UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA

In re:

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

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

This Document Relates to All Actions

DEFENDANT AMERICAN ANESTHESIOLOGY, INC.'S
REPLY BRIEF IN SUPPORT OF ITS MOTION FOR SUMMARY JUDGMENT

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

Other Authorities

I. INTRODUCTION

Plaintiffs make three important concessions in their response: (1) no plaintiff pursues a Maryland Consumer Protection Act claim against American Anesthesiology, Inc. ("AA") (ECF No. 291 ("Opp.") at 10); (2) no plaintiff pursues a Florida Deceptive and Unfair Trade Practices Act claim against AA (*Id.*); and (3) Plaintiffs Baum, Bean, Clark, B.W., Cohen, Rumley, Soto, Jay and Larsen have no claims against American Anesthesiology, Inc. (*Id.* at 18); As such, the only claim remaining against AA in this action is a single count of negligence by Plaintiffs Brooke Nielsen and Gerald Lee.

To survive AA's motion for summary judgment, Plaintiffs Nielsen and Lee must introduce facts—not speculation—that sufficiently show the data in scope of the Cyberattack was actually misused to establish Article III standing and to create a factual dispute under their remaining negligence claim. They cannot. **Both Plaintiffs concede** [redacted]. *See* ECF Nos. 256 ("SOMF") ¶¶ 141, 161; 282 ("Resp. SOMF") ¶¶ 141, 161. They also admit that they have no other evidence linking any alleged misuse of their data to the Cyberattack. *See* SOMF ¶¶ 139, 145-146, 160, 166-168; Resp. SOMF ¶¶ 139, 145-146, 160, 166-168.[1]

In the face of this unwelcomed reality, Plaintiffs resort to a Hail Mary, baldly asserting that the data they claim to have been misused [redacted]. *See* Opp. at 5. This is rank speculation with no factual support. Plaintiffs offer no evidence that [redacted]. *See* SOMF ¶ 13. Plaintiffs cannot manufacture a factual dispute to overcome summary judgment. The established record is clear and undisputed: [redacted]. Summary judgment is due to be granted in favor of AA.

II. ARGUMENT

A. Plaintiffs concede that only the negligence claim filed by Brooke Nielsen and Gerald Lee remains against AA.

There is no dispute that the only claims remaining against AA are the negligence claims raised by Plaintiffs Nielsen and Lee. Opp. at 3 ("Only Plaintiffs Nielsen and Lee (the 'AA

[1] While Plaintiffs claim [redacted], *see* Opp. at 6, they offer no evidence supporting that allegation. *See* SOMF ¶ 203; Resp. SOMF ¶ 203.

Plaintiffs') pursue claims against AA in this action"); *Id*., at 10 ("Plaintiffs Lee and Nielsen do not allege MCPA claims"); *Id*. ("members of the subclass who were patients solely have no FDUTPA claims against AA"). As such, Counts I and IV should be dismissed against AA. Furthermore, all claims filed by Plaintiffs Baum, Bean, Clark, Cohen, Jay, Larsen, Rumely, Soto, and B.W. should be dismissed against AA.

B. Summary judgment is due on the remaining negligence claim.

1. The Eleventh Circuit has made clear that *actual use* of unlawfully accessed data is necessary to establish standing for a data breach claim, but neither Plaintiff can show that their data was accessed, much less actually used.

Unable to show any actual use of their data potentially exposed in the Cyberattack, Plaintiffs run fast and far from *Green-Cooper v. Brinker Int'l, Inc.*, 73 F. 4th 883 (11th Cir. 2023). Plaintiffs argue that *Brinker* is limited to credit card fraud, where any future risk can be avoided by canceling the card. They claim *Brinker* does not apply when personal data cannot be changed and that, in those cases, mere access is sufficient. *See* Opp. at 3. Plaintiffs misread *Brinker*. Regardless of the type of data, establishing concrete harm requires *actual use*. *Brinker* dealt with credit card data *and* other forms of personal data. *See Brinker*, 73 F.4th at 886, 889. Plaintiffs' "no future risk" distinction fails. *Brinker* applies equally to cases where any future threat cannot be abrogated. In both instances, the data must be *used* to cause a concrete injury. *Id.* at 889.[2]

