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

MEDNAX'S REPLY BRIEF IN SUPPORT OF ITS
MOTION FOR SUMMARY JUDGMENT

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

CASES

RULES

STATUTES

INTRODUCTION

Despite extensive discovery, Plaintiffs have been unable to muster any evidence to support their case.[1] With no evidence, Plaintiffs mischaracterize binding Eleventh Circuit precedent and attempt to impugn the investigation that Charles River Associates ("CRA") conducted into the Cyberattack. But Plaintiffs' attacks on CRA's investigation—which they repeat over and over again to try to conceal their evidentiary failures—amount to nothing more than mere speculation that the threat actor who perpetrated the Cyberattack ***might*** have gained access to other parts of Mednax's environment and that those other parts of Mednax's environment that ***might*** have been accessed ***might*** have contained other types of personal information for Plaintiffs that ***might*** have then been used to cause the alleged harms Plaintiffs claim they experienced.[2]

To be absolutely clear, Plaintiffs' speculation is disproven by the undisputed evidence. The corporate representative of CRA testified unequivocally that CRA [redacted] Defendants' Joint Statement of Material Facts ("Defs.' SOMF") Ex. 12 (Mathews Dep.) at 266:7-267:4; *see also* Defs.' SOMF ¶¶ 8–16. But even setting that aside, Plaintiffs' pure speculation does not demonstrate a "genuine issue as to any material fact." Fed. R. Civ. P. 56(c). As the Eleventh Circuit has explained, "[f]or factual issues to be considered genuine, they must have a real basis in the record." *Ellis v. England*, 432 F.3d 1321, 1326 (11th Cir. 2005) (internal quotation marks omitted).

---

[1] Plaintiffs' Response to Mednax's Statement of Undisputed Facts violates Local Rule 56.1(b)(2)(C) by not including evidentiary citations to support Plaintiffs' assertion that certain facts are disputed. *See* ECF No. 282 ¶¶ 35, 199, 200, 205, 207. Mednax's facts in the paragraphs that correspond to those improper responses should be deemed admitted. S.D. Fla. L.R. 56.1(c).

[2] Notably, Plaintiffs rely heavily on CRA's investigation in arguing that they can satisfy Rule 23's requirements for class certification. Plaintiffs argue that their proposed class is ascertainable because it is "easily identified through Defendants' records of current and former patients and individuals whose PHI and PII was compromised, each of whom was notified" of the Cyberattack. ECF No. 232 at 6. Those records were generated from the investigation. Plaintiffs also relied on the investigation's conclusions about the number of individuals whose information was potentially compromised to argue that Rule 23(a)'s numerosity requirement is satisfied. *See id.* at 7 n.19. And Plaintiffs rely on Gary Olsen's report to support their predominance argument, and assert that his methodology is appropriate because it "is based on the categories of PII and PHI that were actually exposed for each individual Plaintiff or Class Member"—categories that were determined by the investigation that Plaintiffs criticize in their response. *Id.* at 15. Plaintiffs cannot have it both ways, relying on CRA's investigation when it suits them but discarding it when it doesn't.

As discussed in Mednax's motion and below, Plaintiffs have not shown that there is a "real basis in the record" to support either Article III standing or their substantive claims. Thus, Mednax is entitled to summary judgment.

ARGUMENT AND CITATION TO AUTHORITIES

I. Plaintiffs Lack Article III Standing.

As discussed below, Plaintiffs have identified no "basis in the record" to support their position that they have suffered any legally cognizable injuries that are fairly traceable to the Cyberattack. *See Ellis*, 432 F.3d at 1326. Plaintiffs therefore lack Article III standing and their claims must be dismissed.

A. Plaintiffs Misconstrue the Eleventh Circuit's *Green-Cooper* Decision.

Plaintiffs argue that, under the Eleventh Circuit's recent decision in *Green-Cooper v. Brinker Int'l, Inc.*, 73 F. 4th 883 (11th Cir. 2023), they must only show that their personal information was actually accessed in the Cyberattack to have Article III standing to sue. Opp. at 3. But Plaintiffs' position flies in the face of the Eleventh Circuit's unequivocal statement that the Court "require[s] misuse of the data cybercriminals acquire from a data breach" to satisfy Article III's injury-in-fact requirement, and that access alone is not enough. *Id.* at 889. In *Green-Cooper*, the district court had certified a class of individuals "who: (1) had their data accessed by cybercriminals and, (2) incurred reasonable expenses or time spent in mitigation of the consequences of the Data Breach." *Id.* at 892. The Eleventh Circuit reserved and remanded with instructions that the district court "clarify its predominance finding" to either "refine the class definitions to include only" individuals who had experienced actual misuse of their data (i.e., had experienced fraudulent charges or had their credit card information posted to the dark web), or to "conduct a predominance analysis anew under Rule 23 with the existing class definitions based on the understanding that the class definitions as they now stand may include uninjured individuals . . . who have simply had their data accessed by cybercriminals and canceled their cards as a result." *Id.* Notably, the Eleventh Circuit held that individuals who merely had their information "accessed" were "uninjured." *Id.*

Plaintiffs suggest that the Court should ignore this unequivocal language in *Green-Cooper*, and that "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." Opp. at 3. But nothing in *Green-Cooper* limits its analysis to a particular type of data. Indeed, other courts have applied *Green-Cooper* to incidents involving the exposure of immutable data elements like Social Security numbers. *See, e.g.*, *Ruskiewicz v. Okla. City Univ.*, 2023 WL 6471716, at *3 (W.D. Okla. Oct. 4, 2023) (dismissing complaint for lack of Article III standing where plaintiff "does

not allege any facts that might suggest a misuse of her personal information from OCU's data breach has occurred").

