No. 21-13146

In the

# United States Court of Appeals

## For the Eleventh Circuit

---

ERIC STEINMETZ; MICHAEL FRANKLIN, AND SHENIKA THEUS,
*individually and on behalf of all others similarly situated,*
*Plaintiffs-Appellees,*

v.

BRINKER INTERNATIONAL, INC.,
*Defendant-Appellant.*

---

On Fed. R. Civ. P. 23(f) Appeal from the
United States District Court for the Middle District of Florida
Judge Timothy J. Corrigan
No. 3:18-cv-00686-TJC-MCR

---

**BRIEF OF *AMICUS CURIAE* THE CHAMBER OF COMMERCE OF THE UNITED STATES OF AMERICA IN SUPPORT OF APPELLANT**

---

Andrew R. Varcoe
Jennifer B. Dickey
U.S. CHAMBER
LITIGATION CENTER
1615 H Street, NW
Washington, DC 20062
T: (202) 463-5337

Gilbert C. Dickey
MCGUIREWOODS LLP
201 North Tryon Street
Suite 3000
Charlotte, NC 28226
T: (704) 343-2396
gdickey@mcguirewoods.com

*Counsel for Amicus Curiae The Chamber of Commerce of the United States of America*

November 23, 2021

**Steinmetz, et al. v. Brinker International, Inc., No. 21-13146**

**CERTIFICATE OF INTERESTED PERSONS AND CORPORATE DISCLOSURE STATEMENT**

Pursuant to Rule 26.1, Federal Rules of Appellate Procedure, and 11th Cir. R. 26.1, amicus curiae the Chamber of Commerce of the United States of America states that, in addition to the persons listed in the Certificate of Interested Persons and Corporate Disclosure Statement filed by Appellants on September 22, 2021, the following persons and entities have an interest in the outcome of this case:

Andrew R. Varcoe, Counsel for Amicus Curiae the Chamber of Commerce of the United States of America

Chamber of Commerce of the United States of America, Amicus Curiae

Gilbert C. Dickey, Counsel for Amicus Curiae the Chamber of Commerce of the United States of America

Jennifer B. Dickey, Counsel for Amicus Curiae the Chamber of Commerce of the United States of America

McGuireWoods LLP, Counsel for Amicus Curiae the Chamber of Commerce of the United States of America

*Amicus curiae* the Chamber of Commerce of the United States of America further certifies that it has no parent company and that no publicly held company holds 10% or greater ownership interest in the Chamber.

Dated: November 23, 2021

Respectfully submitted,

*/s/ Gilbert C. Dickey*
Gilbert C. Dickey

# TABLE OF CONTENTS

# TABLE OF CITATIONS

Page(s)

## Cases

**Statutes**



**Other Authorities**

## STATEMENT OF IDENTITY AND INTEREST[1]

The Chamber of Commerce of the United States of America is the world's largest business federation. It represents approximately 300,000 direct members and indirectly represents the interests of more than three million companies and professional organizations of every size, in every industry sector, and from every region of the country. An important function of the Chamber is to represent the interests of its members in matters before Congress, the Executive Branch, and the courts. To that end, the Chamber regularly files amicus curiae briefs in cases, like this one, that raise issues of concern to the nation's business community.

The Chamber's members have a strong interest in promoting fair and predictable legal standards. They are particularly likely to be defendants in putative class actions. The Chamber's members thus have a strong interest in ensuring that courts comply with the Supreme Court's class action precedents, including undertaking the rigorous analysis required by Federal Rule of Civil Procedure 23. The Chamber

[1] All parties have consented to the filing of this brief. No party's counsel authored this brief in whole or in part, and no entity or person, aside from *amicus curiae*, its members, or its counsel, made any monetary contribution intended to fund the preparation or submission of this brief.

has filed amicus curiae briefs in several recent Rule 23 class action cases, including *Tyson Foods, Inc v. Bouaphakeo*, 136 S. Ct. 1036 (2016); *Comcast Corp v. Behrend*, 569 U.S. 27 (2013); and *Walmart Stores, Inc. v. Dukes*, 564 U.S. 338 (2011).

## STATEMENT OF THE ISSUES

Amicus curiae agrees with Appellant Brinker International's statement of the issues.

## SUMMARY OF THE ARGUMENT

In our increasingly digitized world, it is no surprise that large data breaches are becoming increasingly common. *See* Turner, Walker, and Moore, Data Flows, Technology, and the Need for National Privacy Legislation, at 26, U.S. Chamber of Commerce Technology Engagement Center and Political and Economic Research Council (2019) *available at* https://americaninnovators.com/research/data-flows-technology-the-need-for-national-privacy-legislation/. What might surprise some, however, is that these data breaches generally do not result in any harm to the individual consumers whose information has been accessed. *Tsao v. Captiva MVP Restaurant Partners, LLC*, 986 F.3d 1332, 1343 (11th Cir. 2021). Nevertheless, putative class actions continue to be brought

on behalf of the individuals whose data has been accessed. Permitting these suits to proceed as class actions would impose substantial costs on the business community without redressing even a substantial risk of harm to the consumers.

This case is a perfect example of why data breach cases are so ill suited to use of the class action device. Here, the district court approved both a national and California class composed of customers 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." Doc. 167 at 16. That decision exposes the defendant to significant costs and settlement pressure in violation of bedrock protections for defendants in both Article III and Rule 23.