In *Brinker*, the *actual sale* of the data on the web was "critical" to the analysis. *Id.* The Court held "that [the misuse of the data] is a concrete injury." *Id.* at 889–90. If data is merely "accessed," the individual is "uninjured." *Id.* at 892. Regardless of the type of data, actual misuse is required. Moreover, to show causation, the data allegedly taken must be the same data allegedly used. *See Resnick v. AvMed, Inc*., 693 F.3d 1317, 1327 (11th Cir. 2012) (finding a causal connection where the same data that was allegedly stolen was used to allegedly harm the plaintiff).[3]

[2] Although *Brinker* considered "access" versus "use" in terms of standing, 73 F.4th at 889, the same principles apply to a negligence claim. If actual use is necessary for traceability, it is certainly necessary to cross the much higher causation threshold to prevail on a negligence claim.

[3] Post *Brinker*, without actual use, the other "damages" Plaintiffs assert (emotional damages, mitigation measures, diminution in value, and loss of privacy), Opp. at 8–10, are all irrelevant. *See Brinker*, 73 F.4th at 887–891 (suggesting that cost and time spent monitoring credit is insufficient to establish harm without actual use of the data). *See also Baysal v. Midvale Indem. Co*., 78 F.4th 976, 978 (7th Cir. 2023), *reh'g denied*, 2023 WL 6144390 (7th Cir. Sept. 20, 2023) (finding that anxiety and worry are irrelevant unless the data is actually used, and that the Court would "need

i. Plaintiff Lee admits the data he claims was "used" to his detriment was not involved in the Cyberattack.

Plaintiff Lee concedes that [redacted]. SOMF ¶ 161; Resp. SOMF ¶ 161. Similarly, [redacted]. *Id*. Lee's data, however, [redacted]. SOMF ¶¶ 166–167.[4] [redacted]. Lee cannot establish Article III standing to pursue his claim.

ii. Plaintiff Nielsen cannot show that the data she claims was "used" to her detriment was exposed, much less accessed, in the Cyberattack.

The data that Plaintiff Nielsen alleges was misused [redacted]. *See* SOMF ¶ 141; Resp. SOMF ¶ 141. The data used to [redacted] must have come from another source.[5] Nielsen cannot show that any of the data allegedly "used" was exposed, much less accessed, in the Cyberattack. She cannot establish Article III standing to pursue her claim.[6]

2. Florida law does not govern the negligence claims of out-of-state Plaintiffs against AA.

---

an evidentiary hearing to learn whether [the data's use] contribute[d], to plaintiffs' detriment (and whether the [data] came from [the alleged breach] rather than some other source)").

[4] Lee claims he [redacted] Opp. at 6. [redacted]. *See* SOMF ¶ 166; Resp. SOMF ¶ 160.

[5] Nielsen alleges that the breach negatively impacted her credit. ECF No. 115 at ¶¶ 204-206. Her credit score, however, [redacted]. *See* SOMF ¶¶ 145–46; Resp. SOMF ¶¶ 145–46.

[6] Nielson and Lee also lack standing to bring their negligence claims for the alleged nationwide class. In *Lewis v. Mercedes-Benz USA, LLC*, 530 F. Supp. 3d 1183, 1205–06 (S.D. Fla. 2021) (Ruiz, J.), the Court granted defendant's motion to dismiss plaintiffs' nationwide claims for unjust enrichment because they "'are common law claims [that] rely on state law.'" The Court ruled that the plaintiffs "do not have standing . . . under any state's law but their own because they did not suffer any injuries in fact traceable to alleged violations of laws in other states." The Court held that the plaintiffs "lack standing to bring such claims on a national basis," including "'citizens of unrepresented states.'" *Id*. Similarly, the Court has denied plaintiffs' motion to certify a multi-state class alleging common law unjust enrichment claims, because "a plaintiff may [not] assert claims under a state law other than that which the plaintiff's own claims arises." *Simmons v. Ford Motor Co.*, 592 F. Supp. 3d 1262, 1280–81 (S.D. Fla. 2022) (Ruiz, J.).