B. Even if Actual Access Were Sufficient to Confer Article III Standing, Plaintiffs Have No Evidence Their Information Was Actually Accessed in the Cyberattack.

Even if mere access to Plaintiffs' information were sufficient to confer standing to sue (and it is not), Mednax would still be entitled to summary judgment because Plaintiffs have not offered any evidence that their personal information was actually accessed in the Cyberattack. Plaintiffs rely only on evidence showing that certain Office365 email accounts were involved in the Cyberattack. *See* Opp. at 7. But they have no evidence that ***their personal information*** that was contained in those accounts was actually accessed by the threat actor. *See* Mot. at Section III.A.1. This is insufficient. *Cf. Green-Cooper*, 73 F.4th at 890 (no Article III standing where plaintiff failed to allege he dined at restaurant during the time *that* restaurant "was compromised in the data breach").[3]

C. No Plaintiff Has Demonstrated Actual Misuse of Their Data that Is Fairly Traceable to the Cyberattack.

1. Several Plaintiffs Have Conceded Their Information Was Not Misused.

Plaintiffs do not respond to Mednax's argument that Plaintiffs Bean, Jay, Soto, Baum, and Clark have no evidence that any of their children's personal information has been misused as a result of the Cyberattack. *See* Mot. at Section III.A.2.i. Plaintiffs also do not respond to Mednax's argument that Larsen has no evidence that his own information was misused as a result of the Cyberattack. *See id.* Indeed, four of these Plaintiffs withdrew their allegations that their Social Security numbers were involved in the Cyberattack after Mednax threatened to move for sanctions.[4] These Plaintiffs' claims must be dismissed because this Court lacks Article III standing over their claims.

---

[3] Plaintiffs' assertion that misuse of some individuals' data is sufficient to establish a substantial risk of future injury for all class members does not help them because, as discussed in Mednax's opening brief and below, there is no evidence that any person's information was misused as a result of the Cyberattack. *See* Section I.C., *infra*. And even if Plaintiffs could muster such evidence, "in a suit for damages, the mere risk of future harm, standing alone, cannot qualify as a concrete harm." *TransUnion LLC v. Ramirez*, 594 U.S. 413, 436 (2021).

[4] Despite this, Plaintiffs state in their Statement of Additional Facts that [redacted] and attribute this to the Cyberattack, including in their count those Plaintiffs who have withdrawn their Social Security number allegations. Plaintiffs' Resp. to Mednax's SOMF ("Pls.' SOMF") ¶ 239; *see also* ECF No. 222. Plaintiffs are wrong. [redacted] Defs.' SOMF Ex. 3 at Ex. E, pp. 6, 9, 10, 13, 22, 24, 25, 28, 29. For those individuals who have withdrawn their allegations, [redacted]

2. Mednax Did Not Possess the Social Security Numbers Plaintiffs Allegedly Found on the Dark Web.

Plaintiffs also do not cite any evidence that Mednax ever possessed A.W., B.W., A.L., Lee, or A.H.'s Social Security numbers.[5] They try to sidestep their shortcoming by arguing that Mednax's evidence that it did not have these individuals' Social Security numbers "was the result of a curated and purposefully incomplete investigation." Opp. at 4. Plaintiffs are wrong. In assessing whether Mednax possessed these individuals' Social Security numbers, Mednax did not confine its search to the documents in the e-mail boxes that it determined were involved in the Cyberattack. Instead, Mednax searched five different patient information systems—OBR, BabySteps, iNewborn, OnBase, and GPMS—to assess whether it had these individuals' Social Security numbers anywhere in its possession, even though none of these systems was impacted in the Cyberattack. *See* ECF. No. 84-1 ¶¶ 7-8, 11, 12. Mednax attached to its statement of material facts screenshots from its patient information systems demonstrating that these individuals' Social Security numbers were not present. Defs' SOMF ¶¶ 24 (A.W), 25 (B.W.), 121 (A.L.), 161 (Lee), 179 (A.H.) & Exs. 23, 48, 62, 70. Mednax also searched for hospital facesheets associated with these individuals, because Mednax sometimes has hospital facesheets, which could possibly contain Social Security numbers depending upon the particular hospital, and located none. ECF. No. 84-1 ¶ 10. Thus, this Court need not determine whether Mednax's investigation into the Cyberattack was thorough in order to reject Plaintiffs' argument, because "[i]f Mednax were in possession of a patient or guarantor's Social Security number, that Social Security number would be in one (or more) of the locations referenced above." ECF. No.

