**UNITED STATES DISTRICT COURT**
**SOUTHERN DISTRICT OF FLORIDA**

**CASE NO. 21-MD-02994-RAR**

In re:

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

**MEDNAX INC.; MEDNAX SERVICES, INC.; PEDIATRIX MEDICAL GROUP; AND PEDIATRIX MEDICAL GROUP OF KANSAS, P.C.'s MOTION FOR SUMMARY JUDGMENT AND MEMORANDUM OF LAW IN SUPPORT**

# TABLE OF CONTENTS

# TABLE OF AUTHORITIES

**Page(s)**

**CASES**

**RULES**



**STATUTES**

**OTHER AUTHORITIES**

Pursuant to Rule 56 of the Federal Rules of Civil Procedure, Defendants Mednax Inc., Mednax Services, Inc.,[1] Pediatrix Medical Group,[2] and Pediatrix Medical Group of Kansas, P.C. (collectively, "Mednax") move for summary judgment as to Plaintiffs' Consolidated Second Amended Complaint for Damages (ECF No. 115 ("Complaint" or "SAC")).

## I. INTRODUCTION

This Court allowed Plaintiffs' claims to proceed to discovery based on their *allegations* that they had suffered harm, and were now facing an imminent risk of future harm, because certain of their personally identifiable information ("PII") and protected health information ("PHI") was involved in a phishing attack disclosed by Mednax in December 2020 (the "Cyberattack"). With the benefit of discovery, it has become clear that these allegations were false. It has now been nearly three years since the Cyberattack was disclosed, and over three and a half years since it was remediated, and none of the Plaintiffs has a single shred of evidence that they have suffered ***any*** legally cognizable harm that is fairly traceable to the Cyberattack.

In fact, discovery has demonstrated that there is absolutely no evidence that any of the named Plaintiffs' PII or PHI was accessed or viewed by the threat actor that perpetrated the Cyberattack. Nor is there any evidence that the threat actor stole any of their PII or PHI. But Plaintiffs' inability to prove their case does not stop there. Discovery has also confirmed that all of the allegations of misuse that Plaintiffs alleged in the Complaint could not have been caused by the Cyberattack because they required information that was not included in the files that were involved in the Cyberattack and, in some instances, required information that Mednax did not have anywhere in its computer systems. Thus, to the extent this misuse occurred, discovery has confirmed that it could not have resulted from the Cyberattack.[3]

These undisputed facts preclude Plaintiffs from presenting their claims to a jury. As discussed below, the evidence developed in discovery confirms that no Plaintiff has Article III

[1] Effective as of July 1, 2022, Mednax Inc. changed its name to Pediatrix Medical Group, Inc., and Mednax Services, Inc. changed its name to PMG Services, Inc. For consistency with the Complaint, this Statement uses the entities' previous names.

[2] "Pediatrix Medical Group" is named as a Defendant in several of the individual actions that were consolidated into this MDL but it is not a legal entity.

[3] [redacted]

standing and their claims must be dismissed for that reason. Mednax is also entitled to summary judgment on each of Plaintiffs' remaining substantive claims.

## II. STANDARD OF REVIEW

Summary judgment is appropriate if the pleadings, depositions, answers to interrogatories, and admissions on file, together with any declarations show there is no genuine issue as to any material fact and that the moving party is entitled to judgment as a matter of law. Fed. R. Civ. P. 56(c); *Celotex Corp. v. Catrett*, 477 U.S. 317, 322 (1986); *Kerr v. McDonald's Corp*., 427 F.3d 947, 951 (11th Cir. 2005). If the party seeking summary judgment identifies grounds that show the absence of a genuine issue of material fact, the burden then shifts to the non-moving party, who must go beyond the pleadings and present affirmative evidence to show that a genuine issue of material fact exists. *Porter v. Ray*, 461 F.3d 1315, 1320 (11th Cir. 2006). "[M]ere conclusions and unsupported factual allegations are legally insufficient to defeat a summary judgment motion." *Ellis v. England*, 432 F.3d 1321, 1325-26 (11th Cir. 2005).

## III. ARGUMENT

### A. Plaintiffs Lack Article III Standing.

Standing is "the threshold question in every federal case, determining the power of the court to entertain the suit." *Warth v. Seldin*, 422 U.S. 490, 498 (1975); *CAMP Legal Def. Fund, Inc. v. City of Atlanta*, 451 F.3d 1257, 1269 (11th Cir. 2006). One of the bedrock principles of Article III standing is that plaintiff must have suffered an injury. To satisfy Article III, an injury must be "concrete, particularized, and actual or imminent; fairly traceable to the challenged action; and redressable by a favorable ruling." *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 409 (2013) (quoting *Monsanto Co. v. Geertson Seed Farms*, 561 U.S. 139, 149 (2010)).

In its Order Granting in Part Defendants' Motion to Dismiss (hereinafter, the "Motion to Dismiss Order"), this Court found that Plaintiffs adequately alleged standing to sue for injunctive relief because they "allege both actual misuse and actual access of their personal data resulting from the Data Breaches." ECF No. 104 at 14. This Court also found that Plaintiffs had adequately alleged standing to sue for damages by claiming that they "suffer[ed] emotional distress related to possible identity theft and the cost of the increased time Plaintiffs have spent and must continue to spend reviewing their financial information." *Id.* At the summary judgment stage, however, Plaintiffs can no longer rest on mere allegations. Rather, they must "set forth by affidavit or other evidence specific facts." *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 561 (1992) (citations omitted).

As discussed below, the undisputed record evidence demonstrates that Plaintiffs lack Article III standing because no Plaintiff has suffered a legally cognizable injury that is fairly traceable to Mednax's conduct.

**1. No Plaintiff Has Any Evidence Their Data Was Actually Accessed In The Cyberattack.**

In its Motion to Dismiss Order, this Court suggested that ***either*** "actual misuse ***or*** access of . . . data" was sufficient to satisfy Article III's injury-in-fact requirement. ECF No. 104 at 12 (emphasis added). However, in *Green-Cooper v. Brinker International, Inc.*, which was issued after this Court's Motion to Dismiss Order, the Eleventh Circuit clarified that actual access alone is insufficient to confer Article III standing. 73 F.4th 883, 892 (11th Cir. 2023) (vacating and remanding grant of class certification and recognizing that "the class definitions as they now stand may include uninjured individuals . . . who have simply had their data accessed by cybercriminals"). Instead, the Eleventh Circuit held that "a plaintiff whose personal information is subject to a data breach can establish a concrete injury for purposes of Article III standing if, as a result of the breach, he experiences 'misuse' of his data in some way." *Id.* at 889 (citing *Tsao v. Captiva MVP Rest. Partners, LLC*, 986 F.3d 1332, 1343 (11th Cir. 2021)).

Post-*Green Cooper,* actual access alone is insufficient to satisfy Article III's injury-in-fact requirement. But even if this Court reaches a contrary conclusion, there is no evidence that any Plaintiff's data was actually accessed in the Cyberattack. Mednax retained an industry leading, independent third party to conduct a thorough investigation into the Cyberattack, which concluded that [redacted] Defendants' Joint Statement of Material Facts ("SOMF") ¶ 11. As the corporate representative of Charles River Associates (the forensic investigator Mednax retained to investigate the Cyberattack) explained during his deposition, as is often the case in forensic investigations, [redacted][4] *Id.* For this reason, and in an abundance of caution, Mednax notified all

[4] Mednax's investigation [redacted]. SOMF ¶ 12. But the source files that resulted in each of the Plaintiffs receiving notice of the Cyberattack [redacted] SOMF ¶ 16 & Ex. 18 (Ellman Rep.) ¶ 27.

individuals whose [redacted] *Id.* ¶ 18 & Ex. 5 (Miller Dep. Tr. at 194:7-24). Thus, [redacted] *Id.* Plaintiffs offer no evidence of actual access, meaning that this basis for Article III standing is not only legally unavailable, it is also without evidentiary support. Plaintiffs thus must prove actual misuse of their data to establish standing, something they have not done, as set forth more fully below.

**2. No Plaintiff Can Demonstrate Actual Misuse Of Their Data That Is Fairly Traceable To The Cyberattack.**

The Eleventh Circuit recently held that, to satisfy Article III's injury-in-fact requirement in a data breach case, a plaintiff must show that, "as a result of the breach, he experiences 'misuse' of his data in some way." *Green-Cooper*, 73 F.4th at 889. In addition, to satisfy Article III's fair traceability requirement, there must be "a causal connection between the injury and the conduct complained of" that is "not . . . th[e] result [of] the independent action of some third party not before the court." *Lujan*, 504 U.S. at 560-61. In the data breach context, this means that Plaintiffs must offer evidence that shows "a specific connection between the breach and the type of data used" to cause an actual harm. *Greenstein v. Noble Reciprocal Exch.*, 585 F. Supp. 3d 1220, 1231 (N.D. Cal. 2022); *see also McCombs v. Delta Grp. Elecs., Inc.*, --- F. Supp. 3d ---, 2023 WL 3934666, at *6 (D.N.M. June 9, 2023) (no fair traceability where plaintiff "has not provided a nexus between the data breach and the listed unwanted communications," in part because "[s]he does not allege that her contact information (e.g., phone number, e-mail address) were included in the data breach"); *Blood v. Labette Cnty. Med. Ctr.*, 2022 WL 11745549, at *6 (D. Kan. Oct. 20, 2022) (no fair traceability where data elements required to cause harm were not stolen); *cf. Green-Cooper*, 73 F.4th at 890 (alleged injuries not fairly traceable to data breach involving payment cards used at Chili's restaurant where named plaintiffs visited outside of the period that "*that* Chili's was compromised in the data breach").