As AA previously explained, the Court's initial choice-of-law analysis turned on the motion to dismiss standard and an undeveloped record. ECF No. 250 at 25–29. Now, the case is at the summary judgment stage, the record is clear, and the choice-of-law analysis requires another look. Using Florida's "most significant relationship" test, the Court should weigh four factors: (1) where the injury occurred; (2) where the conduct causing the injury occurred; (3) the domicile, residence, nationality, place of incorporation, and place of business of the parties; and (4) where the relationship between the parties is centered. *Michel v. NYP Holdings, Inc.*, 816 F.3d 686, 694 (11th Cir. 2016).

In its prior Order, the Court focused on "where the injury occurred" and applied Florida negligence law because Florida is where "the data was maintained, multiple Defendants are domiciled, and Defendants' security protocols allegedly broke down." ECF No. 104 at 7–8. As to AA, however, those conclusions do not apply. AA [redacted]. *See* SOMF ¶ 213; Resp. SOMF ¶ 213. When Mednax is removed from the equation, the link to Florida dissolves. The fact that Mednax is headquartered in Florida does not mean that Florida law governs Plaintiffs' claims *against AA*. AA is a separate entity, and Plaintiffs seek to hold AA liable for its own alleged acts—not for Mednax's conduct.[7]

Initially, the Court presumed that the "injury" under consideration was the Cyberattack itself and that the attack "occurred" in Florida, where Mednax is headquartered. That analysis was not based on a complete record and predated *Brinker*, which establishes that the *actual misuse* of the data is the "injury," not mere access. 73 F.4th at 889. Post-*Brinker*, the "place of injury" factor looks not to where criminals infiltrated the network but to where the data's alleged *use* caused the plaintiff injury.[8] Here, that is Virginia for Nielsen and Tennessee or South Carolina for Lee; either

[7] The [redacted]. This suit is not between Mednax and AA, nor is there a contract claim.

[8] Plaintiffs argue that because the Eleventh Circuit did not disturb the lower court's choice-of-law ruling, *Brinker* is irrelevant to choice-of-law considerations. ECF No. 283 (Plaintiffs' Opp. to Mednax's MSJ) at 29. Not so. *Brinker*'s discussion of what constitutes an "injury" matters for the choice-of-law analysis. And while *Brinker* did not instruct the district court to apply the laws of all fifty states to the negligence claim, neither party sought that result—the plaintiff argued that Florida law governed, while the defendant argued that Texas law governed. *See In re Brinker Data Incident Litig.*, 2021 WL 1405508, at *10 (M.D. Fla. Apr. 14, 2021), *vacated in part sub nom. Brinker Int'l, Inc.*, 73 F.4th 883. Neither party considered how the location of the injury caused by a misuse of data would affect the analysis, nor was the issue raised on appeal. *See Brinker*, 73 F.4th at 888. One cannot assume the Eleventh Circuit even considered the choice-of-law ruling.

way, neither Plaintiff was "injured" in Florida.

Nielsen alleges that the hackers "used" her data by (1) opening unauthorized bank accounts in her name, (2) registering her for *Shape* magazine, and (3) sending her spam. Opp. at 7. All of those alleged "uses" were felt in Virginia, [redacted]. None of them has anything to do with Florida. Moreover, the "place of the plaintiff's domicil[e] . . . is the single most important contact for determining the state of the applicable law as to most issues in situations involving [the invasion of the] right of privacy." Restatement (Second) of Conflict of Laws § 145 (1971) (citations omitted). Virginia, not Florida, has the most significant interest in protecting the privacy of a Virginia citizen. Also, [redacted]. SOMF ¶ 128. Virginia law governs.