[redacted] Ex. 3, Frantz Report at Ex. E at 24 (emphasis added). After learning that Plaintiffs [redacted] in the Second Amended Complaint, Mednax served Plaintiffs with a motion for sanctions under Rule 11 in June 2023. *See* Ex. A, Mednax's Motion for Sanctions with Cover Letter to Plaintiffs. In response to Mednax's motion for sanctions, Plaintiffs agreed to withdraw their allegations that B.J., M.S., A.B., Larsen, and Clark's three children (J.C., J.C., and E.M.)'s SSNs were available on the dark web as a result of the Cyberattack. *See* ECF 222. Thus, Plaintiffs' attempt to present evidence to support allegations they previously conceded were unsupportable is improper. *See Rowden v. Target Corp.*, 2021 WL 2554047, at *4 (M.D. Fla. June 22, 2021) (concluding that plaintiff "failed to raise a genuine issue of material fact" in part because he "withdrew his allegation" about why the defendant "failed to maintain its premises in a reasonably safe manner").

[5] Plaintiffs blatantly misrepresent Cohen's deposition testimony in footnote 2 of their response. Cohen testified that [redacted] Defs' SOMF Ex. 68, Cohen Dep. at 92:23-24.

84-1 ¶ 14. It was not, and thus "Mednax is not in possession of those individuals' Social Security numbers at all." *Id.*

3. Plaintiffs' Alleged Evidence of Other Misuse Is Not Fairly Traceable to the Cyberattack.

Mednax demonstrated in its motion that it never possessed the email address at which Plaintiff Rumely contends he received spam messages. Plaintiffs offer no response and fall far short of satisfying their burden of demonstrating there is "sufficient evidence favoring the nonmoving party for a jury to return a verdict for that party." *Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 249 (1986). Accordingly, Rumely's claims must be dismissed for lack of standing.

In response to Mednax's argument that Plaintiffs Lee and Nielsen's allegations of spam calls, text messages, and mail, and Nielsen's allegations of unauthorized accounts being opened in her name could not have been caused by the Cyberattack because the information necessary to cause those harms was not involved in the Cyberattack, Plaintiffs attempt to create a disputed issue of fact by relying on [redacted]. According to Plaintiffs, it is ***possible*** that the threat actor could have accessed other parts of Mednax's network that ***might*** have contained the additional information about Lee and Nielsen that would have been required to cause these alleged harms. Opp. at 4-5. But "expert testimony indicating the 'mere possibility' of causation is . . . insufficient" to survive summary judgment. *Alvarez v. Allergan Sales, LLC*, 2021 WL 6061730, at *4 (M.D. Fla. Dec. 9, 2021) (quoting *Guinn v. AstraZeneca Pharms. LP*, 602 F.3d 1245, 1256 (11th Cir. 2010)). That is all that Frantz has offered. Indeed, when pressed at her deposition, Frantz acknowledged that [redacted] ECF No. 252-13 (Frantz Rebuttal Dep.) at 47:24-53:7. This "speculative and equivocal" testimony is insufficient to create a genuine issue of disputed material fact on whether Plaintiffs' alleged allegations of misuse are fairly traceable to the Cyberattack. *Arevalo v. Mentor Worldwide LLC*, 2022 WL 16753646 (11th Cir. Nov. 8, 2022); *see Marshall v. City of Cape Coral*, 797 F.2d 1555, 1559 (11th Cir. 1986) ("All reasonable inferences arising from the evidence must be resolved in favor of the non-movant, but inferences based upon speculation are not reasonable."); *Walker v. CSX Transp. Inc.*, 650 F.3d 1392, 1401 (11th Cir. 2011) (affirming grant of summary judgment where "[t]o rule otherwise would require us to unreasonably draw unsupported inferences as to how Defendants' [conduct] could have caused" Plaintiffs' injuries).

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

Plaintiffs also cannot establish Article III standing based on allegations of emotional distress, mitigation measures they took after the Cyberattack, an alleged loss of privacy, or an alleged diminution in value of their personal information.

1. Plaintiffs' Alleged Emotional Distress, Mitigation Measures, and Loss of Privacy Are Insufficient Because There Is No Imminent Risk of Future Harm.

Plaintiffs do not address Mednax's argument that emotional distress alone is insufficient to satisfy Article III's injury-in-fact requirement and that it only suffices where it is "coupled with the substantial risk of future harm" as a result of the Cyberattack. ECF No. 104 at 15. Similarly, Plaintiffs do not contest that steps taken to mitigate a risk of future harm are only sufficient to confer Article III standing where the risk of future harm is "substantial or certainly impending." *Id.* at 11-12. Nor do they contest that an alleged loss of privacy is insufficient to confer Article III standing where there is no "substantial and imminent risk of future identity theft."[6] *Id.* at 17.