As discussed below, six Plaintiffs do not even contend that their personal information (or their children's personal information) was misused in any way. And for all of the Plaintiffs who claim some misuse of their personal information, discovery has demonstrated that there is no causal connection between that misuse and the Cyberattack. Accordingly, all Plaintiffs lack Article III standing, and summary judgment must be granted in Mednax's favor.

***i. There Is No Evidence That Plaintiffs Bean, Jay, Soto, Baum, Clark, And Larsen's Personal Information (Or Their Children's Personal Information) Has Been Misused.***

Bean asserts claims only on behalf of her child, SOMF ¶ 59, and there is no evidence that Bean's child's personal information was actually accessed and then misused as a result of the Cyberattack. Bean did not allege any misuse of her child's personal information in the Complaint, [redacted], and testified at her deposition that [redacted]. *See id.* ¶¶ 67-68.

Jay, Soto, Baum, and Clark initially alleged that their children's Social Security numbers have been found for sale on the deep and dark web as a result of the Cyberattack, and Larsen made the same allegation about his own Social Security number.[5] SAC ¶¶ 88, 111, 136, 273, 162. However, Plaintiffs withdrew these allegations "[b]ased upon evidence developed through subsequent discovery," and are no longer contending in this litigation that their Social Security numbers were involved in the Cyberattack. ECF No. 222 at 1. Even if these Plaintiffs had not withdrawn these allegations, any alleged presence of their Social Security numbers on the dark web would not be fairly traceable to the Cyberattack because neither their Social Security numbers nor their children's Social Security numbers were involved in the Cyberattack at all, nor were they even in Mednax's possession.[6] SOMF ¶¶ 73, 93, 106, 119, 193, 195; ECF No. 84-1. Jay, Soto, Baum, and Clark, make no other assertions of actual misuse of their children's PII or PHI, and Larsen makes no other assertions of actual misuse of his own PII or PHI, nor was there any evidence of actual misuse of produced in discovery. Accordingly, these Plaintiffs cannot show that there is actual "misuse" of their personal information, or their children's personal information, as required to establish Article III standing. *Green-Cooper*, 73 F.4th at 889.

---

[5] [redacted] *See* SOMF ¶¶ 71, 91, 104, 117, 189.

[6] [redacted] SOMF ¶ 195. [redacted] *id.* ¶ 189, none of Clark's alleged harms are fairly traceable to Mednax.

### *ii. The Alleged Presence Of Some Plaintiffs' Social Security Numbers On The Dark Web Is Not Fairly Traceable To Mednax.*[7]

Five Plaintiffs—A.W., B.W., Larsen (on behalf of his child, A.L.), Lee, and Cohen (on behalf of her child, A.H.)—contend that their Social Security numbers or their children's Social Security numbers were found for sale on the deep and dark web.[8] The Eleventh Circuit has held 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. *Green-Cooper*, 73 F.4th at 889-90. Here, however, the undisputed record evidence confirms that, to the extent these Plaintiffs' Social Security numbers have been found for sale on the deep and dark web at all, their presence on the dark web is not fairly traceable to the Cyberattack for two reasons.

***First***, Mednax did not even have A.W., B.W., A.L., Lee, or A.H's Social Security numbers in its possession at all. Kathleen O'Hara, Mednax's Vice President, Medical Coding, searched Mednax's patient information databases and concluded that none of those patient information databases contained the Social Security numbers for any these individuals. *See, e.g.*, SOMF ¶ 24, 25, 121, 162, 179; ECF No. 84-1. And documentation produced in discovery further confirmed that Mednax does not have any of these individuals' Social Security numbers in any of its patient information systems. Specifically:

- A.W.'s Social Security number is blank or is listed as 999-99-9999 in each of the places it appears in Mednax's patient information systems. SOMF ¶ 24.
- B.W.'s Social Security number is either blank or, in one place, includes only the last four digits. SOMF ¶ 25.
- A.L.'s Social Security number is listed as 999-99-9999 in each of the places it appears in Mednax's patient information systems. SOMF ¶ 121.

---

[7] [redacted] SOMF ¶ 199.

[8] This evidence is unreliable for the reasons set forth in Defendants' Motion to Exclude Expert Testimony of Gary Olsen and Mary Frantz filed concurrently herewith. For that additional reason, Plaintiffs have not established standing. Even accepting the unreliable evidence, however, Plaintiffs cannot show that the alleged presence of their Social Security numbers on the deep and dark web is fairly traceable to Mednax for the reasons set forth herein.

- Lee was a patient of American Anesthesiology. "[T]he archived copy of the MedSuite system" that contains information about patients of American Anesthesiology "does not contain a Social Security number for Gerald Lee." SOMF ¶¶ 156, 162; ECF No. 84-1 ¶¶ 5, 13.
- A.H.'s Social Security number is listed in 999-99-9999 in each of the places it appears in Mednax's patient information systems. SOMF ¶ 179.

Because Mednax did not have any of these individual's Social Security numbers in any of its computer systems, it is impossible for these individual's Social Security numbers to have been posted on the deep and dark web as a result of the Cyberattack. That alleged injury is not fairly traceable to Mednax's conduct and cannot create Article III standing for any Plaintiff. *Greenstein*, 585 F. Supp. 3d at 1231 (filing of fraudulent application for employment benefits was not fairly traceable to data breach because there was no "specific connection between the breach and the type of data used in the application" and because "it is possible the data used for the fraudulent application could have been obtained from a third-party or unrelated data breach"); *McCombs*, 2023 WL 3934666, at *6; *Antman v. Uber Techs., Inc.*, 2018 WL 2151231, at *10 (N.D. Cal. May 10, 2018) (fraudulent credit card application requiring Social Security number was not fairly traceable to disclosure of plaintiff's name, driver's license information, bank account, and routing number).

***Second***, there is no evidence that A.W., B.W., A.L., Lee, or A.H.'s Social Security numbers were involved in the Cyberattack. [redacted] SOMF ¶¶ 21, 22, 118, 119, 158, 176, 177.[9] [redacted] *Id.* Moreover, none of the underlying source files pertaining to these named Plaintiffs that were potentially involved in the Cyberattack included their Social Security numbers. *Id.* ¶¶ 23, 120, 161, 178. Thus, because these individuals' Social Security numbers were not among the information that the threat actor even potentially could have accessed in the Cyberattack, the

[9] B.W. alleges in the Complaint that her Social Security number was found on the deep and dark web, but the notice letter that she produced in this litigation [redacted] SOMF ¶ 21. If her Social Security number would have been involved, the notice letter would have expressly stated that. *See id.* ¶ 22 & Ex. 21 (template notice letter for individuals with SSN impacted).

alleged presence of these Social Security numbers on the deep and dark web is not fairly traceable to the Cyberattack.

***iii. Plaintiffs Rumely, Lee, And Nielsen's Alleged Spam Emails, Text Messages, And Phone Calls Do Not Create Article III Standing.***

Plaintiffs Rumely, Lee, and Nielsen's assertion that they received spam emails and text messages also does not qualify as an injury-in-fact that is fairly traceable to the Cyberattack. As a gating matter, this Court did not decide in its Motion to Dismiss Order whether spam emails and text messages constitute a legally cognizable injury-in-fact. Courts have repeatedly rejected this argument for standing. *See, e.g.*, *Cherny v. Emigrant Bank*, 604 F. Supp. 2d 605, 609 (S.D.N.Y. 2009) ("The receipt of spam by itself . . . does not constitute a sufficient injury entitling [the plaintiff] to compensable relief."); *Jackson v. Loews Hotels, Inc.*, 2019 U.S. Dist. LEXIS 124525, at *4 (C.D. Cal. July 24, 2019) ("[R]eceiving spam or mass mail does not constitute an injury."); *McCombs*, 2023 WL 3934666, at *6 (collecting authorities). Thus, Plaintiffs cannot establish federal jurisdiction by pointing to alleged injuries caused by the mere receipt of spam emails, mail, phone calls, and text messages. Even if they could, however, they still cannot establish Article III standing on the record here because none of the spam that they received is fairly traceable to Mednax. *See Greenstein*, 585 F. Supp. 3d at 1231 (to establish fair traceability, a plaintiff must show "a specific connection between the breach and the type of data used" to cause the alleged harm).

- Rumely contends that, as a result of the Cyberattack, he "experienced an uptick in phishing emails." SAC ¶ 49. When asked to produce in discovery all of the phishing emails he contends he received as a result of the Cyberattack, [redacted].[10] That email address was not included in the source files pertaining to Rumely's child that were potentially involved in the Cyberattack. SOMF ¶ 56. Moreover, though Rumely alleges in the Complaint that this email address "is the same email address he provided to his children's healthcare provider," specifically the hospital, "who contracted with Defendant Mednax," SAC ¶ 50, Mednax never possessed Rumely's email address at all. SOMF ¶ 57. Thus, these alleged phishing emails

[10] Though Rumely alleges in the Complaint that "[b]ut for the [Cyberattack], Plaintiff Rumely's email address would be difficult to locate," SAC ¶ 50, discovery has demonstrated that the email address [redacted] was compromised in 14 other data Cyberattacks since 2016, including 9 that pre-date the Cyberattack. SOMF ¶ 58.

could not have resulted from the Cyberattack and are not fairly traceable to Mednax. *Blood*, 2022 WL 11745549, at *6 ("[A]n increase in spam phone, texts, and emails calls [sic], while certainly frustrating, cannot be causally linked to the specific data breach here because there is . . . no allegation that phone numbers or email addresses were stolen.").