The choice-of-law analysis for Lee is somewhat complicated by the fact that [redacted]. SOMF ¶¶ 155, 156; Resp. SOMF ¶¶ 155, 156. If the Court focuses on [redacted], South Carolina law governs. If the Court focuses on t[redacted], so Tennessee law governs. Either way, Florida law does not apply to Plaintiffs' negligence claims.[9]

The Supreme Court's rulings in *Phillips Petroleum Co. v. Shutts*, 472 U.S. 797 (1985), and *Erie R.R. Co. v. Thompkins*, 304 U.S. 64 (1938), also shape the choice-of-law analysis, making class-wide application of Florida law unconstitutional. First, Plaintiffs badly misread *Shutts.* Though Plaintiffs posit otherwise, the crux of the *Shutts* analysis is that the "constitutional limits" on choice of law "must be respected even in a nationwide class action" and that applying a forum state's substantive law requires "a 'significant contact or significant aggregation of contacts' to the claims asserted *by each member of the plaintiff class*." 472 U.S. at 821, 823 (emphasis added). Plaintiffs also try to distinguish between "present plaintiffs" and "absent plaintiffs" in a class-

[9] The Court has recognized that a generic common law claim for a putative nationwide class is "'in reality fifty . . . claims – one for each state" because those common law claims "'rely on state law.'" *Lewis*, 530 F. Supp. 3d at 1205 (internal quotation marks omitted); *see also Simmons*, 592 F. Supp. 3d at 1281 (refusing to certify plaintiffs' proposed multi-state class for common law unjust enrichment claim and explaining that while plaintiffs' complaint alleged "'one generic unjust enrichment claim, that claim is, in reality, five unjust enrichment claims – one for each state represented'" by a named plaintiff who was a citizen of that state because common law claims "'rely on state law'") (alterations adopted and internal quotation marks omitted).

action suit, Opp. at 18, but *Shutts* did not limit its choice-of-law holding to "absent plaintiffs."[10] Likewise, Plaintiffs incorrectly describe *Shutts*'s "ultimate[]" finding as being "in favor of the class members on this issue," *id.* at 18, by confusing the ruling on a personal jurisdiction question with the "entirely distinct . . . question of the constitutional limitations on choice of law." *Shutts*, 472 U.S. at 821. The Supreme Court rejected the *Shutts*-plaintiffs' preferred application of the forum state's law where two of the three named plaintiffs were not residents of the forum state and all three named plaintiffs owned gas leases outside the forum state. 472 U.S. at 801. As the Court explained, a "plaintiff's desire for forum law is rarely, if ever controlling." *Id*. at 820.

Second, Plaintiffs urge the Court to ignore *Erie* because it was not a class action. Instead, based on a footnote in an Oregon district court opinion, Plaintiffs seek to create a unique rule that "under non-identical state negligence laws," data breach cases do "not implicate any of the state-specific issues that can sometimes creep into the negligence analysis." Opp. at 7–11 (quoting *In re Premera Blue Cross Customer Data Sec. Breach Litig.*, 2019 WL 3410382, at *18 n.6 (D. Or. July 19, 2019)). But that Oregon decision involved an unopposed class action settlement and never mentioned *Erie* (or *Shutts*) in its footnote. *See In re Premera*, 2019 WL 3410382, at *18 n.6.[11] The very point of *Erie* is that it is unconstitutional for a federal court sitting in diversity to apply general common law rather than the law of the state whose law would apply in state court. *Erie*, 304 U.S. at 77–80. A federal court cannot create a common law that is a mash-up of the non-identical laws of the fifty states. *See id.* at 78–80.

Third, Plaintiffs fail to discuss (much less distinguish) most of AA's cases. This includes five Circuit Court of Appeals decisions and eight district court decisions from the Eleventh Circuit that, since *Erie* and *Shutts*, have enforced the constitutional limits on the application of the forum state's substantive law in a multi-state class action. *See* ECF No. 260 at 28-29.[12] The Court should

[10] Plaintiffs' distinction is also undercut by the Supreme Court's application of its earlier precedents dealing with constitutional limitations on the choice of law in individual lawsuits (involving present plaintiffs) to nationwide class actions (involving present named plaintiffs and absent putative members). *Shutts*, 472 U.S. at 823 ("[T]he constitutional limitations laid down in [] *Allstate* and [] *Dick*," (individual lawsuits), "must be respected even in a nationwide class action.").

