In re Cap. One Consumer Data Sec. Breach Litig.
488 F. Supp. 3d 374 (E.D. Va. 2020) 23–24

In re Equifax, Inc., Customer Data Sec. Breach Litig.
362 F. Supp. 3d 1295 (N.D. Ga. 2019) 1–2

In re Equifax Inc. Customer Data Security Breach Litig.
999 F.3d 1247 (11th Cir. 2021) 19

In re Marriott Int'l, Inc., Customer Data Sec. Breach Litig.
No. 19-MD-2879, 2020 WL 6290670 (D. Md. Oct. 27, 2020) 23

In re Mednax Servs., Inc., Customer Data Sec. Breach Litig.
603 F. Supp. 3d 1183 (S.D. Fla. 2022) 25

In re Solara Medical Supplies, LLC Customer Data Security Breach Litig.
613 F.Supp.3d 1284, 1300 (S.D. Cal. 2020) 15

In re Premera Blue Cross Customer Data Sec. Breach Litig.
2019 WL 3410382 (D. Or. July 29, 2019) 22

In re Yahoo! Inc. Customer Data Sec. Breach Litig.
313 F. Supp. 3d 1113 (N.D. Cal. 2018) 24

In re Zappos.com, Inc.
888 F.3d 1020, 1027–28 (9th Cir. 2018) 4

Klem v. Wash. Mut. Bank
176 Wash. 2d 771, 295 P.3d 1179 (2013) 18

Krefting v. Kaye-Smith Enterprises Inc.
No. 2:23-CV-220, 2023 WL 4846850 (W.D. Wash. July 28, 2023) 22–23

Kuehn v. Stanley
91 P.3d 346 (Ariz. App. 2004) 13

Lady of Am. Franchise Corp. v. Arcese
2006 WL 8431025 (S.D. Fla. May 26, 2006) 19

Lujan v. Defs. of Wildlife
504 U.S. 555 (1992) 21

Mack v. Bristol-Myers Squibb Co.
673 So. 2d 100 (Fla. 1st DCA 1996) 19

Mackey v. Belden, Inc.
No. 4:21-CV-00149-JAR, 2021 WL 3363174 (E.D. Mo. Aug. 3, 2021) 23

Mason v. Mortgage Am., Inc.
114 Wash. 2d 842, 792 P.2d 142 (1990) 18

McMorris v. Carlos Lopez & Assocs., LLC
995 F.3d 295 (2d Cir. 2021) 4

Miccosukee Tribe of Indians of Fla. v. U.S.
516 F.3d 1235 (11th Cir. 2008) 1

Movie Prop Rentals, LLC, et al. v. The Kingdom of God Global Church, et al.
No. 22-cv-22594-BLOOM, 2023 WL 8275922 (S.D. Fla. Nov. 30, 2023) 2

Nails v. S & R, Inc.
334 Md. 398, 639 A.2d 660 (Md. Ct. App. 1994) 12

Nazar v. Harbor Freight Tools USA Inc.
No. 2:18-CV-00348-SMJ, 2020 WL 4741091 (E.D. Wash. Aug. 14, 2020) 18

Ombres v. City of Palm Beach Gardens
788 F. App'x 665 (11th Cir. 2019) 22

Panga v. Farmers Ins. Co. of Wash.
166 Wash. 2d 27, 204 P.3d 885 (2009) 17

Peery v. Hansen.
585 P.2d 574 (Ariz. App. 1978) 14

Purchnicki v. Envision Healthcare Corp.
439 F.Supp.3d 1226 (D. Nev. 2020), *affirmed* 845 F. App'x 613 (9th Cir. 2021) 25

Resnick v. AvMed, Inc.
693 F.3d 1317 (11th Cir. 2012) 4

Rich Morton's Glen Burnie Lincoln Mercury, LLC v. Williams-Moore
2023 WL 166277 (Md. App. Jan. 12, 2023) 12

Stallone v. Farmers Grp., Inc.
No. 221CV01659GMNVCF, 2022 WL 10091489 (D. Nev. Oct. 15, 2022) 25

Spokeo, Inc. v. Robins
578 U.S. 330 (2016) 2

TransUnion, LLC v. Ramirez
594 U.S. 413 (2021) 7

Tsao v. Captiva MVP Restaurant Partners
986 F.3d 1332 (11th Cir. 2021) 2, 3, 13

Warner v. Lerner
115 MD.APP. 428, 693 A.2d 394 (1997) 12

Wilding v. DNC Services Corp.
941 F.3d 1116 (11th Cir. 2019) 4

OTHER AUTHORITIES

15 U.S.C. § 45 11

Fed. R. Civ. P. 17(c) 16

Fed. R. Civ. P. 56 1

Fla. Sta. § 501.204 19

Md. Code, Health-Gen. § 4-301, *et seq.* 11–12

Md. Code, Com. Law § 13-301 10–11

Md. Code, Com. Law § 14-3503 11

Plaintiffs respectfully file this Response in Opposition to Defendants Mednax Inc., Mednax Services, Inc., Pediatrix Medical Group, and Pediatrix Medical Group of Kansas, P.C.'s (collectively "Mednax" or "Defendants") Motion for Summary Judgment ("Motion" or "Motion for Summary Judgment"). In support thereof, Plaintiffs state the following:

I. INTRODUCTION

Mednax does not dispute that a cyber hacker successfully gained access to several Mednax employees' user credentials (logins and passwords) for its employee Office365 accounts. Once the hacker(s) gained access to the first account, they sent additional phishing emails to other users within the Mednax network, prompting them to click on a malicious link in the email and enter their account credentials. Due to Mednax's failure to provide adequate cyber security of its network and training to its employees, cyber criminals were able to access the Personally Identifying Information (PII) and Protected Health Information (PHI) of the named Plaintiffs and nearly 2.7 million others within Mednax's network, including newborn babies and infants (the "Data Breach"). Mednax also does not dispute: (1) the hacker had unfettered access to that PII and PHI for several days, and (2) several Plaintiffs suffered fraud in the days and months following the unauthorized access of their PII and PHI.

In a complete distortion of the summary judgment standard, Mednax ignores the undisputed evidence of this major and preventable Data Breach and the reasonable inferences that this Court may draw from it (that the hacker used Plaintiffs' PII and PHI to perpetrate fraud against them or disseminated it for others to use). Rather, Mednax impermissibly asks this Court to conclude, based on Mednax's curated and restricted investigation, that there is no genuine issue of material fact that the fraud in this case resulted from Mednax's Data Breach. Mednax's Motion must be denied.

II. STANDARD OF REVIEW

To win on a summary judgment motion, Mednax must show "that [1.] there is no genuine dispute as to any material fact and [2.] [Mednax] is entitled to judgment as a matter of law." Fed. R. Civ. P. 56(a). In considering whether summary judgment is appropriate, "the judge's function is not himself to weigh the evidence and determine the truth of the matter but to determine whether there is a genuine issue for trial." *Edmondson v. Velvet Lifestyles, LLC*, 43 F.4th 1153, 1159 (11th Cir. 2022) (citing *Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 249 (1986)). A disputed fact "is 'material' if it would affect the outcome of the suit under the governing law, and 'genuine' if a reasonable trier of fact could return judgment for the non-moving party." *Miccosukee Tribe of Indians of Fla. v. U.S.*, 516 F.3d 1235, 1243 (11th Cir. 2008).

In order to prevail on a motion for summary judgment, the movant has the burden of proof to show that the evidence is *so one-sided* that, as a matter of law, a reasonable jury could not find for the nonmovant. *Anderson*, 477 U.S. at 251. To withstand summary judgment, the nonmovant need only show more than a scintilla of evidence in support of the nonmovant's position. *Id.* at 252. In assessing a motion for summary judgment, the Court must view the facts in the light most favorable to the nonmovant and draw all reasonable inferences in the nonmovant's favor." *Hutchins v. Frontier Airlines, Inc.*, No. 23-CV-80210-ROSENBERG, 2023 WL 7461324, at *2 (S.D. Fla. Oct. 13, 2023) (citing *Davis v. Williams*, 451 F.3d 759, 763 (11th Cir. 2006)). "'If more than one inference could be construed from the facts by a reasonable fact finder, and that inference introduces a genuine issue of material fact, then the district court should not grant summary judgment.'" *Movie Prop Rentals, LLC, et al. v. The Kingdom of God Global Church, et al.*, No. 22-cv-22594-BLOOM, 2023 WL 8275922, at *4 (S.D. Fla. Nov. 30, 2023) (quoting *Bannum v. City of Ft. Lauderdale*, 901 F.2d 989, 996 (11th Cir. 1990)).

III. ARGUMENT

Mednax makes several legal challenges to both Plaintiffs' Article III standing as well as elements of Plaintiffs' claims that are contrary to both state law and this Court's prior rulings. Plaintiffs' allegations (on which this Court concluded Plaintiffs' claims were plausibly stated and that Plaintiffs had standing to pursue them) are now fully borne out by the evidence. Therefore, Mednax's motion for summary judgment must be denied.

a. Plaintiffs Have Set Forth Sufficient Facts to Support Article III Standing.