- Lee also claims that he has experienced an increase in spam calls and text messages as a result of the Cyberattack. SAC ¶¶ 233-34. The evidence produced in discovery, however, confirms that Lee's telephone number and email address were not involved in the Cyberattack. SOMF ¶ 161. Thus, Lee's alleged spam calls and text messages could not have resulted from, and are not fairly traceable to, the Cyberattack. Instead, they likely resulted from [redacted]. *See* SOMF ¶ 166. [redacted] *Id.* ¶ 160. Lee cannot rely on unsubstantiated allegations to demonstrate that he has Article III standing at the summary judgment stage. *Hall v. Sunjoy Indus. Grp., Inc.*, 764 F. Supp. 2d 1297, 1304 (M.D. Fla. 2011) ("unsubstantiated, conclusory allegations are insufficient to survive summary judgment.") (citation omitted).
- Nielsen asserts that she has received spam emails, phone calls, and mail, including an unwanted subscription to *Shape* magazine. SAC ¶¶ 207-08. Any spam emails that Nielsen received, however, cannot be fairly traceable to the Cyberattack because discovery has shown that Nielsen's email address was not included in the files that were potentially involved in the Cyberattack, and she testified at her deposition that [redacted]. SOMF ¶¶ 133, 140. The spam mail that Nielsen contends she received as a result of the Cyberattack is also not fairly traceable to the Cyberattack. [redacted] *Id.* ¶ 133 & Ex. 53. [redacted]. *Id.* ¶¶ 137-38. [redacted]. *Id.* ¶ 133 & Ex. 53, 142. Finally, though Nielsen alleged that she experienced an increase in spam phone calls, she failed to produce any documentation in discovery to substantiate this allegation. She therefore cannot use these unsubstantiated

allegations to create a triable issue of fact sufficient to survive summary judgment, particularly in light of [redacted] *Sunjoy Indus. Grp.*, 764 F. Supp. 2d at 1304; *see also Rollins v. TechSouth, Inc.*, 833 F.2d 1525, 1529 (11th Cir. 1987) ("Unsubstantiated assertions alone are not enough to withstand a motion for summary judgment."); *Larach v. Std. Chartered Bank Int'l (Ams.) Ltd.*, 2011 U.S. Dist. LEXIS 163670, at *39-40 (S.D. Fla. June 7, 2011) (rejecting "Plaintiffs attempt to create a dispute of fact with flatly unsubstantiated . . . facts" and granting summary judgment in defendant's favor), *R&R adopted*, 2011 U.S. Dist. LEXIS 163672 (S.D. Fla. Sept. 15, 2011).

***iv. Nielsen's Other Allegations Of Misuse Are Also Insufficient.***

Nielsen's other allegations of misuse fare no better. She asserts that, as a result of the Cyberattack, twelve bank accounts at Charles Schwab were opened in her maiden name ([redacted] without her authorization, that her credit score allegedly decreased, and that she was forced to pay $81.47 to American Anesthesiology for a charge that her insurance had already paid. SAC ¶¶ 201, 205, 206. None of these alleged injuries is fairly traceable to the Cyberattack.

[redacted] *Id.* ¶ 134. [redacted] *See, e.g.*, *id.* ¶ 141. Nielsen also testified at her deposition that [redacted] *Id.* ¶¶ 134, 136. [redacted] *Id.* ¶ 141. Moreover, opening a bank account with Charles Schwab requires a Social Security number. See https://onboard.schwab.com/retail/personal-info (last visited Nov. 28, 2023) (asking new brokerage account customers to provide their Social Security number and noting that "[a]ll brokerage firms require this information for new account applicants to comply with IRS regulations and the USA PATRIOT Act"); FINRA, Rule 6840 ("Each Industry Member shall submit to the Central Repository the Firm Designated ID, the Transformed Value for individual tax payer identification number ('ITIN')/social security number ('SSN') . . ."); 31 C.F.R. § 1020.220(a)(2)(i)(A)(4)(i) (requiring banks to implement a written Customer Identification Program that includes obtaining a taxpayer identification number for a U.S. person opening a bank account). Nielsen's full Social Security number was not involved in the Cyberattack. SOMF ¶ 141. [redacted]

[redacted] This alleged injury therefore is not fairly traceable to Mednax and does not confer Article III standing to Nielsen. *See Antman*, 2018 WL 2151231, at *10.

Nielsen also contends that the Cyberattack "negatively affected" her credit score and that an $81.47 bill from American Anesthesiology "was marked as overdue and unpaid and had been sent to collections, although the $81.47 was from a bill her insurance had already paid in 2017." SAC ¶¶ 204-05. Nielsen explained at her deposition that [redacted] SOMF ¶ 145. But other than unsubstantiated speculation, Nielsen has no evidence that the $81.47 charge being sent to collections had anything to do with the Cyberattack. *See Wills v. Walmart Assocs., Inc.*, 592 F. Supp. 3d 1203, 1240 (S.D. Fla. 2022) ("[C]onjecture . . . isn't enough to survive summary judgment."). Indeed, Nielsen confirmed at her deposition that [redacted]. SOMF ¶ 146. [redacted].

**3. Plaintiffs' Other Theories Are Insufficient to Establish Article III Standing.**

As discussed above, *Green-Cooper* confirms that actual misuse of information involved in a data breach is required to satisfy Article III's injury-in-fact requirement. Plaintiffs have failed to satisfy this *prima facie* requirement and no further analysis is required. For completeness, however, Mednax addresses each of the other bases for Article III standing that the Court found were sufficiently *alleged* to state a claim in its Motion to Dismiss Order. As discussed below, none of these alleged injuries-in-fact passes muster now that the factual record has been fully developed.

***i. Discovery Confirms There Is No Evidence of a Substantial Risk of Future Harm.***

The Eleventh Circuit has held that, absent "specific evidence of *some* misuse of class members' data," a plaintiff generally cannot show that a "threatened harm of future identity theft [is] 'certainly impending'—or that there [is] a 'substantial risk' of such harm." *Tsao*, 986 F.3d at 1344. Indeed, this Court's previous holding that Plaintiffs had alleged a substantial risk of future

harm was predicated on their *allegations* of "actual misuse and actual access of their personal data resulting from" the Cyberattack. ECF No. 104 at 14. As discussed above, however, discovery has demonstrated that Plaintiffs' allegations of actual misuse and actual access are unsupported by any evidence. Accordingly, Plaintiffs cannot survive summary judgment by relying on a hypothetical risk of future harm. *See id.*; *Green-Cooper*, 73 F.4th at 889 (holding that "misuse of the data cybercriminals acquire from a data breach" is "required" to establish Article III standing "because such misuse constitutes both a 'present' injury and a 'substantial risk' of harm in the future").

***ii. Because Plaintiffs Have Not Demonstrated A Substantial Risk Of Future Harm, Their Allegations Of Emotional Distress Are Insufficient To Confer Article III Standing.***

In its Motion to Dismiss Order, this Court previously held that Plaintiffs had standing to sue for damages based on their "allegations of emotional distress, coupled with the substantial risk of future harm." ECF No. 104 at 15. This Court acknowledged, however, that where emotional distress is not coupled with misuse of information or a substantial risk of future harm, it is insufficient to constitute as a legally cognizable injury-in-fact. *Id.* This is confirmed by the Eleventh Circuit's recent decision in *Green-Cooper*, which held that Article III "require[s] misuse of the data cybercriminals acquire from a data breach." *Id.* at 889. As discussed above, discovery has shown that Plaintiffs' data has not been misused as a result of the Cyberattack and that Plaintiffs are not facing a substantial risk of future harm.

[redacted]

*E.g.*, SOMF ¶¶ 28 ([redacted]), 69 ([redacted]), 115 ([redacted]), 184 ([redacted]).

***iii. Mitigation Measures Protecting Against A Speculative Risk Of Future Harm Do Not Qualify As An Injury-In-Fact.***

In its Motion to Dismiss Order, this Court held that "the cost of the increased time Plaintiffs have spent and must continue to spend reviewing their financial information" constitutes a

"concrete harm[] sufficient to satisfy the [Supreme] Court's holding in *TransUnion*." ECF No. 104 at 14. This holding was predicated on the Court's finding that Plaintiffs had adequately *alleged* a substantial risk of future harm. As the Court acknowledged in its Motion to Dismiss Order:

> [A] plaintiff cannot 'conjure standing by inflicting some direct harm on itself to mitigate a perceived risk.' . . . In other words, any steps plaintiffs take to monitor their credit or financial statements for fraudulent activity establish an injury in fact only if plaintiffs have shown that they face a substantial or certainly impending threat of future harm.

ECF No. 104 at 11-12 (quoting *Tsao*, 986 F.3d at 1339). And in order to demonstrate a substantial or certainly impending threat of future harm, Plaintiffs must show "'actual misuse or actual access to personal data.'" *Id.* at 12 (quoting *Tsao*, 986 F.3d at 1340). For the reasons discussed above, Plaintiffs cannot make that showing. Accordingly, Plaintiffs' assertions that they have spent time and must continue to spend time reviewing their financial information, or have taken other steps to mitigate against the risk of a speculative risk of future harm (such as purchasing or renewing identity theft protection services), do not create Article III standing. *See Tsao*, 986 F.3d at 1344 (where "a 'hypothetical future harm' is not 'certainly impending,' plaintiffs 'cannot manufacture standing merely by inflicting harm on themselves'") (quoting *Muransky v. Godiva Chocolatier, Inc.*, 979 F.3d 917, 931 (11th Cir. 2020) (en banc)).