Though Plaintiffs concede a substantial risk of future harm is required to demonstrate an injury-in-fact based on emotional distress, mitigation measures and a loss of privacy, Plaintiffs have offered no evidence to demonstrate that they are facing a substantial risk of future harm as a result of the Cyberattack. Under binding Eleventh Circuit precedent, to establish a substantial risk of future harm, a plaintiff must offer "specific evidence of *some* misuse of class members' data." *Tsao*, 986 F.3d at 1344. Even though now more than three years have passed since the Cyberattack, Plaintiffs point to no evidence that either their personal information or the personal information of any putative class members has been misused as a result of the Cyberattack. There is therefore not a substantial risk of future harm. *See id.* Accordingly, Plaintiffs' evidence that they suffered emotional distress or took mitigation measures as a result of the incident does not create a disputed issue of material fact on the issue of Article III standing.

Even if Plaintiffs had established a substantial risk of future harm that would allow them to recover for these types of alleged injuries (and they have not), Plaintiffs' argument that the parents who are bringing claims on behalf of their minor children can rely on their own emotional distress "as the caretakers of [their] minor[]" children fails for an independent reason. Opp. at 8. The adults Plaintiffs contend experienced emotional distress in their response all confirmed that they were only

[6] Allowing an alleged loss of privacy, without more, to confer Article III standing would contravene the Eleventh Circuit's admonition that "[e]vidence of a mere data breach does not . . . satisfy the requirements of Article III standing." *Tsao v. Captiva MVP Rest. Partners, LLC*, 986 F.3d 1332, 1344 (11th Cir. 2021).

bringing claims on behalf of their children, not on their own behalf. *See* Defs.' SOMF ¶¶ 20 (B.W.), 34 (Rumely), 59 (Bean), 71 (Jay), 117 (Larsen), 175 (Cohen), 189 (Clark). Moreover, Plaintiffs cite only a single Middle District of Florida decision to support their argument, but that case actually undermines Plaintiffs' position. There, the court granted the defendant's motion to dismiss on the plaintiffs' negligent infliction of emotional distress claim because the minor children had not "allege[d] any specific discernible physical manifestations of their emotional distress." *Gonzalez-Gonzalez-Jimenez de Ruiz v. United States*, 231 F. Supp. 2d 1187, 1201 (M.D. Fla. 2002). In other words, Plaintiffs' own authority confirms that it is the emotional distress of the children, and not the parents who are bringing claims on their behalf, that matters. Plaintiffs offer no evidence that any of their children suffered emotional distress as a result of the Cyberattack, which is an independent reason that precludes them from relying on alleged emotional distress to establish Article III standing.

2. Plaintiffs' Allegations of Diminution in Value Depend on Their Information Being Accessed and There Is No Evidence of Actual Access.

Plaintiffs' final attempt to establish Article III standing is based on the alleged decrease in value of their PII and PHI. But Plaintiffs do not respond to Mednax's argument that this theory of Article III standing is foreclosed by the Eleventh Circuit's *Green-Cooper* decision. *See* Mot. at 13. Even if *Green-Cooper* did not foreclose this theory of standing, however, Plaintiffs have not offered any evidence to demonstrate that their PHI or PII has decreased in value because, as discussed above, they have not offered any evidence that the threat actor actually accessed their PHI or PII. This is fatal to Plaintiffs' argument because, as Mednax explained in its motion, Plaintiffs' own expert acknowledged that [redacted] ECF No. 252-1, Ex. 4 (Olsen Dep.) at 59:22-24 [redacted]; *see also* Defs.' SOMF Ex. 15 ¶ 68. Plaintiffs make a slightly different argument in their response brief, arguing that the alleged diminution in value of their PHI and PII is one of "the effects of both being stolen." Opp. at 9. But whether it is the access to or the theft of the information that leads to the decrease in its value, Plaintiffs cannot survive summary judgment on this theory because they have offered evidence of neither. The undisputed record evidence confirms that Mednax's "investigation could not determine if the files [in the mailboxes of impacted users] were accessed or not." Pls.' Opp. SOMF ¶ 11. And there was similarly no evidence of exfiltration of any information from Mednax's systems. Defs.' SOMF Ex. 5, Miller Dep. at 65:2-17.

Plaintiffs also implicitly acknowledge that the only individual who even argues that her participation in the marketplace of credit was affected in any way by the Cyberattack—which is what this Court said was required to establish this theory—is Plaintiff Nielsen. *See* ECF No. 104 at 17. But Nielsen has no answer to the complete lack of evidence to support her allegation that her credit score decreased because of the Cyberattack. She argues only that "after the Data Breach, [she] experienced a reduction in her credit score" because [redacted] Opp. at 10. But "a mere temporal connection is not sufficient." *Resnick v. AvMed, Inc.*, 693 F.3d 1317, 1327 (11th Cir. 2012). Nielsen cites no evidence to support her assertion that [redacted] had anything to do with the Cyberattack, and doesn't even attempt to explain how those two things are logically connected. This does not even come close to satisfying Plaintiffs' burden on summary judgment.