To establish the prerequisites for Article III standing, a plaintiff must have "(1) suffered an injury in fact, (2) that is fairly traceable to the challenged conduct of the defendant, and (3) that is likely to be redressed by a favorable judicial decision." *Spokeo, Inc. v. Robins*, 578 U.S. 330, 338, (2016). The Eleventh Circuit is clear that the risk of future harm or identity theft is sufficiently concrete to establish injuries in fact when it is a "substantial risk" or "certainly impending." *Tsao v. Captiva MVP Restaurant Partners*, 986 F.3d 1332, 1339 (11th Cir. 2021); *In re Equifax Inc. Customer Data Security Breach Litig.*, 999 F.3d 1247, 1262-63 (11th Cir. 2021). The threat of future identity theft has been considered "certainly impending" or a "substantial risk" in cases where plaintiffs have alleged "actual misuse or actual access to personal data." *Tsao*, 986 F.3d at 1340; *In re Equifax Inc. Customer Data Security Breach Litig.*, 999 F.3d at 1263.

1. The Eleventh Circuit's Decision in *Green-Cooper v. Brinker International, Inc.* Does Not Affect This Court's Prior Holding that Actual Misuse or Access of Data is Sufficient to Satisfy Article III's Injury-in-Fact Requirement.

As they did at the motion to dismiss stage, Defendants continue to misinterpret data breach case law. This time, Defendants rely on a misinterpretation of newly decided *Green-Cooper v. Brinker International, Inc.* ("*Brinker*"), in contending a plaintiff must have suffered actual misuse to confer Article III standing and that unlawful access to PII/PHI is no longer sufficient. 73 F. 4th 883 (11th Cir. 2023). In *Brinker*, the Eleventh Circuit considered a definition for a payment card data breach class certified by the district court. Importantly, the Eleventh Circuit acknowledged the class was properly defined for standing purposes, as it limited the class to individuals who either experienced fraudulent charges as a result of the breach or had their payment card information appear on the dark web. *Id.* at 892. But turning to the question of predominance, the court expressed a limited concern that the language "accessed by cybercriminals" might be overbroad because it could include individuals who had their payment cards accessed in the breach but subsequently canceled them and, therefore, had no continuing risk of fraudulent misuse. *Id.*

The Eleventh Circuit has noted that in payment card data breaches, there is no risk of future injury to an individual who responds to the breach by canceling their card. *See Tsao v. Captiva MVP Rest. Partners, LLC*, 986 F.3d 1332, 1344 (11th Cir. 2021). In *Tsao*, the Eleventh Circuit contrasted payment care information from PII such as social security numbers, birth dates, and driver's license numbers. *Id.* at 1343 ("Tsao has not alleged that social security numbers, birth dates, or driver's license numbers were compromised in the [data] breach, and the card information allegedly accessed by the hackers "generally cannot be used alone to open unauthorized new accounts."). Unlike *Brinker* and *Tsao* where the plaintiffs could save themselves from the risk of future injury by canceling their cards, Plaintiffs and putative class members in this class cannot cancel or otherwise change their birth dates, Social Security numbers, or PHI. That information will remain immutable and be personally identifying for the rest of their lives, thus putting them at a continued risk of misuse of their personal information. Post *Brinker*, the threat of future identity theft can still be established by evidence of actual misuse or actual access to personal data where that data is of the type that cannot be subsequently altered or cancelled by the victim.

2. Plaintiffs Have Demonstrated Actual Misuse of Their Data That is Fairly Traceable to the Data Breach.

Defendants argue Plaintiffs cannot demonstrate traceability between the Data Breach and misuse of their PII and PHI.[1] In the context of Article III standing, however, the "fairly traceable" standard does not mean "certainly traceable." Thus, to satisfy Article III's standing causation requirement, a plaintiff need not show proximate causation. *Wilding v. DNC Services Corp.*, 941 F.3d 1116, 1125 (11th Cir. 2019). "[E]ven harms that flow indirectly from the action in question can be said to be 'fairly traceable' to that action for standing purposes." *Id.* (citing *Focus on the Family v. Pinellas Suncoast Transit Auth.*, 344 F.3d 1263, 1273 (11th Cir. 2003). In the data breach context, as this Court acknowledged in its Order Denying in part Defendants' Motion to Dismiss, "[e]ven if the data accessed in the Data Breaches did not provide all the information necessary to inflict [alleged] harms, they very well could have been enough to aid therein. And '[e]ven a showing that a plaintiff's injury is indirectly caused by a defendant's actions satisfies the fairly traceable requirement.'" [Doc. 104, p. 19 (quoting *Resnick v. AvMed, Inc.*, 693 F.3d 1317, 1324 (11th Cir. 2012))].

i. Plaintiffs' Social Security Numbers Were Found on the Dark Web.

It is undisputed that the Eleventh Circuit recognizes "that the exposure of personal information 'for theft and sale on the dark web . . . establishes both a present injury . . . and a substantial risk of future injury' for Article III standing." [Doc. 254, p. 6 (quoting *Brinker*, 73 F. 4th at 889–90)]. Mednax also does not appear to dispute that several of Plaintiffs' Social Security numbers or their minor children's Social Security numbers were found for sale on the deep and dark web. *Id.* Defendants contend, however, they did not have those Plaintiffs' Social Security numbers, so traceability does not exist. On that issue, there are genuine disputes of material fact precluding summary judgment.

The "evidence" Defendants cite to show they did not possess Plaintiffs' Social Security numbers was the result of a curated and purposefully incomplete investigation. Mednax improperly

[1] As this Court previously found: "[a]s to evidence that certain individuals' data affected by a given data breach has been misused, courts have found such evidence helpful in establishing a "substantial risk" of future harm for plaintiffs who remain unaffected. *See McMorris v. Carlos Lopez & Assocs., LLC*, 995 F.3d 295, 301–02 (2d Cir. 2021) (finding that courts have been more likely to conclude that plaintiffs have established a substantial risk of future injury where they can show that at least some part of the compromised dataset has been misused—even if plaintiffs' particular data subject to the same disclosure incident has not yet been affected); *In re Zappos.com, Inc.*, 888 F.3d 1020, 1027–28, n.7 (9th Cir. 2018) (explaining that although some plaintiffs in the suit had not yet suffered identity theft, allegations that other customers whose data was compromised had reported fraudulent charges helped establish that plaintiffs were at substantial risk of future harm."). [Doc. 104, p. 13].

[redacted]. [Doc. 282, Pl.s' SOMF ¶ 245]. [redacted] *Id.* [redacted]. *Id.* at ¶ 36; [Doc. 282, Pl.s' SOMF ¶ 7]. [redacted] [Doc. 282, Pl.s' SOMF ¶ 247]; *see, e.g.*, *Matthews Deposition*, pp. 113:15; 123:10-125:13; 128:21-130:7; 132:7-15; 142:12-143:21; 188:22-189:2;190:9-25, attached as Exhibit 1 (detailing [redacted] [Doc. 282, Pl.s' SOMF ¶ 245]. After obtaining credentials, the thief could access applications and systems across the network regardless of whether it was in the cloud or in the data center. *Frantz Initial Report*, ¶ 32, attached as Exhibit 2; *Frantz Deposition*, pp. 189:2–192:17, attached as Exhibit 3. [redacted] [Doc. 282, Pl.s' SOMF # 248].

[redacted]. [Doc. 282, Pl.s' SOMF ¶ 245]; Ex. 3, pp. 117:10-23, 119:2-11, 331:10-13, 332:20-333:11 ([redacted]). [redacted]. [Doc. 282, Pl.s' SOMF ¶ 249]. Considering that on summary judgment, the Court must view the record and inferences therefrom in a light most favorable to Plaintiffs and resolve reasonable doubts about the facts in favor of Plaintiffs, the Court must infer from the [redacted]

Further, [redacted] [Doc. 282, Pl.s' SOMF ¶ 239–241, 268]. [redacted]

[redacted] [Doc. 282, Pl.s' SOMF ¶ 241]. [redacted]. *Frantz Wojcieszek Rebuttal Report*, ¶ 27; attached as Exhibit 4; Ex. 2, ¶¶ 208, 227, 237 ("[redacted]").

Accordingly, given the circumstantial evidence, a jury could reasonably find that Mednax *did* have Plaintiffs' Social Security numbers. After all, Social Security numbers are generally provided to (and required by) healthcare providers.[2] [redacted].[3] [Doc. 282, Pl.s' SOMF ¶ 140]. Plaintiffs have certainly produced sufficient evidence, from which the Court must infer, that the presence of certain Plaintiffs' Social Security numbers on the dark web is fairly traceable to the Data Breach.

ii. Plaintiffs Have Produced Evidence of Spam Emails, Text Messages, and Phone Calls, as well as Evidence of Other Misuse of PII and PHI.

