UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA

CASE NO. 21-MD-02994-RAR

IN RE:

MEDNAX SERVICES, INC.,
CUSTOMER DATA SECURITY BREACH LITIGATION

PLAINTIFFS' REPLY IN SUPPORT OF THEIR MOTION FOR CLASS CERTIFICATION

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

TREATISES

INTRODUCTION

Faced with overriding common and predominating liability issues in this case that strongly support class certification as an appropriate and superior means of litigating these claims, Defendants' challenges to certification fail. Plaintiffs—all patients of Defendants whose PHI and PII was exposed to unauthorized persons and stolen in the Data Breach—are typical and adequate to represent each member of the class who similarly had their PII and PHI stolen in the Data Breach. Defendants' meritless challenges to Plaintiffs' class definition and damages methodology do not defeat the common, predominating questions critical to the resolution of every class members' claims. The Court should therefore certify this matter as set forth in Plaintiffs' Motion for Class Certification (hereinafter, "Mot.").

ARGUMENT

I. PLAINTIFFS HAVE STANDING TO LITIGATE THIS ACTION.

Defendants argue in their Opposition that Plaintiffs lack standing to be class representatives in this case because the evidence developed in discovery shows Plaintiffs have not suffered any legally cognizable injury that is fairly traceable to the Data Breach. For the reasons more fully in Plaintiffs' forthcoming Responses in Opposition to Defendants' Motions for Summary Judgment, this contention is without merit. As demonstrated therein, there are genuine issues of material facts concerning the extent to which Plaintiffs' PHI and/or PII was accessed and/or misused as a result of the Data Breach. Because these factual questions must be resolved by a jury, there is no basis for denying Plaintiffs' Motion to Certify the Class on standing grounds.

II. THE CLASS IS PROPERLY DEFINED AND ASCERTAINABLE.

A. The Class Definition Is Not Vague.

A running theme throughout Defendants' Opposition is that the class is improperly defined and overly broad because Plaintiffs do not define what the commonly used word "compromised" means. In data breach actions, the term "compromised" is commonly understood to mean "accessed by cybercriminals," and that is the meaning in which Plaintiffs have used it here.[1] This is the context

[1] *See*, *e.g.*, *Green-Cooper v. Brinker Int'l, Inc.*, 73 F.4th 883, 886 (11th Cir. 2023) ("Brinker International, Inc. ("Brinker"), the owner of Chili's restaurants, faced a cyber-attack in which customers' credit and debit cards were compromised."); *In re 21st Century Oncology Customer Data Sec. Breach Litig.*, 380 F. Supp. 3d 1243, 1246 (M.D. Fla. 2019 (""On March 4, 2016, Defendant 21st Century Oncology Holdings, Inc. announced that on October 3, 2015, an unauthorized third party might have gained access to its database containing patients' personal information ("Data Breach"). As a result of the Data Breach, the information of approximately 2.2 million current and former patients was compromised.").

in which other courts have certified classes of individuals who have had their information "compromised" in a data breach. *See*, *e.g.*, *In re Marriott Int'l, Inc., Customer Data Sec. Breach Litig.*, 341 F.R.D. 128, 152 (D. Md. 2022), vacated and remanded sub nom. *In re Marriott Int'l, Inc.*, 78 F.4th 677 (4th Cir. 2023), and reinstated by *In re Marriott Int'l Customer Data Sec. Breach Litig.*, 2023 WL 8247865 (D. Md. Nov. 29, 2023) (certifying a subclass defined as "All natural persons residing in Florida whose Personal Information, given to Starwood in connection with the making of a reservation at a Starwood property, was compromised in a data breach announced by Marriott on or about November 30, 2018" and twelve identical subclasses also using the term "compromised"); *In re The Home Depot, Inc., Customer Data Sec. Breach Litig.*, 2016 WL 6902351, at *1 (N.D. Ga. Aug. 23, 2016) (approving a settlement class defined as "All residents of the United States whose Personal Information was compromised as a result of the Data Breach first disclosed by Home Depot in September 2014.").