II. Plaintiffs Fail to Show that a Genuine Issue of Material Fact Exists on Any of Their Substantive Claims.

A. Mednax Is Entitled to Summary Judgment on Plaintiff Cohen's Maryland Consumer Protection Act ("MCPA") Claim.

Plaintiffs' response fails to demonstrate a genuine issue of material fact on any of the three elements of an MCPA claim. Mednax demonstrated in its motion that Cohen cannot establish the first element of an MCPA claim, which requires proof of a misrepresentation or omission, because she acknowledged that Mednax never made any representations to her about data security or the protection of patient information. Mot. at 16. In response, Plaintiffs rely on a privacy notice from Mednax's website. But they fail to present any evidence that Plaintiff Cohen received, viewed, read, or even knew about this privacy notice. Nor can they, as Cohen directly contradicted Plaintiffs' argument by confirming that [redacted] Defs.' SOMF ¶ 183 & Ex. 68, Cohen Dep. at 176:12–177:3. The undisputed evidence therefore demonstrates that Mednax did not make a material misrepresentation or omission to Cohen.

Mednax also demonstrated that there was no disputed issue of material fact on the issue of reliance because Cohen admitted to [redacted] Mot. at 16. In response, Plaintiffs argue that Cohen need only demonstrate that Mednax's representations "'substantially induced' her choice." Opp. at 12 (quoting *Allen v. Bank of Am., N.A.*, 822 F. Supp. 2d 505, 532 (D. Md.2013)). But Plaintiffs fail to present any evidence that Mednax's alleged representations about its data security played ***any*** role whatsoever in Cohen's decision to select a medical provider, let alone

that it was a substantial factor in her choice. Mednax is entitled to summary judgment on Cohen's MCPA claim for this reason, too. *See Tucker v. Am. Residential Servs., LLC*, 2018 WL 1471683, at *6 (D. Md. Mar. 26, 2018) (MCPA claim fails at summary judgment where no evidence of reliance).

Finally, Mednax showed in its motion that it was entitled to summary judgment because Cohen has not shown that she has "spent or lost" any money "as a result of . . . her reliance on [any] misrepresentations," as required under Maryland law. *Barnhill v. A&M Homebuyers, Inc.*, 2022 WL 3586448, at *6 (D. Md. Aug. 22, 2022). Plaintiffs do not dispute that Cohen did not spend or lose any money. They instead argue that Cohen has suffered emotional distress and has spent time mitigating the effects of the Cyberattack. Opp. at 13. But Cohen cites no authority to support her novel argument that lost time qualifies as actual damage under the MCPA and cannot recover for her alleged emotional distress because she has no evidence that it is "accompanied by a physical injury." *Wheeling v. Selene Finance LP*, 250 A.3d 197, 222 (Md. 2021).

B. Mednax Is Entitled to Summary Judgment on Plaintiff Larsen's Arizona Consumer Fraud Act ("ACFA") Claim.

Plaintiff Larsen also cannot survive summary judgment on his ACFA claim. As Mednax demonstrated in its motion, the ACFA, like the MCPA, requires Plaintiffs to prove Mednax made a misrepresentation or a material omission. Mot. at 17. Plaintiffs argue in their response that Mednax has concealed unidentified "material information from Plaintiffs," Opp. at 13, and suggest that because Larsen could not recall any representations about its data security they must have been inadequate. *Id.* at 13-14. It is black-letter law, however, that "lack of memory is insufficient to create a genuine dispute of fact." *See, e.g., Larsen v. Citibank FSB*, 871 F.3d 1295, 1308 (11th Cir. 2017). Because Larsen identifies no evidence of any representations or omissions, he has not established a genuine issue of material fact on this required element of his ACFA claim.

Mednax also demonstrated that Larsen could not show that he relied on any representations Mednax allegedly made about its data security because he acknowledged at his deposition that [redacted] Mot. at 17. In response, Larsen argues that [redacted]. Opp. at 14. This proves Mednax's point—data security was not a factor in Larsen's decision about where to take

his children for medical care. Moreover, Larsen admitted that [redacted] Defs' SOMF ¶ 125 & Ex. 46, Larsen Dep. at 196:25-197:2.[7]

C. Plaintiff Rumely's California Consumer Records Act ("CCRA") Claim Fails.

To survive summary judgment on the CCRA claim, Plaintiff Rumely must point to some evidence that he was injured *as a result of* Mednax's alleged delay in sending notice of the Cyberattack. Mot. at 17-18 (citing authorities). Rumely has not done so. He attempts to rely only on arguments about why he was injured by the Cyberattack itself. Opp. at 15-16. Because Rumely "has failed to trace any harm from [Mednax's allegedly] delayed notification," Mednax is entitled to summary judgment on this claim. *Dugas v. Starwood Hotels & Resorts Worldwide, Inc.*, 2016 WL 6523428, at *7 (S.D. Cal. Nov. 3, 2016).