#### *iv. Plaintiffs Cannot Establish Standing Based On A Diminution In Value Of Their Personal Information.*

In the Motion to Dismiss Order, this Court concluded that Plaintiffs' *allegations* that their PHI and PII had lost value were sufficient to confer Article III standing at the motion to dismiss stage because they had *alleged* an "'actual' (rather than 'hypothetical') diminution in value [that] 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.'" ECF No. 104 at 17 (citations omitted). Now that the Eleventh Circuit has clarified that it "require[s] misuse of the data cybercriminals acquire from a data breach" to establish Article III standing, the mere decrease in value of PII or PHI is insufficient. *Green-Cooper*, 73 F.4th at 889.

Even if *Green-Cooper* did not foreclose this theory of standing, however, Plaintiffs still would not be able to survive summary judgment based on an alleged diminution of value of their PHI and PII. That is because, [redacted]

[redacted] *See* SOMF ¶ 14 & Ex. 15 ¶ 68 [redacted] (emphasis added)); *In re Yahoo! Inc. Customer Data Sec. Breach Litig.*, 2017 WL 3727318, at *14 (N.D. Cal. Aug. 30, 2017) (finding that plaintiff plausibly alleged loss of value where plaintiff alleged that "Plaintiffs' PII is being sold by hackers on the dark web"). In addition, now that discovery is over, the undisputed record evidence confirms that the Cyberattack did not damage Plaintiffs' "ability to purchase goods and services remotely and without the need to pay in cash or a check." ECF No. 104 at 17 (internal quotation marks and citations omitted). [redacted] . *See, e.g.,* SOMF ¶¶ 29, 47, 81, 103, 114, 147, 165, 186, 197. Accordingly, the alleged diminution in value of Plaintiffs' PHI and PII does not constitute an injury-in-fact sufficient to establish Article III standing at the summary judgment stage.

***v. Plaintiffs' Alleged Loss of Privacy Is Not an Injury-In-Fact.***

Plaintiffs' assertions that they have suffered a legally cognizable injury because they have suffered a loss of privacy are also foreclosed by Plaintiffs' failure to substantiate their allegations of a substantial risk of future harm. In its Motion to Dismiss Order, this Court found that "Plaintiffs' claims of loss of privacy are sufficient to confer standing" because they had *alleged* that they "are under a substantial and imminent risk of future identity theft because unauthorized third parties, and possibly criminals, gained access to their PHI and PII."[11] ECF No. 104 at 17. As discussed above, however, discovery revealed no evidence that any unauthorized third parties actually "gained access to [Plaintiffs'] PHI and PII." *See id.* Nor is there any evidence that any PII or PHI was misused as a result of the Cyberattack. Thus, Plaintiffs are not facing a substantial

[11] The Eleventh Circuit's *Green-Cooper* decision indicates that a loss of privacy, standing alone, does not suffice to qualify as an injury-in-fact under Article III. *See Green-Cooper*, 73 F.4th at 892-93 (reversing and remanding grant of class certification and suggesting that individuals who merely "had their data accessed by cybercriminals" would not "clear any standing bar imposed by *Tsao*").

and imminent risk of future identity theft and cannot rely on their allegations of loss of privacy to establish Article III standing at the summary judgment stage.[12]

***vi. Plaintiffs Have Not Lost the Benefit of Their Bargain with Mednax.***

Finally, discovery has demonstrated that Plaintiffs' allegations they purportedly did not receive the benefit of their bargain with Mednax because they allegedly paid for privacy protections they did not receive are unfounded. SAC ¶ 8. Though this Court concluded that this was a viable theory based on the Plaintiffs' *allegations*, discovery has shown that there is no evidence to support this theory.[13] *See* ECF No. 104 at 17-18. Indeed, despite being asked to do so in discovery, Plaintiffs produced no evidence to show that they made any payments to Mednax, [redacted]. SOMF ¶¶ 68, 82, 112, 194. Multiple Plaintiffs admitted that [redacted]. *Id.* ¶¶ 45 (Rumely), 80 (Jay), 99 (Soto), 113 (Baum), 124 (Larsen), 148 (Nielsen), 181 (Cohen). In fact, Rumely admitted that he [redacted] *Id.* ¶ 45. Lee testified [redacted] *Id.* ¶ 163. And Plaintiffs B.W., Jay, Larsen, and Cohen [redacted] *Id.* ¶¶ 27, 77, 125, 182. This evidence compels the conclusion that data security was not part of the Plaintiffs' bargain with Mednax.

* * *

In sum, discovery has not substantiated the allegations that this Court relied on in concluding that Plaintiffs had Article III standing to bring these claims at the inception of this case. Thus, because none of the Plaintiffs has Article III standing, summary judgment must be entered in Mednax's favor.[14]

---

[12] Indeed, even Plaintiffs' own damages expert, Gary Olsen, acknowledged in his report that it is [redacted] SOMF ¶ 14 & Ex. 15 ¶ 68. [redacted]

[13] *Green-Cooper* also forecloses Plaintiffs' lost benefit of their bargain theory because it requires "misuse" of data to satisfy Article III's injury-in-fact requirement. *Green-Cooper*, 73 F.4th at 889.

[14] Without standing, the Court need not analyze any substantive claims. Mednax, nonetheless, addresses the deficiencies of each substantive claim below.

**B. The Undisputed Facts Show No Violations of State Statutory Laws.**

**1. Mednax Did Not Violate The Maryland Consumer Protection Act (MCPA).**

To prevail on an MCPA claim, Cohen (the only Maryland Plaintiff) must prove (1) an unfair or deceptive practice or misrepresentation that (2) was relied upon, and (3) caused actual injury. *Barnhill v. A&M Homebuyers, Inc*., 2022 U.S. Dist. LEXIS 151046, at *18 (D. Md. Aug. 22, 2022). Cohen's MCPA claim fails on all fronts.

***First***, Cohen's own testimony precludes her from establishing the first two elements. Mednax could not have made a material misrepresentation to Cohen because she conceded that [redacted]. SOMF ¶ 183. And even if Mednax had somehow made a misrepresentation, Cohen clearly did not rely on it because she testified that [redacted]" *Id.* ¶ 181—not because of any representations regarding Mednax's security practices. *See Attias v. CareFirst, Inc.*, 2023 U.S. Dist. LEXIS 161800, at *59 (D.D.C. Sept. 13, 2023) (granting summary judgment on MCPA claim where there was "no indication Plaintiffs were even cognizant of the alleged misrepresentations when they chose CareFirst as their health insurance"). In fact, she admitted to [redacted]. SOMF ¶ 182. In other words, there is no evidence that any purported "misrepresentation" by Mednax "substantially induce[d] [Cohen]'s choice" to visit a hospital staffed by Mednax-affiliated clinicians. *Tucker v. Am. Residential Servs., LLC*, 2018 U.S. Dist. LEXIS 49022, at *16-17 (D. Md. Mar. 26, 2018) (quoting Md. Code Ann., Com. Law, § 13-303). Without evidence of these elements, Cohen's MCPA claim cannot survive summary judgment.

Second, Cohen has no evidence of actual injury. Under the MCPA, the actual injury "must be objectively identifiable," as "measured by the amount the consumer spent or lost as a result of his or her reliance on the [] misrepresentations." *Barnhill*, 2022 U.S. Dist. LEXIS 151046, at *18 (quoting *Lloyd v. Gen. Motors Corp*., 916 A.2d 257, 277 (Md. 2007)). [redacted] SOMF ¶ 185. And all of her other alleged

damages are either not legally cognizable or could not have resulted from the Cyberattack. *See* section III.A.3, *supra*. Her MCPA claim fails for this reason, as well.[15]

**2. Mednax Did Not Violate The Arizona Consumer Fraud Act (ACFA).**

"To succeed on a claim of consumer fraud [under the ACFA], a plaintiff must show a false promise or misrepresentation made in connection with the sale or advertisement of merchandise and consequent and proximate injury resulting from the promise." *Kuehn v. Stanley*, 91 P.3d 346, 351 (Ct. App. 2004). The plaintiff must establish that he "relie[d] . . . on false or misrepresented information" to establish a violation. *Id.* (affirming summary judgment based on plaintiff's failure to establish requisite reliance on alleged misrepresentation in an appraisal report at the time the purchase offer was made). Like Cohen, Larsen's own admissions defeat his ACFA claim.

Larsen testified that [redacted] *See* SOMF ¶ 124. Nor is there any evidence Larsen relied on any such representations in deciding to obtain or receive services from Pediatrix. On the contrary, Larsen testified that [redacted] *Id.* ¶ 123. This is underscored by [redacted]. *Id.* ¶ 125. Summary judgment in favor of Mednax as to Count II is required on this basis as well.[16]

**3. Mednax Did Not Violate The California Customer Records Act (CCRA).**

Rumely's CCRA claim rests on the allegation that Mednax "fail[ed] to disclose the Healthcare Data Breach in a timely and accurate manner."[17] SAC ¶ 518. To survive summary judgment based on this theory, Rumely must show a "factual basis for the conclusion that an

[15] *See* n.16, *infra.*

[16] Even if plaintiffs' MCPA and ACFA claims could survive summary judgment (which they cannot), under no circumstances can plaintiffs obtain the disgorgement theory of damages sought under the statutes in the Complaint. *See* SAC ¶¶ 498, 509. Neither statute allows private plaintiffs to recover disgorgement of profits. *See Assanah-Carroll v. L. Offs. of Edward J. Maher, P.C.*, 281 A.3d 72, 83 (Md. Ct. App. 2022); *Peery v. Hansen*, 585 P.2d 574, 578 (Ariz. Ct. App. 1978).