B. The Class Definitions Satisfy Standing and Predominance Requirements.

At the class certification stage, the Eleventh Circuit has held that district courts are not required to "ensure that the class definition does not include any individuals who do not have standing before certifying a class." *Cordoba v. DIRECTV, LLC*, 942 F.3d 1259, 1276 (11th Cir. 2019 (emphasis added). Nevertheless, Plaintiffs acknowledge that under *TransUnion LLC v. Ramirez* for purposes of a (b)(3) class seeking damages, in addition to demonstrating a substantial risk of future harm, Plaintiffs and Class Members must also have incurred reasonable expenses or time spent in mitigation of the consequences of the Data Breach. 141 S. Ct. 2190, 2208 (2021). Thus, to prevent any issues of overbreadth or the possibility that some individuals whose PHI and/or PII was compromised in the Data Breach but suffered no additional injury therefrom to date may not have standing, the Court might find it appropriate to modify the proposed class definitions by adding "and have incurred reasonable expenses or time spent in mitigation of the consequences of the Data Breach" to each respective definition.[2] For example, the Nationwide Mednax Class would be defined as: "All current and former patients of Mednax residing in the United States whose PHI and PII was compromised as a result of the Data Breach disclosed beginning in December 2020 and have incurred reasonable expenses or time spent in mitigation of the consequences of the Data Breach."

[2] It is within the Court's authority to revise or redefine the proposed class(es). *See* 7A Charles Alan Wright, Arthur R. Miller & Mary Kay Kane, Federal Practice and Procedure § 1759 at 130-31 (3d ed. 2005) ("[I]f plaintiff's definition of the class is found to be unacceptable, the court may construe the complaint or redefine the class to bring it within the scope of Rule 23.")

As for predominance, Plaintiffs note that in *Green-Cooper v. Brinker Int'l, Inc.*, 73 F.4th 883 (11th Cir. 2023) ("*Brinker*") the Eleventh Circuit considered the district's courts certification of a payment card data breach class defined as: "All persons residing in the United States who made a credit or debit card purchase at any affected Chili's location during the period of the Data Breach (March and April 2018) 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." The Eleventh Circuit acknowledged the class was properly defined for standing purposes. *Id.* at 892. But turning to the question of predominance, the court expressed concerns that the language "accessed by cybercriminals" was overbroad because it might include individuals who had their payment cards accessed in the breach but subsequently canceled their cards and therefore had no continuing risk of fraudulent misuse. *Id.* The court thus encouraged the district court to consider its predominance analysis anew to determine if the class definition needed to be revised to exclude any such individuals. Here, to the extent the Court understands "compromised" to mean "accessed by cybercriminals," that term does not present the same risk of overbreadth as in *Brinker*. The Eleventh Circuit has noted that in payment card data breaches, there is no risk of future injury to an individual who responds to the breach by canceling their card. *See Tsao v. Captiva MVP Rest. Partners, LLC*, 986 F.3d 1332, 1344 (11th Cir. 2021). Importantly, the Eleventh Circuit has contrasted payment card information from PII such as social security numbers, birth dates, and driver's license numbers. *Id.* at 1343 ("Tsao has not alleged that social security numbers, birth dates, or driver's license numbers were compromised in the [data] breach, and the card information allegedly accessed by the [] hackers 'generally cannot be used alone to open unauthorized new accounts.'")[3]; *see also Weisenberger v. Ameritas Mut. Holding Co.*, 597 F. Supp. 3d 1351, 1359 (D. Neb. 2022) ("The kind of PII that the plaintiff alleged was compromised in the data breach—Social Security numbers, addresses, birth dates, names, addresses, and email addresses—is the kind of information, unlike mere credit card information, that can lead to a wide range of identity fraud."). Unlike the plaintiffs in *Brinker* who could save themselves from the risk of future injury by canceling their cards, Plaintiffs and the putative class members in this case cannot cancel or otherwise change their birth dates, social security numbers, or PHI. That information is immutable and will be personally identifying for the rest of their lives, thus putting them at a continued risk of misuse of their personal information. Consequently, the class definition here does not present the same potential predominance concerns that troubled the Eleventh Circuit in *Brinker*.

[3] The Eleventh Circuit's use of the term "compromised" in this context should be noted.