D. Mednax Is Entitled to Summary Judgment on Plaintiff Rumely's Confidentiality of Medical Information Act ("CMIA") Claim.

Mednax demonstrated in its motion that Plaintiff Rumely's CMIA claim fails because that claim—as alleged in the operative Complaint—is expressly predicated on the alleged "release of individually identifiable medical information pertaining to Plaintiff Rumely." ECF No. 115 ¶ 599; *see also id.* ¶ 598 (alleging that Rumely is a patient under the CMIA), 601 ("Plaintiff Rumely's . . . unencrypted personal information was viewed by unauthorized persons . . . ."). In response, Plaintiffs rely only on generalized allegations from other parts of the Complaint—not the CMIA claim—to argue that "[it] cannot be any clearer" that Rumely is asserting claims on his children's behalf. Opp. at 17. This is insufficient. *Swint v. City of Carrollton*, 859 F. App'x 395, 399 (11th Cir. 2021) ("passing references" that are not included in one of the counts of the complaint are insufficient).

Even setting Plaintiffs' pleading failure aside, Rumely's CMIA claim fails because he has no evidence that his (or his children's) information was actually viewed. Mot. at 19-21. Plaintiffs concede that Rumely has no such evidence, and once again resort to speculation that [redacted]

[7] Plaintiffs mischaracterize *Peery v. Hansen*, 585 P.2d 574, 578 (Ariz. Ct. App. 1978) in arguing that disgorgement is an available remedy under the ACFA. It is not. *Peery* held that a "private individual's relief under the [ACFA] is limited to the recovery of *actual damages* suffered as a result of such unlawful act or practice" and that the "civil penalties" (including disgorgement) provided by the statute are only available to the state. 585 P.2d at 578 (emphasis added); *see also* A.R.S. § 44-1528(A)(3) (disgorged funds shall be "paid to the state for deposit in the consumer remediation subaccount. . ."). Plaintiffs have not cited a single example of a court awarding a private plaintiff disgorgement under the ACFA. And doing so would contradict the plain language of the Act, which only provides for disgorgement following an investigation by the attorney general. A.R.S. § 44-1528.

[redacted] Mot. at 17. As discussed above, Plaintiffs' speculation does not create a genuine issue of material fact. *See* Section I.C.3, *supra*. And Plaintiffs' unsupported statement that Mednax [redacted] Opp. at 17, is contradicted by the deposition testimony of the corporate designee of CRA, who stated [redacted] Defs' SOMF Ex. 12 at 264:8-265:6.

E. Plaintiff Jay's Washington Consumer Protection Act ("WCPA") Claim Fails.

As discussed in the Motion, 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 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). Mednax demonstrated conclusively the lack of evidence as to (1) any unfair or deceptive act; (2) injury to business or property; and (3) causation. Any one of these failures is fatal to Jay's claim.

In response to Mednax's first argument that there is no evidence to support Jay's assertion that Mednax committed an unfair or deceptive act, Plaintiffs' only response is to argue that there is a "mountain of evidence." Opp. at 18. Tellingly, however, Plaintiffs do not cite a shred of evidence that purportedly makes up this "mountain." Plaintiffs' hyperbole is no substitute for the "affirmative evidence" that is required to demonstrate a disputed issue of fact on summary judgment. *Porter v. Ray*, 461 F.3d 1315, 1320 (11th Cir. 2006).

Second, on the injury to property requirement, Plaintiffs argue they have "sufficient evidence to show that [redacted]," relying on Frantz's conclusion that [redacted] As discussed above, however, Plaintiffs have withdrawn their allegations that B.J.'s Social Security number was involved in the Cyberattack [redacted]. ECF No. 222; Ex. A (Mot. for Sanctions) at 3; *see* note 4, *supra*. Plaintiffs therefore cannot use this alleged evidence to create a disputed issue of material fact.

Third, Plaintiffs rely on Washington's rebuttable presumption of reliance to argue that there is a disputed issue of material fact on that element of Jay's WCPA clam. Opp. at 18. But Plaintiffs ignore the fact that Mednax has offered evidence to rebut the presumption of reliance, in the form of Jay's own testimony under oath that [redacted]

[redacted] Defs.' SOMF ¶ 80 & Ex. 37, Jay Dep. at 172:22–173:11. Plaintiffs attempt to avoid this clear testimony by suggesting Jay was [redacted] Opp. at 18. Not so. Jay testified that [redacted] Ex. 37, Jay Dep. at 171:1-7; *see also* Defs.' SOMF ¶ 77. [redacted] Given these undisputed facts, "[n]o reasonable factfinder could find that [her] decisions would have been affected" even if Mednax made any cybersecurity representations. *G.G.*, 579 F. Supp. 3d at 1235. Thus, Mednax is entitled to summary judgment on Jay's WCPA claim.