This Court has already found increased spam email, text messages, and phone calls to amount to "actual misuse" of data. *See* [Doc. 104, pp. 18–19]. Mednax does not appear to dispute that at least some Plaintiffs have produced evidence of increased spam after the unauthorized disclosure of their PII and PHI. Rather, Defendants contend the spam is not fairly traceable to the Data Breach because some of the email addresses, phone numbers, and addresses Plaintiffs allege to have received spam were not involved in the Data Breach and/or Mednax did not possess that information. Mednax similarly argues Plaintiff Neilsen's allegations, that twelve fraudulent accounts at Charles Schwab were

[2] For example, [redacted] *Cohen Deposition*, p. 92:20–22, attached as Exhibit 5.

[3] AA was wholly owned by Mednax before it was acquired by NAPA in May 2020, just two short months before the Data Breach. Most of the information that was attributable to AA at the time of the Data Breach, at one time belonged and was controlled by Mednax. After it was acquired, AA continued to do business and "partner" with Mednax. After the purchase of AA by NAPA, Mednax continued to be a Business Associate of AA as is applicable to HIPAA.

opened in her name after the Data Breach and fraudulent bills from AA, a Covered Entity to Mednax Business Associates, are not fairly traceable to the data breach.[4]

For the reasons described in section III.a.2.i, *supra*, there are genuine disputes of material fact regarding the scope of the Data Breach and the information that was involved. Further, "[e]ven if the data accessed in the Data Breaches did not provide all the information necessary to inflict [alleged] harms, they very well could have been enough to aid therein." [Doc. 104, p. 19]. Any argument Mednax asserts that the misuse of Plaintiffs' PII and PHI could have come from other sources is a clear dispute of fact and an issue for the jury to decide.

3. Plaintiffs Have Demonstrated Actual Access of Their PII/PHI Resulting in a Substantial Risk of Future Harm.

It is undisputed that "[o]n June 19, 2020, Mednax discovered that a thief gained access to certain Microsoft Office 365 Mednax business email accounts through a phishing attach beginning June 17, 2020. [Doc. 256, ¶ 5]. It is also undisputed that "[d]uring the investigation of the initial phishing activity, it was discovered that additional unauthorized access had occurred in other business email accounts at different points in time." *Id.* at ¶ 10. While Plaintiffs dispute the thoroughness of Mednax's post-breach investigation and have reason to believe the compromised PII and PHI is more significant than what was reported, as discussed above, *supra* section III.a.2.i, the Parties agree that *at* [redacted]." *Id.* at ¶ 12. The presence of Plaintiffs' Social Security numbers on the dark web only further confirms the thief had actual access to Plaintiffs' PII and PHI.

4. Plaintiffs Have Satisfied the Standard Set Forth in *TransUnion, LLC v. Ramirez* to Support Their Claim for Damages.

In addition to establishing a substantial risk of future harm, Plaintiffs have evidence of separate concrete harms that this Court already recognized would be sufficient to satisfy the U.S. Supreme Court's holding in *TransUnion, LLC v. Ramirez*, 594 U.S. 413, 437 (2021).[5] [Doc. 104, pp. 14–15].

---

[4] Plaintiff Neilsen testified that while she couldn't say with absolute certainty the address she provided to AA, she [redacted] *Neilsen Deposition*, 97:22, 98:1–8, attached as Exhibit 6. That information was used to open the Charles Schwab accounts. Plaintiff Neilsen further testified that she [redacted] *Id.* at 142:14–22, 143:1–4.

[5] Plaintiffs no longer assert a benefit of the bargain theory to support standing.

i. Plaintiffs Have Suffered Emotional Damages.

The record is clear that Plaintiffs have experienced emotional distress over the Data Breach. [Doc. 282, Pl.s' SOMF # 140 (citing *Bean* Deposition, p. 153:3-7, 154:3–15 ([redacted]); *Neilsen Deposition*, p. 110:1–11, 216:17–22 ([redacted]); *Clark Deposition*, p. 93:22–25, 94:1–22 ([redacted]); *B.W. Deposition*, p. 186:8–25, 187:1-23 ([redacted]); *Cohen Deposition*, p. 56:2–23 ([redacted] *Rumley Deposition*, p. 55:17–21 ([redacted] *Lee Deposition*, p. 191:4–23 (Lee [redacted]); *Jay Deposition*, p. 112:11–13, 112:15–17, 146:3–8 ([redacted]); *Larsen Deposition*, p. 110:2–6 ([redacted]

Defendants argues that the infants and toddlers affected by the Data Breach are not old enough to experience emotional distress, which defeats Plaintiffs' claims. But the adult Plaintiffs bring these claims on behalf of their minor children, as their representatives, and they have produced sufficient evidence of emotional distress as the caretakers of these minors. *Gonzalez-Gonzalez-Jimenez de Ruiz v U.S.*, 231 F.Supp.2d 1187, 1976 (M.D. Fla. 2002). To the extent the Court agrees that the affected infants and toddlers must have experienced emotional distress to prevail on this claim, Plaintiffs submit that the extent of the minors' emotional distress is a question of fact for the jury to decide.

ii. Plaintiffs Have Taken Reasonable Mitigating Measures to Protect Themselves Against Future Harm.

The record is clear that Plaintiffs have taken mitigation measures to protect themselves against future harm. [Doc. 282, Pl.s' SOMF ¶ 253 (citing *Bean Deposition*, p. 151:18-20, 152:18–25 (Bean testified she has taken mitigation measures by spending time monitoring her financial accounts and purchasing credit monitoring); *Neilsen Deposition*, p. 110:1–11, 149:9–18 (Neilsen testified she called

three credit bureaus to put a freeze fraud alert on her accounts and filed a police report); *Cohen Deposition*, p. 112:8–25 (Cohen testified she spent significant time emailing and calling various entities after the Data Breach to mitigate harm, time she could have been spending with her daughter); *Soto Deposition*, p. 74:3–24 (Soto testified he enrolled in credit monitoring services and placed a security freeze on his credit with Equifax after receiving notice of the Data Breach); *Larsen Deposition*, p. 108:19–25 (Larsen testified as a result of the Data Breach he has had to work with credit agencies to freeze his daughter's credit))]. Defendants do not appear to dispute Plaintiffs have developed evidence demonstrating mitigation measures have been taken, but instead repeat their argument that Plaintiffs have not shown misuse or access to personal data. For the reasons discussed above in section III.a.2.i, *supra*, Defendants are not entitled to summary judgment based on Mednax's cursory and unreliable investigation into the Data Breach.

iii. Plaintiffs Have Suffered a Diminution in Value of Their PII and PHI.

Defendants argue there is "no evidence to support Plaintiffs' assertion that their personal information has decreased in value." [Doc. 254, p. 14]. As noted by this Court, Plaintiffs need not "reduce their PHI or PII to terms of dollars and cents in some fictitious marketplace where they offer such information for sale to the highest bidder . . . . Rather, Plaintiffs' 'actual' (rather than 'hypothetical') diminution in value . . . occurred within the very marketplace in which they actually use their PHI and PII—the marketplace of credit, wherein the compromise of such information damages their ability to 'purchase goods and services remotely and without the need to pay in cash or a check[.]'" [Doc. 104, pp. 16–17] (citations omitted).

Plaintiffs have produced evidence demonstrating the value of PHI and PII, their role in the marketplace, and the effects of both being stolen. The permanent nature of PHI drives the monetary value and enables bad actors to perpetrate various types of fraud and illegal activities. [Doc. 282, Pl.s' SOMF ¶ 251]. PHI in particular is extremely valuable on the illegal market because, unlike a stolen credit card that can be easily canceled, the misuse of healthcare data is harder to identify and can be misused in many ways before any malicious activity is detected. [Doc. 282, Pl.s' SOMF ¶ 255]. A cybercriminal can sell PHI and PII on the dark web. [Doc. 282, Pl.s' SOMF ¶ 246]. The buyer can then resell the information to someone else. *Id.* The same "set" of PHI and PII can be sold and resold over and over again, thereby increasing its value. *Id.* These sales, of course, do not involve the rightful owner of the PHI and PII. *Olsen Report*, ¶ 59, attached as Exhibit 7. It is clear the very existence of PHI and PII on the Dark Web demonstrates that there is a market for the type of PHI and PII exposed by Mednax as a result of the Data Breach. *Id.* at ¶ 56.

As acknowledged by Defendants, Plaintiff Neilsen testified her participation in the marketplace of credit has directly been affected by the Data Breach. Specifically, she testified that after the Data Breach, she experienced a reduction in her credit score. [Doc. 282, Pl.s' SOMF ¶ 257]. After the Data Breach, Plaintiff Neilsen received notice that her account at [redacted] [Doc. 282, Pl.s' SOMF ¶ 258]. Plaintiff Neilsen established that she did not [redacted]. [Doc. 282, Pl.s' SOMF ¶ 249]. Nevertheless, the debt collection agency appeared on her credit score when she tried financing for a home. *Id.*

iv. Plaintiffs Have Suffered a Loss of Privacy.