[17] The CCRA, generally speaking, is California's data breach notification statute. *See* Cal. Civ. Code § 1798.82.

alleged delay in notifying customers of a data breach [or inaccuracy are] traceable to a [cognizable] harm." to himself or other class members. *See Dugas v. Starwood Hotels & Resorts Worldwide, Inc.*, 2016 U.S. Dist. LEXIS 152838, at *10, *20-21 (S.D. Cal. Nov. 3, 2016) (merely identifying injuries purportedly suffered by plaintiff and alleging defendants' failure to provide prompt notice contributed to those losses insufficient to establish CCRA violation) (citing *In re Adobe Sys. Inc. Privacy Litig.*, 66 F. Supp. 3d 1197, 1216 (N.D. Cal. 2014)).

Rumely [redacted] SOMF ¶ 51. [redacted] *Id.* ¶ 46. But even assuming Rumely had identified some speculative "injury" (which he has not), he has not shown that it was a result of delayed notice (as opposed to the Cyberattack itself). *See In re Sony Gaming Networks & Customer Data Security Breach Litig.*, 996 F. Supp. 2d 942, 965 (S.D. Cal. 2014) ("Plaintiffs allegations do not set forth a plausible claim for relief on the basis that the delay, and not just the intrusion, caused Bova's alleged injuries."). Nor has Rumely demonstrated that the notice he received of the Cyberattack was inadequate in any way. "Accordingly, because Plaintiff has failed to trace any harm from Defendants' delayed notification or to demonstrate a nexus between the alleged harm flowing from the delayed notification and Defendants' actions, Plaintiff has failed to adequately alleged causation with respect to his CRA § 1798.82 claim." *Dugas*, 2016 U.S. Dist. LEXIS 152838, at *21.

**4. Mednax Did Not Violate the California Confidentiality of Medical Information Act (CMIA).**

Plaintiff Rumely also brings a CMIA claim against Mednax, claiming it violated Cal. Civ. Code § 56.101 because its "negligence resulted in the release of individually identifiable medical information pertaining to Plaintiff Rumely…to unauthorized persons and the breach of the

[18] Rumely testified that, [redacted] SOMF ¶ 48. [redacted] *Id.* ¶ 49. [redacted] *Id.* ¶ 50.

confidentiality of that information." SAC ¶ 599. Plaintiff Rumely has not met (and could not meet) his burden to sustain this claim for at least two reasons.

***First***, Rumely alleges in the Complaint that he is bringing a claim under the CMIA for the alleged "release of individually identifiable medical information pertaining to Plaintiff Rumely." SAC ¶ 599; *see also id.* ¶¶ 601-02. [redacted] SOMF ¶¶ 34-35. [redacted] *Id.* ¶ 34. But that is not what he alleged in the complaint, and under binding Eleventh Circuit precedent, "[a] plaintiff may not amend her complaint through argument in a brief opposing summary judgment." *Gilmour v. Gates, McDonald & Co.*, 382 F.3d 1312, 1315 (11th Cir. 2004). Because discovery has failed to reveal evidence to support the CMIA claim Rumely pleaded, Mednax is entitled to summary judgment.

***Second***, regardless of whether Rumely's CMIA claim is predicated on the alleged release of his confidential medical information or his child's confidential medical information, Mednax is entitled to summary judgment because Rumely has zero evidence to support an essential element of his claim. To 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." *In re Ambry Genetics Data Breach Litig.*, 567 F. Supp. 3d 1130, 1148 (C.D. Cal. 2021). Put another way, there can only be a breach of confidentiality under the CMIA when "an unauthorized person views the medical information." *Sutter Health v. Super. Ct.*, 174 Cal. Rptr. 3d 653, 660 (Cal. Ct. App. 3d 2014). This is because "it is the medical information, not the physical record…that is the focus of the [CMIA]. While there is certainly a connection between the information and its physical form, possession of the physical form without actually viewing the information does not offend the basic public policy advanced by the [CMIA]." *Id.*

[redacted] *See, e.g.,* SOMF ¶ 11 & Ex. 18 ¶ 27 ("[redacted]

[redacted]

[redacted]"). This fact is not in dispute.

In other words, Rumely is *assuming* that the information was viewed. But as courts routinely hold, claims that medical information was viewed supported only by conjecture cannot sustain a CMIA claim. *See Doe v. Sutherland Healthcare Sols.*, 2021 WL 5765978, at *7 (Cal. Ct. App. Dec. 6, 2021) (plaintiff cannot rest on "layers of speculation" for the *possibility* that confidential medical information was viewed by an unauthorized individual because "that is not the standard") (unpublished); *Regents of Univ. of Cal. v. Super. Ct.*, 163 Cal. Rptr. 3d 205, 221 (Ct. App. 2013) (no violation of CMIA unless plaintiff pleads and proves an unauthorized person actually viewed information). Stated differently, one does not create a disputed issue of fact by raising "mere possibilities" that the information was viewed. *Brown v. Ransweiler*, 89 Cal. Rptr. 3d 801, 810 (Ct. App. 2009); *see also Doe I v. Health*, 2020 Cal. Super. LEXIS 32001, at *10-11 (Cal. Super. Ct. Nov. 3, 2020) (dismissing CMIA claim because plaintiffs needed to have pointed to "actual, non-speculative disclosure of [their] personal medical history, diagnoses, or care" that was linked to their individually identifiable information).

In fact, it is not enough to show that an unauthorized third party viewed a file containing the plaintiff's medical information. *Vigil v. Muir Med. Grp. IPA, Inc.*, 300 Cal. Rptr. 32, 48 (Ct. App. 2022). Rather, Rumely bears the burden of demonstrating that his specific confidential medical information (or, if proceeding on behalf of his child, his child's confidential medical information) was viewed by an unauthorized third party. [redacted] SOMF ¶ 17. [redacted] .[19] [redacted] *id.* ¶ 38, [redacted]

[19] [redacted] The difference between the varying copies appears to be changes in date as spreadsheets were updated, but the structure and format remained the same.

[redacted] *Id.* ¶ 39. Rumely has no evidence to suggest that the threat actor—or any other unauthorized third-party—did either of those things.

Beyond Rumely's rank speculation that his child's information may have been viewed, the only other "evidence" he has produced to support that assertion are [redacted]. But Rumely has provided absolutely no evidence to connect [redacted] to a threat actor somehow viewing his child's medical information. As explained in Section III.A.2.iii, *supra*, Mednax never possessed the email address to which Rumely claims he received phishing emails. Nor was Rumely's email address included in the source files pertaining to Rumely's child that were potentially involved in the Cyberattack.[20] And even if Rumely's email address had been disclosed (and it was not), an email address is not "medical information" under the CMIA.[21] Mednax is entitled to summary judgment on Rumely's CMIA claim.

**5. Mednax Did Not Violate The Washington Consumer Protection Act (WCPA).**

Jay alleges Mednax made material misrepresentations or omissions regarding its security practices which have caused injury in violation of the WCPA, Wash. Rev. Code Ann. § 19.86.020. SAC ¶¶ 585-93. "To prevail on a [W]CPA claim, a plaintiff must show (1) an unfair or deceptive act or practice, (2) occurring in trade or commerce, (3) impacting the public interest, (4) injury to

---

[20] Any suggestion that access to Rumely's email address exposed medical information is unsupported by Rumely's own testimony. Rumely testified that [redacted]. SOMF ¶ 52.

[21] The CMIA defines "medical information" as "any individually identifiable information, in electronic or physical form, in possession of or derived from a provider of health care, health care service plan, pharmaceutical company, or contractor regarding a patient's medical history, mental health application information, mental or physical condition, or treatment." Cal. Civ. Code § 56.05(i). "[D]emographic or numeric information that does not reveal medical history, diagnosis, or care" is excluded from the definition of "medical information" under the CMIA. *Eisenhower Med. Ctr. v. Super. Ct.,* 172 Cal. Rptr. 3d 165, 168-69 (Ct. App. 2014) (medical index including clerical number linked to individual's name, medical record number, age, date of birth, and the last four digits of their Social Security number did not constitute "medical information" for purposes of the CMIA because index itself did not contain "substantive information regarding a patient's medical condition or history" sufficient to actually "reveal medical history, diagnosis, or care").

the plaintiff's business or property, and (5) causation." *G.G. v. Valve Corp.*, 579 F. Supp. 3d 1224, 1232 (W.D. Wash. 2022), *aff'd sub nom. Galway v. Valve Corp.*, 2023 WL 334012 (9th Cir. Jan. 20, 2023). Jay cannot meet the first, fourth, and fifth elements.

First, there is no evidence to suggest that Mednax engaged in any unfair or deceptive acts or practices. As discussed below, discovery confirmed that [redacted] At best, Jay merely has evidence to show that Mednax was among the many companies impacted by third-party criminal cyberattacks.

Second, Jay has not met the injury to business or property requirement. The Washington Supreme Court has been clear: personal injuries are *not* acceptable for a WCPA claim. *Wash. State Physicians Ins. Exch. & Ass'n v. Fisons Corp.*, 858 P.2d 1054, 1064 (Wash. 1993). Thus, "pain and suffering and emotional distress damages are not compensable [W]CPA injuries." *Steele v. Extendicare Health Servs., Inc.*, 607 F. Supp. 2d 1227, 1230 (W.D. Wash. 2009). In the Motion to Dismiss Order, the Court allowed Plaintiff Jay's WCPA claim to proceed based on Jay's claim that there was a "diminution in [] value [of her son's personal information] within the marketplace of credit." ECF No. 104 at 40. But with the benefit of discovery, Jay has not offered a shred of evidence that would support her child's personal information has somehow lost value. [redacted] SOMF ¶ 85. [redacted] *See Id.* ¶ 14. [redacted] *Id.* ¶ 84 & Ex. 37 at 126:2-8 (testifying that [redacted]"). In fact, Jay withdrew the allegations that her son's Social Security number was available for sale on the dark web, acknowledging that they were unsupported by the evidence. ECF No. 222. What is more—Jay clearly and unambiguously testified that [redacted]. *See* SOMF ¶ 81.