[11] *In re Premera* relied on a California federal district court decision that also involved an unopposed class action settlement and did not cite *Erie*. *See In re Anthem, Inc. Data Breach Litig.*, 327 F.R.D. 299, 314 (N.D. Cal. 2018).

[12] Plaintiffs try to distinguish *Morris v. ADT Security Services, Inc.*, 2009 WL 10691165, at *8 (S.D. Fla. Sept. 11, 2009), but that decision held that it was unconstitutional to apply Florida substantive law to out-of-state class members even though the defendant was based in Florida.

not apply Florida law nationwide to Plaintiffs' negligence claims against AA.

3. Regardless of what law is applied, Plaintiffs cannot prevail on their negligence claim.[13]

A negligence claim generally requires a showing of (1) duty, (2) breach, (3) causation, and (4) injury. Here, regardless of the state law applied, Plaintiffs cannot show duty or causation.[14] As shown below, under any of the state's laws that could conceivably apply, neither Plaintiff can establish a negligence claim as a matter of law.

i. Plaintiffs' negligence claims fail under Florida law.

Neither Plaintiff can show the causation necessary to prevail on their negligence claims under Florida law. Contrary to Plaintiffs' characterization, in Florida, causation does not "merely require[] a showing [of] foreseeabil[ity]," Opp. at 13. It is much more stringent, requiring the introduction of "evidence which affords a reasonable basis for the conclusion that it is more likely than not that the conduct of the defendant was a substantial factor in bringing about the result. A mere possibility of such causation is not enough; and when the matter remains one of pure speculation or conjecture, or the probabilities are at best evenly balanced, it becomes the duty of the court to direct a verdict for the defendant." *Sanders v. ERP Operating Ltd. P'ship*, 157 So. 3d 273, 277 (Fla. 2015) (citation omitted). Moreover, causation requires that a "defendant's conduct foreseeably and substantially caused the *specific* injury that actually occurred." *Grieco v. Daiho Sangyo, Inc.*, 344 So. 3d 11, 23 (Fla. Dist. Ct. App. 2022) (internal quotation marks omitted) (emphasis added).

To prove causation in the context of a data breach specifically, Plaintiffs must show a "nexus between the two instances [(breach and injury)] beyond allegations of time and sequence."

---

[13] Plaintiff Lee argues, for the first time, that [redacted]. Opp. at 16. First, neither allegation is made in the Second Amended Complaint. *See* ECF No. 115. Plaintiffs cannot amend their complaint through briefing. *Miccosukee Tribe of Indians of Fla. v. U.S.*, 716 F.3d 535, 559 (11th Cir. 2013). Second, [redacted]. Regardless, [redacted].

[14] Plaintiffs spend nearly eight pages of their brief on standing. *See* Opp. at 2–10. They spend a single page on proximate cause. *Id.* at 13–14. While there is no question that Plaintiffs cannot demonstrate the traceability necessary for standing, it is abundantly clear that Plaintiffs cannot meet the much more stringent requirement of demonstrating proximate cause for their negligence claims. AA relies on its prior briefing on standing and focuses on the negligence claim here.

Resnick v. AvMed, Inc., 693 F.3d 1317, 1326–27 (11th Cir. 2012) (applying Florida law). To establish this "nexus," Plaintiffs must prove: (1) the data stolen was the same data used; (2) prior to the breach, their identities had not been stolen; and (3) they took precautions to protect their sensitive data. *See id.* Plaintiffs cannot do so. In this case, it is not just "more likely" that the data came from another source; it is certain. For both Plaintiffs, the data allegedly "misused" was *not* part of the data potentially exposed in the Cyberattack.