C. The Class Is Ascertainable.

In addition to being properly defined, the Class is also ascertainable. Mednax notified 835,151 individuals who were capable of identification but claims it had to give "substitute notice" under HIPAA to the other 608,565 unidentified individuals in its patient population who were subject to the Data Breach. Opp. at 5. Because it cannot identify every individual who was impacted by the Data Breach, Mednax contends that the class is not ascertainable. "In general, courts do not look favorably upon the argument that records a defendant treats as accurate for business purposes are not accurate enough to define a class." *In re Marriott*, 341 F.R.D. at 145 (citation omitted). In any event, a class is ascertainable "if it is adequately defined such that its membership is capable of determination." *Cherry v. Dometic Corp.*, 986 F.3d 1296, 1304 (11th Cir. 2021. The membership of this class is clearly capable of determination. Many members are identifiable by Mednax's records, but those who are not can be recognized through self-identification. *See In re Marriott*, 341 F.R.D. at 145 (noting that because Marriott had a database of customer records, even where those records were incomplete and missing some fields for certain customers, plaintiffs "can use affidavits to help ascertain the class."). Defendants argue that many of the unidentifiable members of the class "were newborns for whom Mednax lacked sufficient demographic information to specifically identify." Opp. at 6. Surely Defendants' records contain the names and likely contact information of those newborns' parents. Accordingly, any child claiming to be a member of the class can present through a parent or guardian an affidavit that allows Defendants to cross-reference their patient records by using their parents' names and other demographic information. There is nothing administratively unfeasible about this, as "the need to review individual files to identify [class] members [is] not [a] reason[ ] to deny class certification." *In re Marriott*, 341 F.R.D. at 145.

III. PLAINTIFFS SATISFY THE REQUIREMENTS OF RULE 23(a).

A. Numerosity of the Subclasses Is Satisfied.

Defendants do not dispute the numerosity of the proposed Nationwide Mednax Class and Nationwide AA Class. Instead, Defendants argue that Plaintiffs have not established the numerosity of the five state-specific subclasses, all of which, by definition, consist of only Mednax patients. "Parties seeking class certification do not need to know the precise number of class members, but they must make reasonable estimates with support as to the size of the proposed class." *Just v. Rheem Mfg. Co.*, 318 F.R.D. 687, 694 (S.D. Fla. 2016).

Mednax acknowledges that 1,443,716 Mednax patients were potentially impacted in the Data Breach. *See* Opp. at 5-6. With more than 200 locations throughout Florida, is it a virtual certainty that

at least 40 Floridians are putative members of the Florida Subclass, sufficient to establish numerosity. *See Cox v. Am. Cast Iron Pipe Co.*, 784 F.2d 1546, 1553 (11th Cir. 1986) (noting "more than forty" is adequate to satisfy numerosity). Similarly, with at least 20 locations in Arizona, 50 locations in California, 15 locations in Maryland, and 45 locations in Washington[4], common sense can surmise that at least 40 individuals in each of those states are putative members of the class.

B. Commonality Is Satisfied.

Defendants contend that Plaintiffs failed to satisfy the commonality requirement because they cannot prove that each class member's data was "compromised" in the same way. This argument fails because it focuses on the Plaintiffs' injuries rather than Defendants' conduct. *See Cnty. of Monroe, Fla. v. Priceline.com, Inc.*, 265 F.R.D. 659, 667 (S.D. Fla. 2010) ("Allegations of a common course of conduct by defendants affecting all class members will satisfy the commonality requirement."). Particularly, in data breach class actions, the questions of "whether [defendant] had a duty to protect customer data, whether [defendant] knew or should have known its data systems were susceptible, and whether [defendant] failed to implement adequate data security measures to protect customers' data" have been found to be "questions that are common to the class and capable of classwide resolution." *In re Brinker Data Incident Litig.*, 2021 WL 1405508, at *8 (M.D. Fla. Apr. 14, 2021), vacated in part on other grounds by *Brinker*, 73 F.4th 883; *see also In re Marriott*, 341 F.R.D. 147 ("Common questions of fact include whether Defendants knew about their data security vulnerabilities, what Defendants did or did not do to address those vulnerabilities, and whether the hacker(s) exploited those vulnerabilities to exfiltrate customers' PII.").

C. Plaintiffs' Satisfy Typicality and Adequacy.

Defendants argue that Plaintiffs cannot establish typicality or adequacy because not all putative class members' PII and PHI was "exposed to fraudulent misuse," the types of information involved in the Data Breach vary substantially across the putative class, and different categories of damages apply to putative class members. Again, these arguments fail. "The claim of a class representative is typical if 'the claims or defenses of the class and the class representative arise from the same event or pattern or practice and are based on the same legal theory.'" *Williams v. Mohawk Indus., Inc.*, 568 F.3d 1350, 1357 (11th Cir. 2009) (quoting *Kornberg v. Carnival Cruise Lines, Inc.*, 741 F.2d 1332, 1337 (11th Cir.1984)). "The typicality requirement may be satisfied despite substantial factual differences ... when there is a strong similarity of legal theories." *Id.*

[4] *See* https://www.pediatrix.com/find-care (last visited December 18, 2023).