Defendants do not appear to dispute Plaintiffs have established evidence they have suffered a loss of privacy – Plaintiffs clearly have. [Doc. 282, Pl.s' SOMF ¶ 260 (citing *Bean Deposition*, p. 150:14–16, 151:11–13 (Bean testified it has been stressful to have her newborn's private, sensitive information no longer private, and rather exposed to the world since nearly the day he was born); *Neilsen Deposition*, p. 258:1–18 (Neilsen testified she experienced stress after losing control over her private information); *B.W. Deposition*, p. 187:1–23 (B.W. testified as a result of the Data Breach she does not know who has access to her private information, who is able to use it and how it is going to be used); *Cohen Deposition*, p. 107:7–25, 108:1–2 (Cohen testified she has experienced anxiety because her daughter's sensitive, private information should be confidential and "shouldn't be for everyone to see); *Lee Deposition*, p. 191:4–23 (Lee testified he has concerns for the loss of his privacy, specifically not knowing what has his private information and what they are doing with it))]. Once again, Defendants narrow their argument to maintaining Plaintiffs have not established unauthorized access or misuse of their PII and PHI. For the reasons discussed above in section III.a.2.i, *supra*, this Court must find Plaintiffs have demonstrated standing.

b. The Facts Show that Defendants Violated State Statutory Laws.

1. Evidence exists that Mednax violated the Maryland Consumer Protection Act

The Maryland Consumer Protection Act ("MCPA") is a crucial piece of legislation designed to safeguard consumers, such as Plaintiff Cohen and the class members she represents, from unfair and deceptive trade practices. "The MCPA defines unfair or deceptive practices to include both misrepresentations, § 13-301(1), and material omissions, § 13-301(3)." *Clark v. Bank of America, N.A.*, 561 F. Supp. 3d 542, 557 (D. Md. 2021). In order to prevail on her MCPA claim, Plaintiff Cohen must show (1) misrepresentation/omission, (2) reliance, and (3) causation and injury. *Ayers v. Ocwen Loan*

Servicing, LLC, 129 F. Supp. 3d 249, 270 (D. Md. 2015). Mednax makes improper arguments in an attempt to attack all three elements of Plaintiff Cohen's MCPA claim.

First, Mednax claims that Plaintiff Cohen cannot establish that Mednax engaged in an unfair or deceptive practice or made a misrepresentation or omission because Cohen testified that she could not recall Mednax making any representations about its data security. [Doc. 254, p. 16]. A false or misleading representation that "has the capacity, tendency, or effect of deceiving or misleading consumers" is an "unfair, abusive, or deceptive trade practice." Md. Code, Com. Law § 13-301(1). To establish a misrepresentation, plaintiff need not prove that the defendant intended to mislead the plaintiff, but rather that the representation was objectively misleading to a reasonable, but unsophisticated, consumer. *Allen v. Bank of Am., N.A.*, 933 F. Supp. 2d 716, 730 (D. Md. 2013). Similarly, an omission is material "if a significant number of unsophisticated consumers would find that information important" such that the information would likely affect their decision to use said good or service. *Bank of Am., N.A. v. Jill P. Mitchell Living Trust*, 822 F. Supp. 2d 505, 532 (D. Md. 2011). Although Mednax's clinicians may not have expressly stated in detail to Plaintiff Cohen Mednax's cyber security promises (which would be a rather difficult and odd conversation to have while treating a patient), Maryland laws and Mednax's own privacy policy are sufficient evidence of Mednax's misrepresentations.

Mednax need not make explicit promises and privacy guarantees to each patient that walks through their doors. Many patients arrive at their facilities during medical emergencies—not feeling well, having been injured, in the middle of active labor, etc. Rather than concerning themselves with the minutiae of Mednax's data security practices, patients have a reasonable expectation that, as a medical facility, Mednax is in compliance with federal and state privacy laws unless informed otherwise. Mednax tells consumers in its public facing "Privacy Notice" that they are "**required by law to maintain the privacy of your health information** ("Protected Health Information" or "PHI") and to provide you with Notice of our legal duties and privacy practices with respect to your PHI." [Doc. 115, ¶ 297 (citing *Notice of Privacy Practices*, Mednax, https://www.pediatrix.com/notice-of-privacy-practices/ (last visited Jan. 5, 2021)]. These laws include HIPAA, HITECH, the Federal Trade Commission ("FTC") Act (15 U.S.C. § 45), Maryland's Personal Information Protection Act (Md. Code, Com. Law § 14-3503), and Maryland's Confidentiality of Medical Records Act (Md. Code, Health-Gen. § 4-301, *et seq.*)[6] *See also* [Doc. 115, ¶¶ 332–360, 481]. In its Privacy Notice, Mednax

[6] Maryland courts have recognized that the purpose of the Confidentiality of Records Act is to "provide for the confidentiality of medical records, to establish clear and certain rules for the

further represents that, "[w]hen 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.* Given Mednax's Privacy Policy and its promise to comply with federal and state laws, Mednax was under a duty to disclose pertinent information to its patients regarding its known failures to provide adequate cyber security measures necessary to protect Plaintiffs' and the Class Members PII/PHI.

Next, Defendants argue that Cohen cannot show she relied on Mednax's misrepresentations and omissions. Under Maryland law, Plaintiff Cohen does not need to show that "but-for" Defendants' misrepresentations and omissions, she would not have entrusted Defendants with her PII/PHI. *Bank of Am., N.A.*, 822 F. Supp. 2d at 532. Rather, Cohen establishes this element in showing that Defendants misrepresentations "substantially induced" her choice. *Id.* In that same vein, Cohen can establish reliance on a material omission by showing that it is substantially likely that she would not have entrusted Defendants with her PHI/PII had they disclosed the omitted information. *Id.* at 535. "Whether a misrepresentation [or omission] substantially induces a consumer's choice is ordinarily a question of fact for the trier of fact." *Id.* at 532–35. The amount of evidence necessary to show that a factfinder could reasonably conclude that an alleged misrepresentation substantially induces a consumer's choice is relatively low. *Id.* at 532 (citing *Nails v. S & R, Inc.*, 334 Md. 398, 639 A.2d 660, 669–70 (Md. Ct. App. 1994)).[7]

---

disclosure of medical records, and generally to bolster the privacy rights of patients." *Warner v. Lerner*, 115 MD.APP. 428, 693 A.2d 394 (1997). A "medical record" is defined as any "oral, written, or other transmission in any form or medium of information that…identifies or can be readily associated with the identity of a patient or recipient." Md. Code, Health-Gen. § 4-301(g)(1). Mednax cannot dispute that its conduct is governed by this act. Mednax further cannot dispute that every reasonable (even unsophisticated) patient of Mednax's, including Cohen, is free, indeed encouraged, to rely upon the fact that Mednax is legally providing medical services in Maryland and is, therefore, in compliance with its laws, including laws protecting general personal data as well as specific medical data of the kind collected by Mednax. Without such reliance, no reasonable person would turn over their private health information to Mednax's care. *Rich Morton's Glen Burnie Lincoln Mercury, LLC v. Williams-Moore*, 2023 WL 166277, at * 12 (Md. App. Jan. 12, 2023).

[7] As discussed in *Bank of Am., N.A.*, the Maryland Court of Appeals in *Nails v. S&R., Inc.* rejected the lower courts' requirement that a claimant must show but-for reliance to claim state a claim for fraud. *Bank of Am., N.A.*, 822 F. Supp. 2d at 532. In *Nails*, the plaintiffs testified that their employer promised to pay them 5% commission. *Id.* However, the employer failed to inform them that it would deduct 15% from their gross receipts prior to paying the 5% commission. The plaintiffs testified that "they did not know whether they would have taken the job had then known about the 15% commission." *Id.* The Maryland Court of Appeal overturned the lower courts' decision, finding sufficient evidence to show "substantial inducement" because (1) the plaintiffs did not receive a "substantial" sum of money because of the 15% deduction, and (2) the plaintiffs testified that the amount they expected to be paid was of the "utmost importance." *Id.* at 532–33.

Here, information regarding Defendants' failure to protect and keep confidential Plaintiffs' PII/PHI would have substantially induced the decision of unsophisticated patients, like Plaintiff Cohen, to entrust Defendants with their PII/PHI. During her deposition, Plaintiff Cohen testified that Defendants' failure to safeguard her daughter's PII and PHI "can ruin her life" and "nobody should be getting that [information] except for her parents." Ex. 5, p. 70:7–21. Defendants' arguments as to the proximity of the facility and Cohen's choice to seek t[redacted]. Similarly, [redacted] Cohen's evidence of reliance, because choosing another facility at this point is arguably moot, since Mednax already has stored (and has not proven that it has destroyed) A.H.'s PII/PHI.