F. Plaintiffs Are Not Entitled to Injunctive Relief Under FDUTPA.

Plaintiffs acknowledge that, to be entitled to injunctive relief under FDUTPA, they must demonstrate that they are facing an "actual or imminent threat" of future harm. *Calderon v. SIXT Rent A Car, LLC*, 2022 WL 4355761, at *6 (S.D. Fla. Sept. 20, 2022). Mednax demonstrated in its Motion that Plaintiffs have no evidence to support such a finding. Mot. at 24. Plaintiffs' only response is to cite to a smattering of paragraphs from Mary Frantz's report. Opp. at 20. But the paragraphs Plaintiffs cite do not suggest that Plaintiffs' data is at risk of another data breach. To the contrary, Frantz acknowledges in her report that [redacted]. Defs' SOMF Ex. 3, Frantz Rep. ¶ 242. At best, the statements from Frantz's report that Plaintiffs cite demonstrate that Mednax "faces much the same risk of future cyberhacking as virtually every other holder of private data." *Webb v. Injured Workers Pharmacy, LLC*, 72 F.4th 365, 378 (1st Cir. 2023). As the First Circuit recently explained, "[i]f that risk were deemed sufficiently imminent to justify injunctive relief, virtually every company and government agency might be exposed to requests for injunctive relief like the one the plaintiffs seek here." *Id.* Mednax is entitled to summary judgment on Plaintiffs' FDUTPA claim.

G. Plaintiffs' Negligence Claim Fails.

i. Plaintiffs' Claims Are Governed By a Multitude of State Laws.

Mednax showed in its motion that, even though this Court applied Florida negligence law to all Plaintiffs' claims when deciding Defendants' motion to dismiss, intervening case law and facts developed in discovery now demonstrate that each Plaintiffs' negligence claim is governed by his or her home state's laws. Mot. at 25-27.

As Mednax explained in its motion, the Eleventh Circuit's *Green-Cooper* decision confirms that plaintiffs in a data breach case are injured, if at all, when their data is misused. This is directly relevant to the first factor of Florida's choice-of-law test, which examines the place where the injury occurred. Mot. at 26. Plaintiffs respond by arguing that *Green-Cooper* did not change what a plaintiff must establish to satisfy Article III's injury-in-fact requirement because older cases had also examined whether misuse had occurred in assessing whether a plaintiff had established a legally cognizable injury in fact. Opp. at 21. But Plaintiffs miss the point, which is that in its prior choice-of-law analysis, this Court assumed that the place of the injury was the place where the Cyberattack occurred, which the Complaint alleged was Florida. ECF No. 104 at 7-8. *Green-Cooper* confirms, however, that a data breach alone is not an injury, and that an injury does not occur unless and until, "as a result of the breach, [a plaintiff] experiences 'misuse' of his data in some way." 73 F.4th at 889. This holding directly impacts this Court's prior analysis of first factor of Florida's choice-of-law test by requiring the Court to look to the place where each Plaintiff has experienced misuse of the data, which has occurred, if at all, in the Plaintiffs' home state. *See* Mot. at 26.

Mednax also explained that the allegations about the location of the Cyberattack that the Court credited about where Plaintiffs' data was maintained and where Mednax's security protocols allegedly broke down were proven false in discovery. Plaintiffs respond by arguing that Florida "was the hub [redacted] Opp. at 21. But Plaintiffs don't explain how [redacted] They do not argue that the Cyberattack was caused by the failure to implement any policies or procedures, nor do they argue that it was caused by a lack of monitoring. As Plaintiffs are well aware, and as the undisputed record evidence confirms, the Cyberattack began [redacted] Defs.' SOMF ¶¶ 6, 9, 13. Thus, Plaintiffs' arguments do not support the application of Florida law.

ii. Mednax Had no Duty to Protect Plaintiffs' PII/PHI from Third-Party Criminal Conduct.

Plaintiffs string cite to various cases in each Plaintiff's home state in an effort to persuade this Court that Mednax had a duty to protect Plaintiffs' PII/PHI from criminal acts of third parties. But a closer look at each case makes clear that Plaintiffs have either misstated the cases they cite or the cases are readily distinguishable. For example, Plaintiffs cite *Krefting v. Kaye-Smith Enterprises, Inc.*, 2023