This case is far more akin to *Allgood v. PaperlessPay Corporation.*, 2022 WL 846070 (M.D. Fla. Mar. 22, 2022). In *Allgood*, the plaintiffs claimed that someone gained access to their confidential data and had a chance to review it. *See* 2022 WL 846070, at *10. But there was insufficient evidence to show that any specific data was actually accessed, much less taken, and the case was dismissed. *Id.* The plaintiffs could not show a "logical connection between the two incidents." *Id.* And though the *Allgood* Court admitted that it was *possible* that the breach caused the alleged damages, "a possible claim is not the same thing as a plausible claim." *Id.* at *11. A showing of causation requires more than plausibility; the alleged conduct must "more likely than not" have caused the harm. *See Montgomery v. Walgreen Co.*, 2019 WL 10747146, at *2 (M.D. Fla. Jan. 30, 2019). No reasonable jury could make such a finding here.

ii. Plaintiff Nielsen's negligence claim fails under Virginia law.

Plaintiff Nielsen cannot show the existence of a duty or causation necessary for her negligence claim under Virginia law. First, she cannot show that AA owed her a duty to protect her data. Plaintiffs cite two cases for the proposition that a healthcare provider owes a duty of nondisclosure to its patients. Opp. at 14 (citing *In re Cap. One Con. Data Breach Litig.*, 488 F. Supp. 3d 374 (E.D. Va. 2020) and *S.E. v. Inova Healthcare Servs.*, 1999 WL 797192 (Va. 1999)). Neither is applicable here. *Inova* simply stands for the unremarkable proposition that a healthcare provider cannot *intentionally* disclose data without permission. 1999 WL 797192 at *5. It says nothing of *unintentional* disclosure. *In re Capital One* is likewise irrelevant. There, the Court found a duty because of the defendant's "affirmative acts and representations regarding its ability and responsibility to render adequate data protection services" *and* because the defendant was "aware of the vulnerabilities and risks associated with their servers" but "failed to take reasonable care to protect Plaintiffs' PII." 488 F. Supp. 3d at 400. The Court held that "*[t]ogether*, these allegations plausibly satisfy the voluntary undertaking doctrine" under Virginia law. *Id* (emphasis added).

Neither of the determinative factors in *In re Capital One* is present here.[15]

Recognizing that Virginia law does not automatically impose a duty, Nielsen argues that AA voluntarily assumed a duty to protect her data, citing a "privacy policy" found on a "NAPA" webpage. Opp. at 14–17, 18. Unfortunately, in what is surely an innocent mistake, the "NAPA" webpage referenced by Plaintiffs does not belong to North American Partners in Anesthesia affiliated with the Defendant, but rather to a maritime software provider headquartered in Finland. The policy is completely irrelevant, and Nielsen points to no other source of an assumed duty. She cannot establish that AA ever assumed a duty to protect her data.[16] Plaintiffs' citations to other jurisdictions are wholly irrelevant. *See* Opp. at 15. Nielsen's claim is governed by Virginia law, and settled Virginia law forecloses forcing a tort duty on healthcare providers to protect a patient's data. *Deutsche Bank Nat'l Tr. Co. v. Buck*, 2019 WL 1440280, at *6 (E.D. Va. Mar. 29, 2019) (Virginia law does not "recognize[] a common law duty to protect an individual's private data from an electronic data breach"). Because AA did not assume any duty, Nielsen's claim is also barred by the economic loss rule. *See In re Cap. One Cons. Data Sec. Breach Litig.*, 2020 WL 13589625, at *2 (E.D. Va. Nov. 25, 2020) (economic loss rule applies unless a duty is *voluntarily* assumed). Likewise, Nielsen cannot show that any alleged breach caused her harm. Virginia law requires that the alleged breach be a "direct, efficient contributing cause" of the harm. *See Grimsley v. Watkins*, 2021 WL 4468437, at *3 (Va. Sept. 30, 2021). In other words, without the alleged breach, there would be no harm. *See Kellermann v. McDonough*, 684 S.E.2d 786, 793 (2009). Here, the data allegedly "used" to cause her injury was not exposed in the Cyberattack. It cannot be a cause of harm, direct or otherwise.

iii. Plaintiff Lee's negligence claim fails under Tennessee law.