Finally, Defendants argue that Cohen has not produced evidence of actual injury. Plaintiff Cohen has presented evidence that Mednax's inadequate data security omissions caused her injury in the form of emotional stress and several hours of lost time mitigating the effects of the data breach. [Doc. 282, Pl.s' SOMF ¶¶ 252–53]. These are measurable and compensable injuries. *Tsao*, 986 F.3d at 1344.

Thus, Plaintiffs have presented evidence supporting all three elements of their MCPA claim precluding summary judgment on this claim.

2. Plaintiff Larsen Has Established A Genuine Issue of Material Fact as to His Arizona Consumer Fraud Act Claim.

Mednax only attacks the misrepresentation and reliance elements of Plaintiff Larsen's Arizona Consumer Fraud Act ("ACFA") claim. Mednax does not address Plaintiffs' evidence of Mednax's inadequate data security and privacy measures and its omission, suppression and concealment of this material information from Plaintiffs. These material omissions are sufficient to support an ACFA claim. *Garner v. Medicis Pharmaceutical Corp.*, 2023 WL 6295052 at *2 (D. Ariz. Sept. 27, 2023) ("A material omission can support an ACFA claim").

"While reliance on a material omission is necessary, **it need not be reasonable**." *Id.* (emphasis added) (distinguishing Mednax's cited authority, *Kuehn v. Stanley*, 91 P.3d 346, 352 (Ariz. App. 2004)). Mednax's reliance argument mischaracterizes Plaintiff Larsen's deposition testimony and ignores his reasonable expectation that Mednax would comply with its data-security duties under statutory and common law. Accurately stated, Larsen testified that: in researching Pediatrix, he never saw any reviews of data security such as would put him on notice of the material omissions; he did not recall

if Defendant made any affirmative representations regarding data security, encryption or storage; and, he continued to use Pediatrix after the Data Breach, not because the omissions were immaterial, but because his daughter was in the middle of painful and daunting medical treatments, and he did not want to further traumatize her by switching providers. [Doc. 282, Pl.s' SOMF ¶ 277]. Larsen's testimony establishes that Mednax's disclosures about its inadequate data security were nonexistent or, at the very least, not memorable, clear and conspicuous to consumers.

Moreover, as stated above, Defendants have duties under federal and state laws to protect Plaintiffs' PII/PHI. Section III.b.1, *supra*. Based on Defendants' Notice of Privacy Policy and tits requirements under law, Plaintiffs reasonably believed that Defendants would protect and keep their PII/PHI confidential. Defendants owed a duty to disclose to Plaintiffs their cybersecurity was inadequate.

Finally, Mednax provides no authority supporting its footnoted argument that disgorgement is not an available remedy. The lone case it cites – *Peery v. Hansen*, 585 P.2d 574 (Ariz. App. 1978) – does not address this remedy. Instead, the Arizona Appellate Court in *Peery* notes that the ACFA was enacted out of the "necessity for broadened private remedies in the consumer protection field." *Id.* at 577. To that end, if the fact finder credits Plaintiffs' evidence that Mednax profited from its inadequate data security, Mednax should be made to disgorge those profits.

Thus, Plaintiffs have presented evidence of Larsen's reliance, precluding summary judgment on their ACFA claim.

3. Plaintiff Rumely Has Established that Genuine Issues of Material Fact Exist as to His California Consumer Records Act Claim.

Plaintiff Rumely has clearly raised genuine issues of material fact in his California Consumer Records Act ("CCRA") claim as to the issues of Defendant's delay harming Plaintiff Rumely and the California Class. [redacted] [Doc. 282, Pl.s' SOMF ¶ 232]. [redacted] [Doc. 282, Pl.s' SOMF ¶ 233]. Indeed, this evidence clearly raises a genuine issue of material fact as to whether that Defendant's delay in notifying customers and this must be decided by a trier of fact. As such, Plaintiff Rumely has established that genuine issues of material fact exist as to his CCRA claim. Therefore, Defendant's Motion should be denied.

Genuine issues of material fact exist regarding Plaintiff Rumely's California Consumer Records Act ("CCRA") claim The CCRA "regulates businesses with regard to treatment and notification procedures related to their customers' personal information." *In re Solara Medical Supplies, LLC Customer Data Security Breach Litigation*, 613 F.Supp.3d 1284, 1300 (S.D. Cal. 2020) (quoting *Corona v. Sony Pictures Ent'mt*, No. 14-CV-09600 RGK, 2015 WL 3916744 at *6 (C.D. Cal. June 15, 2015)). "The statute requires that disclosure shall be made in the most expedient time possible without unreasonable delay." *Id.* (quoting Cal. Civ. Code § 1798.82(a). Defendants would have the Court believe that Plaintiff Rumely has alleged no injuries at all let alone ones associated with the excessive and unreasonable delay.

Mednax waited almost six months (over 180 days) to send its patients notice of the Data Breach. Such a delay is in violation of Mednax's obligations under HIPAA as well as [redacted] Specifically, [redacted] [Doc. 282, Pl.s' SOMF ¶ 232]. [redacted]. [Doc. 282, Pl.s' SOMF ¶ 233]. Indeed, this evidence clearly raises a genuine issue of material fact as to whether Defendant's delay in notifying patients and this must be decided by a trier of fact. As such, Plaintiff Rumely has established that genuine issues of material fact exist as to his CCRA claim. Therefore, Defendant's Motion should be denied.

Further, Defendant would have the Court believe Plaintiff Rumley testified that he suffered no injury which is blatantly wrong and mischaracterizes the evidence. Plaintiff Rumely brought this case on behalf of his children, H.R. and M.R. [Doc. 282, Pl.s' SOMF ¶ 234]. He stands in the shoes of his children and believes that they have been irrevocably harmed as a result of the breach. [Doc. 282, Pl.s' SOMF ¶ 235]. In order to protect his children from some of the effects of the breach Plaintiff Rumely purchased Norton Life Lock and monitored accounts. [Doc. 282, Pl.s' SOMF ¶ 237]. Mr. Rumely purchased Norton Life Lock because the notice of the Data Breach he received from Mednax

[8] This 60-day notice requirement is also part of the obligations for notice pursuant to the HIPAA statute 45 C.F.R. § 164.404. The notice to the effected patients should be given within that time even all the details are not yet known in full. Supplemental notice can always be given as more details become clear. This requirement is so that, as early as possible, patients can take steps to mitigate the harm they suffer because of the disclosure. Despite knowing that it suffered a massive Data Breach which effected millions of patients, Mednax waited six months to let its patients know about the breach.

was vague. *Id.* Further, Mr. Rumely claimed that he experienced an uptick in phishing and spam emails following the date of the actual breach. *Rumely Deposition*, p. 98:4–99:8, attached as Exhibit 8. Mr. Rumely claims that this delay led to the harm and increased risk of harm as he could have gotten Norton Life Lock sooner or have taken other steps to protect himself and his children from the harms caused by the Data Breach. [Doc 115, ¶¶ 513, 517].

The evidence is in conflict over these facts of the case and therefore the issue is for a jury to decide. Defendant's Motion for Summary Judgment on Plaintiff Runely's CCRA claim should, therefore, be denied.

4. Plaintiff Rumely Has Established that Genuine Issues of Material Fact Exist as to His CMIA Claim.

Defendant again attempts to impose in its own standard of review for summary judgment by mischaracterizing the *Ambry* court's ruling and claiming that "[t]o survive summary judgment, '[a] plaintiff must [prove] that a defendant's negligence resulted in unauthorized or wrongful access to the information, i.e., that the information was improperly viewed or otherwise accessed.'" [Doc. 252, p. 19]. First, as detailed *infra*, the burden is upon the moving party to demonstrate facts underlying all legal questions raised by the pleadings are not in dispute. *See Herzog*, 193 F.3d 1241, 1246 (11th Cir. 1999). A genuine issue of material fact exists "if the evidence is such that a reasonable jury could return a verdict for the nonmoving party." *Anderson*, 106 S.Ct. 2505 at 248. Moreover, the Court must also view the facts 'in the light most favorable to the non-moving party on each motion. *See Chavez v. Mercantil Commercebank*, 701 F.3d 896, 899 (11th Cir. 2012).

Mednax is not entitled to summary judgment on Plaintiff Rumely's CMIA claim for two reasons: (1) Plaintiff Rumely unequivocally alleges in the operative Complaint and his deposition that he is bringing claims on behalf of his minor children; and (2) Mednax is unable to carry its burden in showing that no genuine issue of material fact exists.