Third, Jay cannot prove causation. To sustain a claim under the WCPA, "the plaintiff must establish that, but for the defendant's unfair or deceptive practice, the plaintiff would not have suffered an injury." *G.G.*, 579 F. Supp. 3d at 1233. And where, as here, "the injury would have occurred regardless of whether the alleged violation existed, causation cannot be established." *Id.* Jay bases her WCPA claim on alleged misrepresentations and omissions regarding Mednax's cybersecurity. SAC ¶¶ 588-89. There is no evidence to suggest that if these so-called misrepresentations or omissions had not occurred, her alleged injuries would have been prevented.

[redacted][22][redacted]

[redacted] SOMF ¶ 77. [redacted]

[redacted]

*Id.* ¶ 80 & Ex. 37 at 171:12-21. [redacted]

[redacted] *Id.* ¶ 78 & Ex. 37 at 170:15–171:7. [redacted]

[redacted] *Id.* ¶ 80 & Ex. 37 at 172:22–173:11. Given these undisputed facts, "[n]o reasonable factfinder could find that [her] decisions would have been affected" even if Mednax made any security practice-related representations. *G.G.*, 579 F. Supp. 3d at 1235. Mednax is entitled to summary judgment on Jay's WCPA claim.

**6. Mednax Did Not Violate The Florida Deceptive And Unfair Trade Practice Act (FDUTPA).**

Plaintiffs assert a FDUTPA claim for injunctive relief, not damages. SAC ¶¶ 531-32. This claim fails for a multitude of reasons. As a preliminary matter, there is no evidence to support a claim that any Defendant engaged in "[u]nfair methods of competition, unconscionable acts or

[22] In their Motion for Class Certification, Plaintiffs argue that there is a "rebuttable presumption" of reliance under the WCPA in omissions cases. *See* Motion for Class Certification at 16. But Plaintiffs allege both representations *and* omissions, so the presumption does not apply. *See* SAC ¶¶ 588-89. Even if it did, the presumption is rebuttable when it applies. As the *G.G.* court held, "[t]his presumption can be rebutted by a showing that the plaintiff's decision would have been unaffected even if the omitted fact had been disclosed." 579 F. Supp. 3d at 1234. As set forth above, Jay's own testimony and decision to utilize the same hospital after the Cyberattack confirms her decision was unaffected by anything related to Mednax's cybersecurity.

practices, and unfair or deceptive acts or practices in the conduct of any trade or commerce," as required to violate the statute. *See* Fla. Stat. § 501.204(1).

Second, Plaintiffs' FDUTPA claim is limited to one for injunctive relief, not damages. But only an "aggrieved" party that has experienced a "non-speculative injury that has affected the plaintiff beyond a general interest in curbing deceptive or unfair conduct" can bring a claim for injunctive relief under FDUTPA. *See Farmer v. Humana, Inc.*, 582 F. Supp. 3d 1176, 1190 (M.D. Fla. 2022). And importantly, "although the FDUTPA allows a plaintiff to pursue injunctive relief even where the individual plaintiff will not benefit from an injunction, it cannot supplant Constitutional standing requirements." *In re Am. Med. Collection Agency Customer Data Sec. Breach Litig.*, 2021 U.S. Dist. LEXIS 240360, at *92-93 (D.N.J. Dec. 16, 2021) (dismissing FDUTPA injunctive relief claim where plaintiffs alleged no threat of future harm from a data breach) (quoting *Marjam Supply Co. v. Pliteq, Inc.*, 2018 WL 4932871, at *4 (S.D. Fla. Apr. 23, 2018)). Thus, to survive summary judgment on a claim for injunctive relief under FDUTPA, Plaintiffs must "offer evidence that [they] could suffer a future injury." *Phillips v. Hobby Lobby Stores, Inc.*, 2019 WL 8348163, at *8 (N.D. Ala. Dec. 16, 2019) (granting defendants' motion for summary judgment on FDUTPA claim); *Calderon v. SIXT Rent A Car, LLC*, 2022 WL 4355761, at *6 (S.D. Fla. Sept. 20, 2022) (granting summary judgment to defendant on FDUTPA claim where "there is simply no record evidence that could support a finding of actual or imminent threat" of future harm). Discovery now demonstrates that there is no evidence Plaintiffs are facing an actual or imminent threat of future harm. *See* Section III.A.3.i, *supra*. As all companies should, Mednax is continually improving its cybersecurity, and [redacted] SOMF ¶ 19 & Ex. 2 at MEDNAX0130104. [redacted] SOMF Ex. 3 ¶ 242. Thus, Plaintiffs' FDUTPA claim fails.

### C. Mednax Is Entitled To Summary Judgment On Plaintiffs' Negligence Claims.

To state a viable claim for negligence, Plaintiffs must ***prove*** a legally recognized duty, breach of that duty, and damages proximately caused by the alleged breach.[23] Failure to prove any one of these elements is fatal to a negligence claim.

#### 1. Plaintiffs' Negligence Claims Are Governed By A Multitude Of States' Laws.

Though this Court previously applied Florida law to Plaintiffs' negligence claims in ruling on Defendants' motion to dismiss, intervening Eleventh Circuit case law and facts developed in discovery require the Court to revisit its choice-of-law analysis. This Court's holding that Florida law applies globally was predicated on its belief that "the location of the injury" was the "breach," and on its crediting of the Plaintiffs' *allegations* that "Florida is where the data was maintained, multiple Defendants are domiciled, and Defendants' security protocols allegedly broke down." ECF No. 104 at 7-8. In *Green-Cooper*, which was issued after this Court's motion to dismiss order, the Eleventh Circuit has now clarified that a plaintiff experiences injury not from a data breach itself, but instead when, "as a result of the breach, [she] experiences 'misuse' of [her] data in some way." 73 F.4th at 889. And discovery has shown that [redacted]. SOMF ¶¶ 6, 9, 13.

These new developments change the outcome of the choice-of-law analysis. Florida's choice-of-law rules require this Court to apply the "'most significant relationship' test" to Plaintiffs' negligence claims. *Grupo Televisa, S.A. v. Telemundo Communs. Grp.*, 485 F.3d 1233, 1240 (11th Cir. 2007).[24] Under that test, "[w]hen determining the most significant relationship,

---

[23] *Jordan v. Jordan*, 257 S.E.2d 761, 762 (Va. 1979); *Jacques v. First Nat'l Bank of Md.,* 515 A.2d 756, 758 (Md. 1986); *Martishius v. Carolco Studios, Inc.*, 562 S.E.2d 887, 892 (N.C. 2002); *IHS Cedars Treatment Ctr. of DeSoto, Tex., Inc. v. Mason*, 143 S.W.3d 794, 798 (Tex. 2004); *Gipson v. Kasey*, 150 P.3d 228, 230 (Ariz. 2007) (en banc); *BancFirst v. Dixie Rests., Inc.*, 2012 WL 12879, at *3 (W.D. Okla. Jan. 4, 2012); *Tribeca Cos., LLC v. First Am. Title Ins. Co.,* 192 Cal. Rptr. 3d 354, 375 (Ct. App. 2015); *Buckley v. Santander Consumer USA, Inc.*, 2018 WL 1532671, at *5 (W.D. Wash. Mar. 29, 2018); *Jenkins v. CEC Ent. Inc.*, 421 F. Supp. 3d 257, 262 (D.S.C. 2019).

[24] Mednax focuses on Florida's choice-of-law test because the Eleventh Circuit recently held an "MDL court" "sitting in diversity in Florida" must "appl[y] Florida's choice-of-law rules." *In re Jan. 2021 Short Squeeze Trading Litig*, 76 F.4th 1335, 1346 (11th Cir. 2023). This is "[b]ecause the master complaint superseded the original complaints," making Florida "the forum for pretrial

the courts consider '(a) the place where the injury occurred, (b) the place where the conduct causing the injury occurred, (c) the domicile, residence, nationality, place of incorporation and place of business of the parties, and (d) the place where the relationship, if any, between the parties is centered.'" *Michel v. NYP Holdings, Inc.*, 816 F.3d 686, 694 (11th Cir. 2016) (quoting *Bishop v. Fla. Specialty Paint Co.*, 389 So. 2d 999, 1001 (Fla. 1980)). Applying these four choice-of-law factors to each of the Plaintiffs' negligence claims points to the application of a multitude of states' laws.

The first factor examines the place where the injury occurred. *Id.* Under *Green-Cooper*, the injury occurs when the Plaintiffs experience misuse of their data. 73 F.4th at 889. Though no Plaintiffs have experienced misuse of their data caused by the Cyberattack, to the extent any misuse has occurred, it has happened in each Plaintiff's home State. *See, e.g.*, SOMF ¶¶ 137 ([redacted]); 53 ([redacted]); 155, 160 ([redacted]).