Here, Plaintiffs' negligence claim and state statutory claims "arise from a single event"—the Data Breach—"and there is no variation in legal theory." *Id.* Regardless of how and whether a class member's PII and PHI was misused, regardless of what PII or PHI was exposed or accessed in the Data Breach, regardless of what damages a class member suffered, they, like Plaintiffs, "must show that Defendants w[ere] negligent … or violated [state consumer protection statutes], and that [Defendants'] conduct caused their damages, which are alleged to be similar." *In re Brinker*, 2021 WL 1405508 at *8. Typicality is thus satisfied, as is adequacy.

IV. PLAINTIFFS SATISFY THE REQUIREMENTS OF RULE 23(b)(3).

A. Common Issues Predominate Over Individualized Issues.

Defendants go to great lengths to describe every possible sense in which Plaintiffs' and the putative Class's claims may be subject to individualized proof. What Defendants conveniently ignore is the common questions of liability that exist in this case. Common issues of law or fact predominate where they "'ha[ve] a direct impact on every class member's effort to establish liability' that is more substantial than the impact of individualized issues in resolving the claim or claims of each class member." *Vega v. T-Mobile USA, Inc.*, 564 F.3d 1256, 1270 (11th Cir. 2009) (quoting *Klay v. Humana, Inc.*, 382 F.3d 1241, 1255 (11th Cir. 2004). In the data breach context, "the glue binding th[e] putative class action is Defendants' data security policies and practices and … Defendants' responsibilities to class members regarding data protection to which all class members are subject." *In re Marriott*, 341 F.R.D. at 155 (internal quotation marks omitted). On a similar basis, the district court in *In re Brinker* found that predominance was satisfied with respect to the plaintiffs' nationwide negligence class, even though there were issues of causation and damages that would have to be resolved on an individualized basis. 2021 WL 1405508, at *11.[5]

Here, too, whether Defendants owed a duty to secure patients' confidential information, the actions Defendants did or did not take to secure patients' PII and PHI, and whether Defendants' actions (or lack thereof) enabled the Data Breach to occur are questions that "ha[ve] a direct impact on every class member's effort to establish liability and on every class member's entitlement to

[5] *See also In re Wawa, Inc. Data Sec. Litig.*, 2021 WL 3276148, at *4 (E.D. Pa. July 30, 2021); *In re Premera Blue Cross Customer Data Sec. Breach Litig.*, 2019 WL 3410382, at *18 (D. Or. July 29, 2019); *In re Yahoo! Inc. Customer Data Sec. Breach Litig.*, 2020 WL 4212811, at *7 (N.D. Cal. July 22, 2020; *In re Anthem, Inc. Data Breach Litig.*, 327 F.R.D. 299, 312 (N.D. Cal. 2018). Although each of these decisions was made in the context of settlement approval, they represent the widely held view that the common issues of a defendants' data security predominate over individualized issues concerning the data breach victims' damages.

injunctive and monetary relief." *Klay*, 382 F.3d at 1255. These questions thus predominate over individualized issues. To the extent Defendants argue there are individualized issues of causation, such as whether Plaintiffs or putative class members have fallen victim to other data breaches, "the multiple breach issue [is] not a disqualifying causation issue, but rather to be determined at the damages phase." *In re Brinker*, 2021 WL 1405508, at *12.