WL 4846850, at *4 (W.D. Wash. July 28, 2023) to argue that Mednax had a duty to protect B.J.'s personal information from a third-party criminal Cyberattack, but that case is distinguishable because it involved an "affirmative act" that "creates a recognizable high degree of risk of harm." Plaintiffs here identify no such affirmative act. Plaintiffs' reliance on *In re Marriott Int'l, Inc., Customer Data Sec. Breach Litig.*, 2020 WL 6290670 (D. Md. Oct. 27, 2020), is similarly misplaced. In *Marriott*, the Court found a duty because of statements the defendant had made in a contract and in public filings and based on allegations that the defendant owed a statutory duty under Section 5 of the FTC Act. *Id.* at 102-03. Here, Plaintiffs' allegation that "Defendants owed a duty" is not supported by any reference to a contract, a public statement, or a statute. ECF No. 115 ¶ 604. Plaintiffs also egregiously misrepresent *In re Banner Health Data Breach Litigation*, which has no absolutely no discussion of the duty element of a negligence claim. 2017 WL 6763549, at *8 (D. Ariz. Dec. 20, 2017). The same is true of Plaintiffs' Missouri case, which discusses only a negligence *per se* claim, and therefore has no duty discussion. *Baldwin v. Nat'l W. Life Ins. Co.*, 2021 WL 4206736, at *5 (W.D. Mo. Sep. 15, 2021). Finally, under Virginia law, plaintiffs erroneously rely on *In re Capital One Consumer Data Security Breach Litigation*. 488 F. Supp. 3d 374, 399 (E.D. Va. 2020). But that case found a duty based on allegations that Capital One "mined customer data for purposes of product development, targeted solicitation for new products, and target marketing of new partners—all in an effort to boost its profits." *Id.* Plaintiffs do not (and cannot) make similar arguments for Mednax.

iii. Plaintiffs' Claims Are Barred by the Economic Loss Rule.

Plaintiffs' economic loss rule case law fares no better. First, in Plaintiffs' South Carolina case, the court explicitly noted: "the court does not need to address the economic loss doctrine under South Carolina law in ruling on the instant motion." *In re Blackbaud, Inc.*, 567 F. Supp. 3d 667, 686 n.16 (D.S.C. 2021). That case therefore obviously has no application to the discussion here.

Plaintiffs also rely on *Mackey v. Belden, Inc.*, 2021 WL 3363174, at *7–8 (E.D. Mo. Aug. 3, 2021). But that case's entire negligence discussion, including its economic loss rule analysis, hinged on the special relationship between the parties recognized under Missouri law—the employer/employee relationship. *Id.* at *8. No special relationship under Missouri law exists here. *Id.* at *6 ("Special relationships which are recognized in Missouri include innkeeper-guest, common carrier-passenger, school-student, and sometimes employer-employee."). The same is true in Plaintiffs' California cases. *In re: Yahoo! Inc. Customer Data Sec. Breach Litig.*, 313 F. Supp. 3d 1113, 1133 (N.D. Cal. 2018) ("Plaintiffs have adequately pled a 'special relationship' with Defendants, so Plaintiffs' negligence and deceit by concealment claims are not barred by the economic-loss rule."). Finally, *In re Capital One* is

distinguishable for the same reasons as described above, which were also integral to that decision's economic loss rule analysis. 488 F. Supp. 3d at 397. Thus, the economic loss rule bars Rumely, B.W., Clark, Lee, Nielsen, and Soto's negligence claims under California, Missouri, South Carolina (for both Clark and Lee), Virginia, and Texas law. Mot. at 28-29.

iv. Plaintiffs Fail to Offer Evidence of Any Legally Cognizable Damages.

Mednax demonstrated in its opening brief that, regardless of which state's law applies to Plaintiffs' negligence claims, no Plaintiff has suffered any actual damage sufficient to support their negligence claims. Mot. at 29-31. In response, Plaintiffs address only the alleged disclosure of their PII/PHI and mitigation expenses. Opp. at 24-25. Both are insufficient to establish a genuine issue of material fact.

Plaintiffs state, without pointing to any evidence, that "their PHI and PII has been accessed and exfiltrated from Mednax's network." Opp. at 24. As discussed above, there is absolutely no evidence to support that conclusion—[redacted].

As to mitigation efforts, the cases Plaintiffs cite completely undermine their position. *See Purchnicki v. Envision Healthcare Corp.*, 439 F.Supp.3d 1226, 1244 (D. Nev. 2020) (lost time allegations are "not a cognizable injury sufficient to support the element of damages"); *Green v. eBay Inc.*, 2015 WL 2066531, at *5 (E.D. La. May 4, 2015) ("[M]itigation expenses do not qualify as injury-in-fact when the alleged harm is not imminent."). And Plaintiffs do not offer any evidence that they took any mitigation steps after the Cyberattack whatsoever.

v. There Is No Issue of Material Fact as to Causation.

Mednax explained in detail in its motion why each of the five allegations the Court previously determined could establish causation had been proven false in discovery. Mot. at 32-34. Plaintiffs ignore this detailed discussion and attempt to divert the Court's attention away from their complete lack of evidence by once again complaining about the alleged insufficiency of the investigation into the Cyberattack. This fails for all of the reasons set forth above.

CONCLUSION

For the reasons set forth in Mednax's motion and above, Plaintiffs lack Article III standing and the undisputed record evidence demonstrates that Plaintiffs' claims all fail on the merits. Mednax is entitled to summary judgment.

Dated: January 11, 2024

/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

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. and Mednax Services, Inc.

CERTIFICATE OF SERVICE

I hereby certify that on January 11, 2024, 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/ Kristine McAlister Brown
Kristine McAlister Brown
Florida Bar No. 443640

EXHIBIT A

(Filed under seal)