The second factor examines the place where the conduct causing the injury occurred. *Michel*, 86 F.3d at 694. As discussed in Defendants' Opposition to Plaintiffs' Motion for Class Certification, no evidence supports the allegation, on which this Court relied at the motion-to-dismiss stage, that "Florida is where [Plaintiffs'] data was maintained." ECF No. 104 at 8. Discovery demonstrated that the Cyberattack involved only Mednax's Microsoft Office 365 environment. SOMF ¶ 13 & Ex. 14 ¶ 28 [redacted]). That is a cloud-based environment. *Id.* ¶ 6. As this Court pointed out, the location of "data stored on the cloud" may "be unknown or even unknowable." ECF No. 104 at 8. The unknown nature of this location prevents this factor from weighing heavily in the choice-of-law analysis. Nor is there evidence that Defendants' "security protocols allegedly broke down" in Florida. *Id.* [redacted] SOMF ¶ 9.

---

purposes." *Id.* at 1345–46. As discussed in Defendants' Opposition to Plaintiffs' Motion for Class Certification, if the choice-of-law rules of the other four transferor States were to apply, the result would be the same.

The third factor examines the domicile of the parties. *Michel*, 86 F.3d at 694. The Plaintiffs' domicile at the time of the Cyberattack "is the single most important contact for determining the state of the applicable law as to most issues" when, as here, they allege that private information was exposed. Restatement (Second) of Conflict of Laws §§ 145, 153. [redacted] SOMF ¶¶ 20, 34, 59, 71, 91, 104, 117, 127, 155, 174, 189.

The fourth factor examines the location where the relationship between the parties is centered. With one exception, the relationship between each Plaintiff and Defendants is centered in the Plaintiffs' home States at the time of the Cyberattack.[25] *Id.* ¶¶ 26, 44, 61, 74, 96, 109, 122, 128, 180, 192.

Applying these factors results in the application of a multitude of states' laws. Specifically, Baum and Bean's claims are governed by Oklahoma law, Clark and Lee's claims are governed by South Carolina law, Cohen's claims are governed by Maryland law, Jay's claims are governed by Washington law, Larsen's claims are governed by Arizona law, Nielsen's claims are governed by Virginia law, Rumely's claims are governed by California law, Soto's claims are governed by Texas law, and B.W.'s claims are governed by Missouri law. [26]

**2. Mednax Is Entitled To Summary Judgment On Larsen, B.W., Bean, Baum, Nielsen, Jay, And Cohen's Negligence Claims Because The Governing State Laws Do Not Recognize A Duty To Safeguard Personal Information From A Data Breach.[27]**

Discovery has demonstrated that Larsen, B.W., Bean, Baum, Nielsen, and Jay's negligence claims are governed by Arizona, Missouri, Oklahoma, Virginia, and Washington law, respectively.

---

[25] [redacted] SOMF ¶ 156.

[26] Even if Plaintiffs' claims were all governed by Florida law, Mednax would still be entitled to summary judgment on all Plaintiffs' negligence claims because Florida law requires Plaintiffs to prove causation and damages to demonstrate negligence. *John Morrell & Co. v. Royal Caribbean Cruises, Ltd.*, 534 F. Supp. 2d 1345, 1350 (S.D. Fla. 2008). Plaintiffs have no evidence to support either of these elements. *See* Sections III.c.4-III.c.5, *infra*.

[27] The only evidence that Plaintiffs have to support the breach element of their negligence claims is the unreliable conclusions of their cybersecurity expert, Mary Frantz. As discussed in

All of those States have expressly rejected negligence claims based on an alleged duty to safeguard personal information, holding no such duty exists. *See Parker v. Carilion Clinic*, 819 S.E.2d 809, 825 (Va. 2018) ("None of our precedents has ever imposed a tort duty on a healthcare provider" to safeguard PHI from unauthorized access); *Irwin v. Jimmy John's Franchise, LLC*, 175 F. Supp. 3d 1064, 1071 (C.D. Ill. 2016) (under Arizona law, no common-law duty to safeguard personal information from a data breach); *Cmty. Bank of Trenton v. Schnuck Mkts., Inc.*, 887 F.3d 803, 818 (7th Cir. 2018) (upholding dismissal of negligence claims and concluding that Missouri would not recognize a common-law duty to safeguard data); *BancFirst v. Dixie Rests., Inc.*, 2012 WL 12879, at *4 (W.D. Okla. Jan 4, 2012) (no duty to safeguard against theft of sensitive information under Oklahoma law); *Veridian Credit Union v. Eddie Bauer, LLC*, 295 F. Supp. 3d 1140, 1150 (W.D. Wash. 2017) (no duty to safeguard sensitive information "based on common law principles of negligence in Washington").

Cohen's negligence claim, which is governed by Maryland law, also fails because, under Maryland law, there is no duty to protect against the acts of a third party absent a special relationship. *Warr v. JMGM Grp.*, 70 A.3d 347, 358 (Md. 2013). Discovery confirms that no special relationship exists here. *See* Restatement (Second) of Torts § 314 (1965) (listing the special relationships that give rise to a duty to protect, including common carriers, innkeepers, and a possessor of land who holds it open to the public). Indeed, [redacted] SOMF ¶ 180.

**3. The Economic Loss Rule Bars Rumely, B.W., Clark, Lee, Nielsen, And Soto's Negligence Claims.**

Rumely, B.W., Clark, Lee, Nielsen, and Soto's negligence claims, which are governed by California, Missouri, South Carolina (for both Clark and Lee), Virginia, and Texas law, respectively, run headlong into their States' economic loss rules, which preclude liability in negligence for purely economic losses, which are those losses that do not involve personal injury

Defendants' Motion to Exclude Expert Testimony of Gary Olsen and Mary Frantz, Frantz's conclusions about Mednax's cybersecurity must be excluded. Without that evidence, Plaintiffs have nothing to support their allegations that Mednax breached a duty to safeguard their personal information, and Mednax is entitled to summary judgment on Plaintiffs' negligence claim for that reason, as well.

or property damage.[28] Discovery has demonstrated that none of these Plaintiffs have experienced any legally cognizable damages at all, let alone any personal injury or property damage that would allow them to recover under the governing State laws. *See* Section III.A, *supra*.

**4. Plaintiffs Have No Evidence To Support The Required Legally Cognizable Damages Element Of Their Negligence Claim.**

While related, injury-in-fact for the purpose of Article III standing is a lower burden than actual harm/damages for the purpose of negligence. *Attias v. CareFirst, Inc.*, 365 F. Supp. 3d 1, 13 (D.D.C. 2019) ("the standard for alleging actual damages is generally higher than that for plausibly alleging an injury-in-fact"). In other words, if Plaintiffs fail to support Article III standing (which, for reasons set forth above in Section III.A, they have), they necessarily fail to support actual damages for negligence. But the reverse is not true—even if Plaintiffs can establish Article III standing, that does not establish actual damages sufficient to support their negligence claims. The record demonstrates, with the benefit of discovery, there is no actual damage sufficient to support Plaintiffs' negligence claims.[29] Specifically:

***Improper disclosure of PHI/PII.*** Fatally, no Plaintiff can show that any of their PHI or PII was actually accessed, *see* Section III.A.1, *supra*; nor has a single Plaintiff produced a single iota of evidence that any information that was traceable to the Cyberattack was improperly disclosed anywhere. *See* Section III.A.2, *supra.* Accordingly, there can be no damages flowing from this baseless allegation.

***Loss of privacy.*** Plaintiffs have presented no evidence of a loss of privacy as a result of the Cyberattack. *See* Section III.A.3.v, *supra*. Even if they had, the Southern District of Florida has held that loss of privacy is insufficient to maintain a claim for damages on a negligence claim because "invasion of privacy under Florida common law is an intentional tort and therefore cannot

[28] *Golden Spread Elec. Coop., Inc. v. Emerson Process Mgmt. Power & Water Sols.*, 954 F.3d 804, 808 (5th Cir. 2020) (Texas law); *Tri-Lift NC, Inc. v. Drive Auto. Indus. of Am.*, 2021 WL 131017, at *3 (D.S.C. Jan. 13, 2021); *see also JPMCCM 2010-C1 Aquia Office LLC v. Mosaic Aquia Owner, LLC*, 2019 WL 4134035, at *6 (Va. Cir. Jan. 15, 2019); *In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, 903 F. Supp. 2d 942, 961 (S.D. Cal. 2012); *Autry Morlan Chevrolet Cadillac, Inc. v. RJF Agencies, Inc.*, 332 S.W.3d 184, 192 (Mo. Ct. App. 2010).

[29] Mednax does not re-hash Plaintiffs' evidentiary shortcomings (or standing-related precedent applicable to Plaintiffs' damages), which are addressed in great detail above. However, it suffices to say that to the extent the Court views any of the evidence as a "close call" for standing, the record is not sufficient to establish legally cognizable damages.

be pleaded as part of a claim for negligence." *Burrows v. Purchasing Power, LLC*, 2012 U.S. Dist. Lexis 186556, at *13 (S.D. Fla. Oct. 18, 2012).