Likewise, Lee's negligence claim fails under Tennessee law for want of a duty or causation. First, Lee cannot show that AA owed him a duty of care. Lee claims that Tennessee common law provides that "all persons have a duty to use reasonable care to refrain from conduct that will foreseeably cause injury to others." Opp. at 17. Lee fails to point out, however, that the rule applies to *physical harm* to person or property. *Satterfield v. Breeding Insulation Co.*, 266 S.W.3d 347,

[15] In *In re Capital One*, the Court applied the substantive tort law of each plaintiffs' *individual* residence to each negligence claim. *See* 488 F. Supp. 3d at 393.

[16] Even if Nielsen located a privacy policy for the correct NAPA, that policy would be irrelevant to any duty AA allegedly assumed. The alleged duty of AA, not NAPA, is at issue. *See* SOMF ¶ 128; Resp. SOMF ¶ 128.

362 (Tenn. 2008). Lee, like Nielsen, offers the irrelevant "NAPA" privacy policy. Opp. at 18. Finally, Lee looks to HIPAA, but he cannot establish a duty there. *See Faber v. Ciox Health, LLC*, 944 F.3d 593, 597–98 & n.3 (6th Cir. 2019) (rejecting an attempt to use HIPAA to establish a common law duty in support of a negligence claim). AA had no duty to protect Lee's data, and his negligence claim fails under Tennessee law.

Even if Lee could show that AA owed him a duty, his negligence claim still fails for lack of causation. Lee must offer enough evidence showing that AA's alleged breach of duty was "more probable than any other cause" of his injuries. *Roberts v. Ray*, 322 S.W.2d 435, 437 (Tenn. Ct. App. 1958). Like Nielsen, he cannot. Lee cannot link the alleged "use" of his confidential data to any data actually exposed in the Cyberattack. That's because [redacted]. The Cyberattack could not have been the "cause" of Lee's alleged injuries; it certainly was not the "more probable" cause.

iv. Plaintiff Lee's negligence claim fails under South Carolina law.

Finally, Lee's negligence claim fails under South Carolina law. Again, Plaintiffs cite the wrong "NAPA" privacy policy in a desperate attempt to establish a duty. Opp. at 16-17. Lee also cites cases where a physician *voluntarily* disclosed data against the patient's wishes. *Id.* at 17. Those cases are inapposite here, where any disclosure was the result of unintentional, third-party, *criminal* conduct. Under South Carolina law, "there is no general duty to control the conduct of another or to warn a third person or potential victim of danger." *Faile v. S.C. Dep't of Juv. Just.*, 566 S.E.2d 536, 546 (S.C. 2002).

Nor can Lee prove causation. South Carolina law requires that the alleged injury would not have occurred "but for" the alleged negligence. *See Bramlette v. Charter–Med.–Columbia*, 393 S.E.2d 914, 916 (S.C. 1990). Lee cannot show that he suffered any harm that he would not have otherwise suffered given his [redacted]

III. CONCLUSION

For all these reasons, AA requests that its Motion for Summary Judgment be granted.

Respectfully submitted this the 5th day of April, 2024.

/s/ Starr T. Drum
Starr T. Drum
Xeris E. Gregory
POLSINELLI
Birmingham, AL
Phone: (205) 963-7136
sdrum@polsinelli.com
xgregory@polsinelli.com

Lee E. Bains, Jr.
Thomas J. Butler
MAYNARD NEXSEN PC
1901 Sixth Avenue North, Suite 1700
Birmingham, AL 35203
Phone: (205) 254-1000
Fax: (205) 254-1999
lbains@maynardnexsen.com
tbutler@maynardnexsen.com

ATTORNEYS FOR DEFENDANT AMERICAN ANESTHESIOLOGY, INC.

CERTIFICATE OF SERVICE

I hereby certify that on April 5, 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/ Starr T. Drum
Starr T. Drum