Mednax's first argument, that the CMIA claim fails because it is only brought on behalf of Plaintiff Rumely, falls flat on its face when examined against the allegations of the Second Amended Complaint and the deposition testimony of Plaintiff Rumely. As alleged in the Complaint, Plaintiff Rumely received a Notice of Data Security Event from Mednax dated December 16, 2020, notifying him that his minor children's PII/PHI was compromised in the Data Breach. [Doc. 115, ¶ 41]. One of the only avenues for Plaintiff Rumely's minor children to pursue their data breach claims against Mednax was through a parent represented by counsel. *See Garcia v. City of Fresno*, No. 116CV01340LJOSAB, 2017 WL 6383814, at *4 (E.D. Cal. Dec. 14, 2017); *see also* Fed. R. Civ. P. 17(c).

Therefore, "Michael Rumley, as legal guardian of minor children whose initials are H.R. and M.R." brought claims against Mednax "on behalf of H.R. and M.R." as stated multiple times in the operative Complaint. [Doc. 115, ¶¶ 41–58]. There would be no need to mention Plaintiff Rumley's minor children in the Complaint if he was not bringing claims on their behalf. Furthermore, and as Mednax recognizes, Mr. Rumely testified pointblank in his deposition that he is *not* bringing claims on behalf of himself—but on behalf of his children. [Doc. 252, p. 19]. As stated above, Mr. Rumely is bringing the case on behalf of his children. [Doc. 282, Pl.s' SOMF ¶ 234]. *See also*, [Doc. 115, ¶¶ 41–58]. There is not dispute that his children's information was included in this breach as he received a notice letter from Defendant telling him so. *[Doc. 282, Pl.s' SOMF* ¶ 238]. It cannot be any clearer. Plaintiff Rumely is asserting claims on behalf of his children, not himself, and Mednax is not entitled to summary judgment on this account.

Mednax's second argument, that Plaintiff Rumely's CMIA claim fails because he has "zero evidence" to prove that his children's PHI and PHI were viewed by an unauthorized third-party, must be denied because Mednax [redacted]. As Plaintiff's Expert Mary Frantz identified in her report, [redacted]. *See supra*, Section III.a.2.i. The full scope will never be known because of Mednax's actions post Breach, but a reasonable jury could find that had Mednax [redacted]

However, even with Mednax's self-serving limitations in place, Plaintiff Rumely still proffers evidence that demonstrates a genuine issue of material fact exists. [redacted] [Doc. 282, Pl.s' SOMF ¶ 239]. [redacted] Ex. 4, ¶ 27; Ex. 2, ¶¶ 208, 227, 237. That breach is the Mednax breach as there was no other correlation between the searched names.

5. Plaintiff Jay Has Established that Genuine Issues of Material Fact Exist as to Her WCPA Claim.

To establish a "deceptive" act under the Washington Consumer Protection Act ("WCPA"), the plaintiff must show that the defendants' act or conduct "had the capacity to deceive a substantial portion of the public." *Gray v. Amazon.com, Inc.*, 653 F. Supp. 3d 847, 858 (W.D. Wa. 2023) (quoting *Panga v. Farmers Ins. Co. of Wash.*, 166 Wash. 2d 27, 47, 50, 204 P.3d 885 (2009). An act may be unfair

without being deceptive. *Klem v. Wash. Mut. Bank*, 176 Wash. 2d 771, 786, 295 P.3d 1179 (2013). "To prevail on such a theory, the plaintiff must establish that the act or practice "causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and is not outweighed by countervailing benefits [to consumers or to competition]."' *Gray*, 653 F. Supp. 3d at 858 (quoting *Alpert v. Nationstar Mortg. LLC*, No. 15-cv-1164, 2019 WL 1200541, at *6 (W.D. Wash. Mar. 14, 2019)).

Defendants mispresent the evidence in this case in stating that Plaintiff Jay cannot prevail on his WCPA claim. The mountain of evidence pointing to the fact that Mednax engaged in unfair or deceptive acts and practices is most prominently seen in the breach itself. Moreover, as stated above, Section III.b.1, *supra*, Defendants have duties under federal and state laws to protect Plaintiffs' PII/PHI; Defendants' made promises under their Notice of Privacy Policy and their requirements under law, to protect and keep confidential Plaintiffs' PII/PHI; and Defendants had a duty to disclose to Plaintiffs their inadequate cybersecurity system.

Contrary to Defendants' assertions, "[t]he injury element will be met if the consumer's property interest or money is diminished because of the unlawful conduct even if the expenses caused by the statutory violation are minimal." *Mason v. Mortgage Am., Inc.*, 114 Wash. 2d 842, 792 P.2d 142, 148 (1990) Here, Plaintiffs have sufficient evidence to show [redacted] Ex. 2 (Exhibit E), and, thus, his property has lost significant value due the lost value, [Doc. 282, Pl.s' SOMF ¶ 244].

Defendants claim that Plaintiff Jay cannot establish the causation element because she testified that Mednax's cybersecurity did not [redacted] [Doc. 252, p. 23]. But "Washington courts apply a rebuttable presumption that the plaintiff relied on the defendant's representations concerning the product, so as to avoid putting the plaintiff in the 'impossible position' of proving 'they believed the opposite of the omitted fact.'" *Nazar v. Harbor Freight Tools USA Inc.*, No. 2:18-CV-00348-SMJ, 2020 WL 4741091, at *3 (E.D. Wash. Aug. 14, 2020) (quoting *Deegan v. Windermere Real Estate / Ctr.-Isle, Inc.*, 197 Wash. App. 875, 391 P.3d 582, 587 (2017)). However, in her deposition, Plaintiff Jay was discussing her use of [redacted] *Jay Deposition*, pp. 171:24–172:12, attached as Exhibit 9. This is not enough to rebut Plaintiffs' presumption that, had she known that her children's [redacted] she would not have gone to a Mednax facility.

6. There are Genuine Issues of Facts as to Whether Mednax Violated the Florida Deceptive and Unfair Trade Practices Act.

Mednax argues there is no evidence to support a claim that it engaged in "unfair methods of competition, unconscionable acts or practices, and unfair or deceptive acts or practices in the conduct of any trade or commerce," in violation of the Florida Deceptive and Unfair Trade Practices Act ("FDUTPA"). [Doc. 252, p. 24 (quoting Fla. Sta. § 501.204(1))]. But Mednax's business practice of maintaining inadequate data security *itself* violates the FDUTPA, regardless of the misrepresentations and omissions that were made to its patients. *See*, *e.g.*, *Burrows v. Purchasing Power, LLC*, No. 1:120CV022800-UU, 2012 WL 9391827, at *6 (S.D. Fla. Oct. 18, 2012) (holding inadequate data security is an unfair trade practice for FDUTPA purposes); *see also Farmer v. Humana, Inc.*, 582 F. Supp. 3d 1176, 1190 (M.D. Fla. 2022) (citing *Burrows*); *In re Brinker Data Incident Litig.*, 2020 WL 691848, at *12 (M.D. Fla. Jan. 27, 2020) (same).

Moreover, courts have been instructed "that when deciding whether a particular conduct violates FDUTPA[,] to look to whether the FTC Act and federal courts find such conduct to be an unfair method of competition or an unconscionable, unfair, or deceptive act or practice under the FTC Act." *Lady of Am. Franchise Corp. v. Arcese*, 2006 WL 8431025, at *8 (S.D. Fla. May 26, 2006) (citing *Mack v. Bristol-Myers Squibb Co.*, 673 So. 2d 100, 104-05 (Fla. 1st DCA 1996)). Courts have determined that the failure to maintain reasonable and appropriate data security for sensitive personal information violates the FTC Act. *See*, *e.g.*, *F.T.C. v. Wyndham Worldwide Corp.*, 799 F.3d 236, 247 (3d Cir. 2015) (finding that lax cybersecurity resulting in a data breach falls within the meaning of "unfair" under the FTCA); *In re Equifax, Inc., Customer Data Sec. Breach Litig.*, 362 F. Supp. 3d 1295, 1327 (N.D. Ga. 2019) ("The failure to maintain reasonable and appropriate data security for consumers' sensitive personal information can constitute an unfair method of competition in commerce in violation of the Federal Trade Commission Act.").

Additionally, as stated above, Section III.b.1, *supra*, Defendants have duties under federal and state laws to protect Plaintiffs' PII/PHI; Defendants' made promises under its Notice of Privacy Policy and their requirements under law, to protect and keep confidential Plaintiffs' PII/PHI; and Defendants had a duty to disclose to Plaintiffs their inadequate cybersecurity system. As discussed in Section III.a.2.i, *supra*, there are genuine issues of material fact as to whether Mednax's failure to properly secure its data systems was a proximate cause of the Data Breach. Its argument that it did not engage in an unfair, unconscionable, or deceptive act within the meaning of FDUTPA must therefore be rejected.