B. Choice of Law Issues Do Not Defeat Predominance.

Seeking to defeat predominance on grounds that variations in state law preclude certification of Plaintiffs' negligence claim on a nationwide basis, Defendants ask the Court to revisit its previous determination that Florida law governs Plaintiffs' negligence claim. Defendants argue that each Plaintiff and putative Class Member's claim must be governed by the negligence laws of their home state because that is where each of their injuries occurred. For this proposition, Defendants rely on the Eleventh Circuit's decision in *Brinker*. There, in explaining that standing had been properly demonstrated, the Court noted, "We typically require misuse of the data cybercriminals acquire from a data breach because such misuse constitutes both a 'present' injury and a 'substantial risk' of harm in the future." 73 F.4th at 889. Defendants oddly interpret this statement as a hard and fast rule that the choice of law analysis for a negligence claim turns on where a plaintiff or class member experienced the misuse of their data. Nothing in *Brinker* can fairly be read to suggest such a rule, especially in light of the fact that the Eleventh Circuit did not disturb the part of the district court's order certifying a nationwide negligence class. The parties disagreed whether Texas law or Florida law governed the negligence claim, but the district court noted that, either way, under the "most substantial relationship" test, only one state's law would apply, "so that claim is not a concern for manageability or predominance." *In re Brinker*, 2021 WL 1405508, at *11 (citing other data breach cases certifying nationwide negligence claims). The Eleventh Circuit did not instruct the court to reassess its predominance analysis on the basis that each putative class members' claims would be governed by the laws of their home states, which it surely would have done if it believed their injuries occurred only where they experienced the misuse of their data. No such rule exists, and the Court should not apply it here.

This Court should find, as the district court did in *In re Brinker* and as other courts have in other data breach actions, that "under non-identical state negligence laws, '[t]his case does not implicate any of the state-specific issues that can sometimes creep into the negligence analysis.'" *In re*

Premera Blue Cross Customer Data Sec. Breach Litig., 2019 WL 3410382, at *18 n.6 (D. Or. July 29, 2019 (quoting *In re Anthem, Inc. Data Breach Litig.*, 327 F.R.D. 299, 312 (N.D. Cal. 2018)).[6]

C. Predominance Is Satisfied as to Plaintiffs' Statutory Claims.

Defendants' challenges to predominance as to Plaintiffs' statutory claims likewise fail. Defendants do not contest that their conduct of maintaining inadequate data security is a business practice that itself violates the FDUTPA, MCPA, and WCPA without regard to any misrepresentations or omissions that were made. *See* Mot. at 16. Nor do Defendants dispute that whether its data security was inadequate, and thus in violation of these statutes, is subject to classwide proof. And while Defendants challenge whether each class member received uniform misrepresentations about Defendants' data security, they do not contest that they failed to disclose their inadequate data security and prior breaches to all class members. Nor do Defendants contest that class members are entitled to a presumption of reliance on Defendants' omissions, even though they conveniently overlook Plaintiffs' allegations of the omissions in this case. *See* [Doc. 115, ¶¶ 481(e), 481(g), 525-26, 530, 588(f), 588(g), 589]. Accordingly, the Court need not determine any individual issues about whether class members were all exposed to and relied upon the same alleged misrepresentations to certify Plaintiffs' FDUTPA, MCPA, and WCPA claims where Defendants uniformly failed to disclose material information to all class members. *See In re Premera*, 2019 WL 3410382 at *17 (noting that "idiosyncratic differences between state consumer protection laws" did not defeat predominance in a data breach action because "Plaintiffs' unfair practices act claim is based on Premera's alleged failure to provide adequate data security, [and] involves the uniform aspects of state CPA laws."). Thus, "[l]iability is not tied to an element, like reliance, that may sometimes require evaluating each individual Plaintiff's circumstances. Rather, because the common issues turn on a common course of conduct by the defendant, '[a] common nucleus of facts and potential legal remedies dominates this litigation.'" *Id.* (quoting *In re Anthem*, 327 F.R.D. at 315).

D. Individualized Issues of Damages Do Not Predominate.

In their Motion, Plaintiffs explained why their damages model avoids any concerns about individualized damages determinations predominating over the common issues in this case, and they

[6] Plaintiffs further note that Defendants' "example" of the choice-of-law problems does not support their argument. Defendants point to Plaintiff Brooke Nielsen, a Virginia resident, as an individual who would not have a viable negligence claim under Virginia law. But, as Judge Trenga found in a well-reasoned analysis, Virginia law would not bar a negligence claim arising out of a data breach similar to this one. *See In re Capital One Consumer Data Sec. Breach Litig.*, 488 F. supp. 3d 374, 397–401 (E.D. Va. 2020).