***Out-of-pocket expenses and mitigation costs.*** Because Plaintiffs have not shown they are facing a substantial risk of future harm, they cannot manufacture standing by incurring out-of-pocket expenses or mitigation costs. *See* Section III.A.3.iii, *supra*. By the same token, these unnecessary voluntary expenditures do not suffice to create a triable issue of fact on the damages element of their negligence claim. *Forbes v. Wells Fargo Bank, N.A.*, 420 F. Supp. 2d 1018, 1019 (D. Minn. 2006) (granting summary judgment against the plaintiffs on their negligence claim because their expenditure of time and money monitoring their credit did not establish the essential element of damages); *Torres v. Wendy's Co.*, 195 F. Supp. 3d 1278, 1284 (M.D. Fla. 2016) (cost to mitigate hypothetical future harm is not a legally cognizable injury); *Durgan v. U-Haul Int'l Inc.*, 2023 U.S. Dist. LEXIS 131177, at *11 (D. Ariz. July 27, 2023) ("As explained above, Plaintiffs' allegations surrounding the [Cyberattack] merely establish conjectural or hypothetical harms. Without a finding to the contrary, Plaintiffs' mitigation expenses are similarly speculative."); *Gardiner v. Walmart Inc.*, 2021 WL 2520103, at *4-5 (N.D. Cal. Mar. 5, 2021) (finding no cognizable damages where plaintiff failed to establish that out-of-pocket expenses and lost time were reasonable and necessary); *Worix v. Medassets, Inc*., 857 F. Supp. 2d 699, 704-05 (N.D. Ill. 2012) (collecting cases dismissing negligence claims where only damage alleged was cost of guarding against risk of identity theft); *Shafran v. Harley-Davidson*, 2008 WL 763177, at *3 (S.D.N.Y. Mar. 24, 2008) ("Courts have uniformly ruled that the time and expense of credit monitoring to combat an increased risk of future identity theft is not, in itself, an injury that the law is prepared to remedy.").

***Increased risk of identity theft.*** Because discovery has revealed no evidence that any information belonging to Plaintiffs (or their children) was actually accessed in the Cyberattack, Plaintiffs' claim for damages relating to a hypothetical increase in the possibility of identity theft is not a cognizable injury for negligence claims. *In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, 996 F. Supp. 2d at 996 ("[T]he potential risk of future identity theft resulting from the loss of personal information is not a cognizable injury."); *Hammond v. Bank of N.Y. Mellon,* 2010 WL 2643307, at *13 (S.D.N.Y. June 25, 2010) ("[I]ncreased risk of identity theft (in the future) is not a cognizable claim."); *Gardiner,* 2021 WL 2520103, at *4 ("conclusory allegations of an increased risk of identity theft are insufficient to establish injury"); *Durgan*, 2023

U.S. Dist. LEXIS 131177, at *11 ("Without disclosure of social security number, bank, or credit card information, [compromised] PII does not present a clear ability for unscrupulous actors to commit fraud or identity theft.").

***Diminution in value of PII.*** To have cognizable damages under a diminution in value theory, Plaintiffs must show that they "participated or intended to participate in the market they identify, or that the defendants prevented them from capturing the full value of their internet usage information for themselves." *In re Google Inc. Cookie Placement Consumer Privacy Litig.,* 806 F.3d 125, 148-49, 152 (3d Cir. 2015). Plaintiffs have no evidence that could even conceivably satisfy this standard. *See* Section III.A.3.iv, *supra.* Therefore, they cannot rely on this theory of damages in support of their negligence claim.

***Benefit of the bargain.*** Lost benefit of the bargain is not a legally sufficient theory of damages for a negligence claim. *See Attias*, 365 F. Supp. 3d at 13 ("[T]he Court concludes that plaintiffs fail to state a claim for actual damages under their benefit-of-the-bargain theory."); *In re Cap. One Consumer Data Sec. Breach Litig*., 488 F. Supp. 3d 374, 404 (E.D. Va. 2020) (concluding that "Plaintiffs have failed to allege cognizable damages under their negligence claims based on the benefit of the bargain theory").[30]

**5. Plaintiffs Have No Evidence To Support Causation.**

To establish causation, there must be a "nexus between" the harm allegedly suffered and the Cyberattack. *Resnick v. AvMed, Inc.*, 693 F.3d 1317, 1326-27 (11th Cir. 2012). In other words, there needs to be a "logical connection between the data breach and the" harm suffered. *Almon v. Conduent Business Services, LLC*, 2019 WL 132078564, at *9 (N.D. Ga. Aug. 9, 2019); *see also Stephens v. Availity*, 2019 U.S. Dist. LEXIS 239572, at *13 n.5 (M.D. Fla. Oct. 1, 2019) (noting that if plaintiff alleging spam calls for medical services following data breach "is unable to show that her medical history, provider information, and telephone number were exposed in the data breach, then she likely would be unable to prove a *prima facie* case of negligence to get past the summary judgment stage"); *McGlenn v. Driveline Retail Merch., Inc.*, 2021 U.S. Dist. LEXIS 179775, at *27-31 (C.D. Ill. Sept. 21, 2021) (granting summary judgment in favor of defendant Driveline because plaintiff failed to show sufficient evidence that Driveline proximately caused

[30] Benefit of the bargain damages are "traditionally the core concern of contract law." *E. River S.S. Corp. v. Transamerica Delaval, Inc.*, 476 U.S. 858, 870 (1986). Plaintiffs contract-based claims against Mednax have been dismissed.

her injuries where "[plaintiff's] incidents of identity theft necessarily relied on PII that was not disclosed in Driveline's Disclosure. The obvious implication is that the thieves could not have relied on Driveline's Disclosure alone to commit the incidents of identity theft"). Here, even if one were to assume any Plaintiff suffered a legally cognizable harm, Plaintiffs have no evidence to connect that harm to the Cyberattack.

In its Motion to Dismiss Order, the Court concluded that five allegations, taken as true at the motion to dismiss stage, were sufficient to *allege* causation. ECF No. 104 at 51-52. Discovery now has proven that each of these allegations is false. Taking each in turn:

- ***"Plaintiffs allege that their PHI and PII were found available for purchase on the dark web following the Data Breaches.***" As a starting point, Plaintiffs Jay, Soto, Baum, and Larsen have withdrawn this allegation. See ECF No. 222. This leaves Plaintiffs A.W., B.W., Cohen, and Clark. But the only evidence these four individuals have to support this allegation is [redacted][31] SOMF ¶ 205. Frantz's conjecture is not enough to create a disputed issue of material fact. But even if it were, the Social Security numbers could not have come from the Cyberattack because Mednax did not even have them anywhere in its systems. *See* Section III.A.2.ii, *supra*.
- ***"Plaintiffs allege that their PHI and PII found for sale on the dark web contained the same information provided to medical providers that contracted with Defendant Mednax.***" This allegation has been proven false in discovery for the same reasons discussed above. *See* Section III.A.2.ii, *supra*.
- ***"Plaintiff Nielsen alleges that she has suffered identity theft, that twelve bank accounts have been opened in her name, that her credit score has been damaged, that she has experienced***

[31] As discussed in Defendants' Motion to Exclude Expert Testimony of Gary Olsen and Mary Frantz filed concurrently herewith, Frantz's opinions on this subject are unreliable and should be excluded. If they are, Plaintiffs have no other evidence that their Social Security numbers were available on the deep and dark web.

***errors in processing her medical bills, and that a four-year magazine subscription was started in her name."*** Plaintiff Nielsen cannot tie the alleged identity theft (or bank accounts, credit score hit, or bill processing errors) to Mednax because [redacted] *See* Section III.A.2.iv, *supra*.

- ***"Plaintiffs allege that considering the geographic distribution of Plaintiffs and the inclusion of multiple Plaintiffs' PHI and PII in one sample database, it can be reasonably assumed that the data likely came from the same source data breach."*** This allegation was based upon a premise discovery has proven false—that multiple Plaintiffs information was in "one" database. [redacted] And it is undisputed that Mednax did not possess the Social Security numbers of any of the individuals who made the dark web allegations in the Complaint.
- ***"Plaintiffs allege that they exercise care in sharing their sensitive PHI and PII, do not knowingly transmit unencrypted sensitive PHI and PII over the internet or any other unsecured source, and store any documents containing their sensitive PHI and PII in a safe and secure location or destroy the documents."*** This allegation, as it turns out, is also objectively false. For example, Defendants' expert Keith Wojcieszek completed a search on open websites (like social media) for PHI and PII and found numerous instances where Plaintiffs had publicly posted their personal information. SOMF ¶ 209. [redacted] *Id.* ¶ 90. [redacted] *Id.* ¶¶ 32, 33.[32] Simply put, the evidence contradicts Plaintiffs'

[32] The list goes on. [redacted] SOMF ¶ 187. [redacted] *Id.* ¶ 188. [redacted]

allegations that they were so cautious in sharing their PHI and PII that the Cyberattack must have been the source of their harm. [redacted] *Id.* ¶ 210. And one Plaintiff, Lee, has filed a total of three data breach lawsuits (including this one), seeking to recover for the same alleged injuries in all three distinct cases. [redacted] *Id.* ¶¶ 169-170.

In short, while Plaintiffs' allegations were given the benefit of a presumption of truth at the motion to dismiss phase, they can no longer rely on assumptions and speculation to survive summary judgment. The fact is that Plaintiffs have not suffered any legally cognizable harm and, even if they had identified some type of harm, it is factually impossible to connect that to Mednax. Mednax is therefore entitled to summary judgment on Plaintiffs' negligence claim.

## IV. CONCLUSION

For the reasons set forth above, Plaintiffs lack Article III standing and the undisputed record evidence demonstrates that Plaintiffs' claims all fail on the merits. Thus, summary judgment should be granted in Mednax's favor.

Dated: November 29, 2023

*/s/ Kristine McAlister Brown*

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

---

[redacted] *Id.* ¶ 173. [redacted]

*Id.* ¶ 116.

*Id.* ¶ 98.

[redacted] *Id.* ¶ 102.

Martin B. Goldberg
Florida Bar No. 827029
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

*Attorneys for Defendants Mednax, Inc.; Mednax Services, Inc.; Pediatrix Medical Group; and Pediatrix Medical Group of Kansas, P.C.*

**CERTIFICATE OF SERVICE**

I hereby certify that on November 29, 2023, I electronically filed the foregoing document with the Clerk of Court using the CM/ECF system, which will send notice of electronic filing to all counsel of record.

*/s/ Kristine McAlister Brown*
Kristine McAlister Brown