Mednax's argument that Plaintiffs have not shown evidence warranting injunctive relief also fails. There is no dispute of fact that Plaintiffs' PII and PHI remain in Mednax's possession, and there is a material dispute of fact as to whether it is sufficiently protected. [redacted]." [Doc. 525, p. 24]. However, [redacted] [Doc. 282, Pl.s' SOMF ¶ 218]. [redacted].

Indeed, as Plaintiffs' expert Mary Frantz concluded, Mednax has still not sufficiently mitigated the risk. [redacted]." [Doc. 282, Pl.s' SOMF ¶ 261]. [redacted]." *Id.* ¶ 262. [redacted] (*id.* ¶¶ 261); [redacted] (*id.* ¶ 263); [redacted] (*id.* ¶ 264); (3) [redacted] (*id.* ¶ 266); [redacted]" (*id.*). Because material questions exist about the extent to which Plaintiffs' and class members' PII and PHI is still at risk while it remains in Mednax's possession, Mednax is not entitled to summary judgment on Plaintiffs' claim for injunctive relief under FDUTPA.

c. There are Genuine Issues of Material Fact as to Plaintiffs' Negligence Claims.

1. Plaintiffs' Negligence Claims Are Governed by Florida Law.

Despite this Court's correct application of Florida law to Plaintiffs' negligence claims at the motion to dismiss stage [Doc. 104, pp. 6–8], Mednax plucks a single sentence from the Eleventh

Circuit's ruling in *Brinker* and uses it for the proposition that Plaintiffs' negligence must be governed by the laws of the jurisdiction in which each Plaintiff received medical treatment. This is inaccurate.

Nothing in *Brinker* can fairly be read to suggest that, under the Eleventh Circuits decision, the Court must reassess its choice-of-law analysis. Rather, in the *Brinker* case, the Eleventh Circuit did not disturb the part of the district court's order certifying a nationwide negligence class. At the district court level, the parties disagreed whether Texas law or Florida law governed the negligence claim, but the district court noted that, either way, under the "most substantial relationship" test, only one state's law would apply, "so that claim is not a concern for manageability or predominance." *In re Brinker*, 2021 WL 1405508, at *11 (M.D. Fla. Apr. 14, 2021) (citing other data breach cases certifying nationwide negligence claims). The Eleventh Circuit did not instruct the court to reassess its predominance analysis on the basis that each putative class members' claims would be governed by the laws of their home states, which it surely would have done if it believed their injuries occurred only where they experienced the misuse of their data.

Rather, the portion of *Brinker*, on which Defendants improperly rely, discusses establishing a concrete injury for purposes of Article III standing. 73 F.4th at 889. In making this determination, the Eleventh Circuit was merely restating previously determined factors from *Lujan v. Defs. of Wildlife,* 504 U.S. 555, 560–61 (1992). *Id.* (reiterating old case law requiring "misuse of the data cybercriminals acquire from a data breach because such misuse constitutes both a 'present' injury and a 'substantial risk' of harm in the future."). Mednax argues that the *Brinker* decision impacts the first element of the "most significant relationship" test—"the place where the injury occurred." [Doc. 254, pp. 25–26]. However, the standing requirements from the *Brinker* analysis was already used prior to this Court's Order Denying in part Defendants' Motion to Dismiss [Doc. 104].

Moreover, *Brinker*'s opinion on standing does not affect this Court's choice-of-law analysis. In determining that Florida law will apply, this Court noted the difficulties in conducting an analysis with a cloud-basis system and decided to join other courts in finding that the location of the breach itself is fortuitous in data breach cases. [Doc. 104, pp. 7–8]. This Court noted that multiple Defendants are domiciled in Florida and Defendants' security protocols allegedly broke down in Florida. [redacted] *Cox Deposition*, pp. 34:14–35:12, attached as Exhibit 10 ([redacted] This was the hub [redacted] *See, e.g.*, *id.* at 10:19–14:10. [redacted]

[redacted] [Doc. 254, p. 26]. However, as a result of the Data Breach, Plaintiffs have suffered actual and imminent injuries including [redacted]. *Supra*, section III.a.2.i. Injuries as a result of information being sold on the Dark Web produces the same issues as cloud-based storage systems. Yet, these injuries resulted from Mednax's failures to maintain a proper cyber security system—these failures occurring in Florida. Given the challenges presented with internet systems, it's clear that the place where the conduct causing injuries occurred and the Defendants' domiciliary should govern the choice-of-law analysis in this case (as the Court has previously opined). [Doc. 104, pp. 7–8]. The existing choice-of-law analysis correctly governs Plaintiffs' negligence claims under Florida law.[9]

2. Mednax Had a Duty to Protect Plaintiffs' PII/PHI.

Mednax relies on outdated (and outlier) case law to argue that it has no duty to protect the PII/PHI of Plaintiffs Larsen, B.W. Bean, Baum Nielsen, Jay, and Cohen. First, contrary to Mednax's assertion, Plaintiffs' negligence claims are governed by Florida law. *See* Section III.c.1, *supra.* In this Circuit,

> Where a defendant's conduct creates a foreseeable zone of risk, the law generally will recognize a duty placed upon defendant either to lessen the risk or see that sufficient precautions are taken to protect others from the harm that the risk poses.

Ombres v. City of Palm Beach Gardens, 788 F. App'x 665, 667 (11th Cir. 2019) (internal citations omitted). Given the results of prior penetration tests, and Mednax's understanding of the value of PII/PHI, the Data Breach—and Plaintiffs' subsequent harms as a result thereof—were reasonably foreseeable. Ex. 2, ¶¶ 50–203.

Second, even were Plaintiffs' negligence claims governed by the laws of their resident states, legal authority overwhelmingly demonstrates that Mednax has a duty to protect Plaintiffs' PII/PHI. *See Krefting v. Kaye-Smith Enterprises Inc.*, No. 2:23-CV-220, 2023 WL 4846850, at *5 (W.D. Wash. July 28, 2023) (recognizing duty to protect PII under Washington law since defendant's acts "exposed [plaintiff] to a high risk of harm thereby creating a duty"); *Buckley v. Santander Consumer USA, Inc.*, No. C17-5813 BHS, 2018 WL 1532671, at *5 (W.D. Wash. Mar. 29, 2018) (same); *In re Banner Health Data*

[9] Regardless of the choice-of-law, this Court should find, as the district court did in *In re Brinker* and as other courts have in other data breach actions, that "under non-identical state negligence laws, '[t]his case does not implicate any of the state-specific issues that can sometimes creep into the negligence analysis.'" *In re Premera Blue Cross Customer Data Sec. Breach Litig.*, 2019 WL 3410382, at *18 n.6 (D. Or. July 29, 2019 (quoting *In re Anthem, Inc. Data Breach Litig.*, 327 F.R.D. 299, 312 (N.D. Cal. 2018).

Breach Litig., No. CV-16-02696-PHX-SRB, 2017 WL 6763548, at *8 (D. Ariz. Dec. 20, 2017) (applying Arizona law and recognizing duty to protect patient information sufficient to state a negligence claim); *Carr v. Oklahoma Student Loan Auth.*, No. CIV-23-99-R, 2023 WL 6929850, at *2 (W.D. Okla. Oct. 19, 2023) (Defendant, who allegedly had no prior relationship with the named plaintiffs, "owed a duty to Plaintiffs to act reasonably in safeguarding the Plaintiffs' PII" under Oklahoma law); *In re Cap. One Consumer Data Sec. Breach Litig.*, 488 F. Supp. 3d 374, 400–01 (E.D. Va. 2020) (holding that a duty to protect exists in data breach case based on the "voluntary undertaking doctrine under Virginia law"); *Baldwin v. Nat'l W. Life Ins. Co.*, No. 2:21-CV-04066-WJE, 2021 WL 4206736, at *3-4 (W.D. Mo. Sept. 15, 2021) (finding negligence claim sufficiently pled under Missouri law on behalf of data breach victims and thereby finding duty to protect PII); *Krefting*, 2023 WL 4846850, at *5 (recognizing duty to protect PII under Washington law since defendant's acts "exposed [plaintiff] to a high risk of harm thereby creating a duty"); *Buckley v. Santander Consumer USA, Inc.*, No. C17-5813 BHS, 2018 WL 1532671, at *5 (W.D. Wash. Mar. 29, 2018) (same); *In re Marriott Int'l, Inc., Customer Data Sec. Breach Litig.*, No. 19-MD-2879, 2020 WL 6290670, at *6-7 (D. Md. Oct. 27, 2020) (holding that defendant had a duty to protect customers' PII under Maryland law). Mednax also had duties to protect Plaintiffs' PII/PHI under HIPAA, HITECH, the FTC Act, and various state laws.

Mednax further asserts that the opinions of Plaintiffs' expert Mary Frantz are Plaintiffs' only evidence that Mednax failed to satisfy its duty to protect Plaintiffs' PII/PHI. Yet, [redacted]).