need not repeat those arguments here. But, once again, Plaintiffs need to correct Defendants' misreading of the Eleventh Circuit's decision in *Brinker*. Addressing Mr. Olsen's report, Defendants claim that *Brinker* "confirms that neither of the categories of alleged damages [proposed by Mr. Olsen] is compensable. In *Brinker*, the Eleventh Circuit reversed and remanded a district court's grant of class certification because the district court did not explain how it could 'weed out' individuals whose information had merely been "accessed by cybercriminals" and therefore 'uninjured' under Eleventh Circuit precedent." Opp. at 25 (citing *Brinker*, 73 F.4th 891-92). However, this was not the basis upon which the Eleventh Circuit vacated the district court's class certification order. The court vacated the order only to the extent the order concluded that two of the named plaintiffs had standing. Notably, with respect to damages, the Eleventh Circuit rejected the defendant's argument that individualized damages claims would predominate over the issues common to the class and found the district court did not abuse its discretion in holding that the plaintiffs' damages model was sufficient to satisfy the predominance requirement. *Brinker*, 73 F.4th at 893. So too is the damages model set forth by Mr. Olsen here.

V. THE COURT MAY CERTIFY BOTH A (B)(3) AND (B)(2) CLASS IN THIS CASE.

Defendants also misinterpret the cases they cite in support of their argument that the Court cannot certify a (b)(2) class for injunctive relieve in this case because Plaintiffs are also seeking damages for a (b)(3) class. *Wal-Mart Stores, Inc. v. Dukes*, 564 U.S. 338 (2011) does not stand for the proposition that a court cannot certify a (b)(2) class and a (b)(3) class in the same action. It stands only for the proposition that claims that will require an individualized determination of money damages (like the claims for backpay female workers asserted in that case) must be certified under (b)(3) so that plaintiffs have an opportunity to opt out of the class, which they cannot do in a mandatory (b)(2) class. *See id.* at 361–62. Furthermore, as the Eleventh Circuit has clarified, plaintiffs cannot use a (b)(2) class to obtain an injunction or declaratory relief that redresses past harms (e.g., requiring a company to give backpay or requiring an auto insurance company to reprocess claims that were previously capped at a lower dollar amount than they should have been). *AA Suncoast Chiropractic Clinic, P.A. v. Progressive Am. Ins. Co.*, 938 F.3d 1170, 1175 (11th Cir. 2019). The purpose of (b)(2) relief is solely to prevent future injury, not past harms.

Nothing in the rationale of these decisions prevents courts from certifying in the same action a (b)(3) class for damages redressing injuries the class has already suffered and a separate (b)(2) class to prevent future harm to the class. Here, Plaintiffs have articulated that there is an ongoing threat to their PII and PHI that remains in Defendants' control. Accordingly, Plaintiffs' request for

certification of a (b)(2) class does not run afoul of *Dukes*. *See*, *e.g., Spegele v. USAA Life Ins. Co.*, *336 F.R.D. 537*, 558 (W.D. Tex. 2020) (approving of "'divided certification,' certifying the damages claims under Rule 23(b)(3) while certifying the injunctive relief under 23(b)(2)") (citing cases).

VI. AA'S SEPARATE ARGUMENTS ARE MOOT.

Finally, AA argues: (1) that nine of the named Plaintiffs lack standing to assert claims against AA because they have no relevant connection to AA, and (2) that no subclasses should be certified against AA. Opp. at 33-35. But as AA itself acknowledges, "Plaintiffs themselves do not seek to certify any subclasses against AA." *Id.* at 34. This is true, making AA's argument moot. AA's first argument is also moot. By definition, the proposed Nationwide AA Class is limited to "patients of AA." Thus, any Plaintiff or putative class member who was not a patient of AA is, by definition, not included in the class.

CONCLUSION

For all of the foregoing reasons and those set forth in Plaintiffs' opening memorandum, Plaintiffs' Motion for Class Certification should be granted.

Dated: December 27, 2023.

Respectfully submitted,

/s/ William B. Federman

William B. Federman*
FEDERMAN & SHERWOOD
10205 N. Pennsylvania Ave.
Oklahoma City, Oklahoma 73120
(405) 235-1560
(405) 239-2112 (facsimile)
wbf@federmanlaw.com

**admitted pro hac vice*

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

ATTORNEYS FOR PLAINTIFFS

CERTIFICATE OF SERVICE

I hereby certify that on December 27, 2023, I electronically filed the foregoing document with the Clerk of the Court using the CM/ECF system, which will send notice of electronic filing to all counsel of record.

By: */s/ William B. Federman*