3. Plaintiffs' Claims Are Not Barred by the Economic Loss Rule.

Mednax argues that the economic loss doctrine precludes negligence claims for Plaintiffs Rumely, B.W., Clark, Lee, Nielsen, and Soto. Again, Mednax is wrong. Regardless of the governing state law, the economic loss rule does *not* preclude a negligence claim in the context of a data breach. *See, e.g.*, *Mackey v. Belden, Inc.*, No. 4:21-CV-00149-JAR, 2021 WL 3363174, at *7–8 (E.D. Mo. Aug. 3, 2021) (finding that economic loss doctrine does not bar negligence claim in data breach case under

Missouri law); *In re Yahoo! Inc. Customer Data Sec. Breach Litig.*, 313 F. Supp. 3d 1113, 1132–33 (N.D. Cal. 2018) (holding that economic loss rule does not apply in data breach case under California law); *In re Cap. One Consumer Data Sec. Breach Litig.*, 488 F. Supp. 3d 374, 401 (E.D. Va. 2020) (economic loss rule does not bar negligence claim in data breach case under Virginia law since defendant "voluntarily undertook a duty to protect its customers' PII"); *id.* at 397 (doctrine would not apply to a data breach case under Texas law); *In re Blackbaud, Inc., Customer Data Breach Litig.*, 567 F. Supp. 3d 667, 680–82 (D.S.C. 2021) (finding negligence claim is viable in data breach cases under South Carolina law as defendant plausibly created the risk).

4. Plaintiffs Have More Than a Scintilla of Evidence to Establish Damages.

Plaintiffs have sufficient evidence of their injury and damages resulting from the Data Breach. *Huynh v. Quora, Inc.*, 508 F. Supp. 3d 633, 653–54 (N.D. Cal. 2020). As stated above, despite Defendants ineffective investigation, Plaintiffs have sufficient circumstantial evidence to show that their PII/PHI was accessed and exfiltrated as a result of the Data Breach. Section III.a.2.i, *supra*. This evidence includes [redacted]. [Doc. 282, Pl.s' SOMF ¶ 239–41].

In *In re 21st Century Oncology*, the Middle District of Florida set out a three-pronged test to determine whether plaintiffs have suffered an injury in fact based on an increased risk of identity theft following a data breach: (1) the motive of the unauthorized third-party who took the information; (2) the type of information seized; and (3) whether the information has been accessed or misused. *Id.* at 1255. As this Court noted in its ruling on Defendants' Motion to Dismiss: evidence showing that Plaintiffs information has been offered for sale on the "Dark Net" is sufficient to show that Plaintiffs' data has been accessed and misused. [Doc. 104, pp. 52–52].[10]

i. Evidence that Plaintiffs' PII/PHI was Improperly Disclosed and Is Being Sold on the Dark Web.

Plaintiffs produced sufficient evidence showing that their PHI and PII has been accessed and exfiltrated from Mednax's network, and has ended up for sale on the Dark Web. [redacted]

[10] [redacted] [Doc. 258, pp. 16–17].

[redacted]. [Doc. 282, Pl.s' SOMF ¶ 239–41] [redacted]. [Doc. 282, Pl.s' SOMF ¶ 251]. [redacted] Net, there is substantial evidence that the victims of the Mednax Data Breach have suffered from an improper disclosure of their PHI and PII.

ii. Plaintiffs' Mitigation of Costs and Damages.

Plaintiffs' out-of-pocket expenses and mitigation costs are clearly damages caused by Mednax's negligence, and Plaintiffs are entitled to compensation. Federal courts, including this Court, have held Plaintiffs are entitled to recover out of pocket expenses and mitigation costs in the event of a Data Breach. *In re Mednax Servs., Inc., Customer Data Sec. Breach Litig.*, 603 F. Supp. 3d 1183, 1203–04 (S.D. Fla. 2022); *Stallone v. Farmers Grp., Inc.*, No. 221CV01659GMNVCF, 2022 WL 10091489, at *7 (D. Nev. Oct. 15, 2022); *Purchnicki v. Envision Healthcare Corp.*, 439 F.Supp.3d 1226, 1244 (D. Nev. 2020), *affirmed* 845 F. App'x 613 (9th Cir. 2021); *Green v. eBay Inc.*, No. CIV.A. 14-1688, 2015 WL 2066531, at *5 (E.D. La. May 4, 2015). Plaintiffs only need to show that the mitigation and out of pocket expenses are reasonable, necessary, and that the alleged harm is imminent. *Griffey v. Magellan Health Inc.*, 562 F. Supp. 3d 34, 47 (D. Ariz. 2021).

As noted above, Plaintiffs' PII and PHI, including the PII and PHI of children born in 2019 and 2020, are currently being offered for sale to criminals on the Dark Net. [Doc. 282, Pl.s' SOMF ¶ 271]. Further, [redacted] Ex. 2, ¶¶ 238–252. [redacted] *Id.* at ¶ 239(a). [redacted] *Id.* at ¶ 239(b), (d). [redacted] *Id.* at ¶ 239(c). [redacted]

[redacted]. *Id.* at ¶ 252. [redacted] *Id.* at ¶ 12(b). Plaintiffs have no reason to believe that Mednax's lax data security has been, or will be, corrected going forward. As such, Plaintiffs must take and fund their own mitigation of Mednax's negligence and bad acts.

5. There Exists a Genuine Issue of Material Fact as to Causation.

Again, Defendants attempt to evade liability by pointing to their limited investigation and the possibility that Plaintiffs have been victims of other data breaches. However, Plaintiffs have established sufficient evidence to show a causal connection between the Mednax Data Breach and Plaintiffs injuries.

Defendants attempt to rely on their insufficient review of the Data Breach to establish "conclusively" that Mednax did not have Plaintiffs' PII/PHI saved on its network. [redacted]). Ex. 3, pp. 288:14–17, 325:15–326:2

As this Court is aware, many of the parties harmed by Defendants' negligent behavior are children ranging in age from newborn infants to five (5) year old children. Unlike data breaches involving adults who are active on the internet and whose information is subject to risk due to their online presence, the PII and PHI of children as young as one (1) month old have been found for sale on the Dark Net by Plaintiffs' counsel. [Doc. 282, Pl.s' SOMF ¶ 268].Children's data and health data are considered high value data by cybercriminals due to its greater ease of use and the length of time the data may be used without detection as opposed to an adult's PII or PHI. [Doc. 282, Pl.s' SOMF ¶ 269]. The fact that a one (1) month old child's PII and/or PHI is for sale on the Dark Web is highly likely to persuade a jury that Mednax's negligence and failure to properly secure and protect Plaintiffs PII and PHI is the cause of Plaintiffs' damages.

6. Conclusion

Plaintiffs have uncovered ample evidence showing: 1) Plaintiffs' PHI and PII are available for purchase on the Dark Web; 2) said PHI and PII was information provided by Plaintiffs to Mednax; 3) Plaintiffs have suffered mitigation damages as well as having fraudulent bank accounts and subscriptions opened in their names; 4) it is likely (if not obvious in the case of certain named Plaintiffs) that the source of Plaintiffs' damages is the Mednax Data Breach; and 5) that Plaintiffs

either show care in protecting their data or are too young to have their data widely disseminated. Summary judgment can only be given if there is no genuine dispute as to any material fact. *Id.* Mednax has woefully failed to meet this burden and, as such, its Motion for Summary Judgment must be denied.

IV. CONCLUSION

Plaintiffs have established sufficient evidence to create a genuine issue of material fact as to (1) Article III standing, (2) violations of state statutes, and (3) negligence. Mednax intentionally overlooks, omits, and misstates Plaintiffs' supporting evidence in an attempt to avoid liability and its duties under the law. As such, Defendants' Motion for Summary Judgment must be denied.

Respectfully submitted,

/s/ William B. Federman

William B. Federman (admitted *pro hac vice*)
FEDERMAN & SHERWOOD
10205 N. Pennsylvania Ave.
Oklahoma City, Oklahoma 73120
Telephone: (405) 235-1560
Facsimile: (405) 239-2112
Email: wbf@federmanlaw.com

Maureen M. Brady (admitted *pro hac vice*)
MCSHANE & BRADY, LLC
1656 Washington Street, Suite 120
Kansas City, MO 64108
Telephone: (816) 888-8010
Facsimile: (816) 332-6295
E-mail: mbrady@mcshanebradylaw.com

Co-Lead Counsel for Plaintiffs and the Proposed Classes

CERTIFICATE OF CONFERENCE

I hereby certify that on December 28, 2023, counsel for the movant has conferred with all parties and non-parties who may be affected by the relief sought in the underlying Motion in a good faith effort to resolve the issues raised in the motion and have been unable to do so.

/s/ William B. Federman

William B. Federman

CERTIFICATE OF SERVICE

I hereby certify that on December 28, 2023, I electronically filed the foregoing document with the Clerk of the Court using the CM/ECF system, which will send notice of electronic filing to all counsel of record.

/s/ William B. Federman
William B. Federman