*First*, the certified classes cannot be reconciled with the limits that this Court has imposed on standing in data breach cases. This Court has explained that "[e]vidence of a mere data breach does not, standing alone, satisfy the requirements of Article III standing." *Tsao*, 986 F.3d at 1344. Each plaintiff must show a "substantial risk" of harm that is "certainly impending." *Id.* And neither vague allegations of the risk of future harm nor self-imposed costs undertaken in response to a data breach meet that

standard. *Id.* But the district court approved a class based on exactly those considerations. Indeed, it defined the class based on the putative members' self-imposed decision to incur expenses or spend time in mitigation of the possible consequences of the Data Breach. Doc. 167 at 16.

*Second*, in defining the classes in this manner, the district court all but ensured that individual issues will predominate. Each member of the class must show expenses or time spent in mitigation of the consequences of the data breach before he or she can recover. But neither the district court nor the plaintiffs have suggested any way to resolve that inquiry without individual adjudications that would predominate over common issues.

*Third*, the district court approved the classes on the theory that damages could be awarded based on an average amount of each category of damages even when a plaintiff had not suffered any damages in such category. The Supreme Court rejected a similar proposal for "Trial by Formula" in *Wal-Mart Stores, Inc. v. Dukes*, 564 U.S. 338, 367, 131 S. Ct. 2541, 2561 (2011). *Dukes* establishes that class action defendants must have the opportunity to present their defenses to individual claims. And

*Tyson Foods, Inc. v. Bouaphakeo*, 577 U.S. 442, 459 (2016), confirms that representative evidence that would not be sufficient to sustain a jury finding if it were introduced in each individual action cannot be used to meet that task in a class action. Since the representative evidence in this case does not meet that standard and instead would prevent the defendant from litigating its individualized defenses, the district court's method for assessing damages in this suit is impermissible.

## ARGUMENT AND CITATIONS OF AUTHORITY

### I. Plaintiffs cannot establish standing in a data breach case without showing the kind of "misuse" that raises a substantial risk of certainly impending harm.

All federal litigation, including class actions, must comport with the Constitution's limits on judicial power. Article III of the Constitution limits the jurisdiction of federal courts to "case[s]" or "controvers[ies]." Each plaintiff must show that he has standing to sue to satisfy this requirement. *See Spokeo, Inc. v. Robins*, 578 U.S. 330, 338, 136 S. Ct. 1540, 1547 (2016). To show standing, a plaintiff must have "(1) suffered an injury in fact, (2) that is fairly traceable to the challenged conduct of the defendant, and (3) that is likely to be redressed by a favorable judicial decision." *Id.*

Rule 23 is not an end-run around the standing requirement. "Rule 23's requirements must be interpreted in keeping with Article III constraints, and with the Rules Enabling Act, which instructs that rules of procedure 'shall not abridge, enlarge or modify any substantive right,' 28 U.S.C. § 2072(b)." *Amchem Prod., Inc. v. Windsor*, 521 U.S. 591, 613 (1997). So each class member must demonstrate standing before an award in his favor, *TransUnion LLC v. Ramirez*, 141 S. Ct. 2190, 2208 (2021), and indeed must establish standing at the successive stages of the litigation "with the manner and degree of evidence required at" those stages, *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 561 (1992). Thus, "whether absent class members can establish standing may be exceedingly relevant to the class certification analysis required by Federal Rule of Civil Procedure 23." *Cordoba v. DIRECTV, LLC*, 942 F.3d 1259, 1273 (11th Cir. 2019). In particular, common issues will not predominate if "many claims of the absent class members" are not justiciable. *Id.*

In consumer data breach cases, identification of a putative class that can meet Article III and Rule 23 requirements will often prove impossible. Modern systems for gathering and storing customer data

have made large data breaches increasingly common. *See* Turner, Walker, and Moore, Data Flows, Technology, and the Need for National Privacy Legislation, at 26, U.S. Chamber of Commerce Technology Engagement Center and Political and Economic Research Council (2019). But most data breaches do not result in either fraud on an existing account or identity theft. *Tsao*, 986 F.3d at 1343. Thus, "[e]vidence of a mere data breach does not, standing alone, satisfy the requirements of Article III standing." *Id.* at 1344.

Instead, a putative data breach class must show a "substantial risk" of harm that is "certainly impending." *Id.* at 1344. "[T]hreadbare allegations" of potential harm will not satisfy this standard. *Id.* at 1343. Nor can a plaintiff rely on self-inflicted injuries following a data breach to establish standing. *Id.* at 1345. Instead, each plaintiff must advance evidence to show that the data breach presented a substantial and certainly impending threat of harm to him. *See id.* at 1343 (explaining that reports about the general risk of identity theft failed to show a risk "in this case") (emphasis omitted).

This Court has already correctly held that allegations of a data breach without any specific evidence of actual misuse of the data will not

ordinarily suffice to establish standing. In *Tsao*, the plaintiff argued that a "substantial risk of identity theft, fraud, and other harm in the future as a result of the data breach" met his burden to establish Article III standing. *Tsao*, 986 F.3d at 1340. This Court, however, found that the data breach did not create a substantial risk of certainly impending harm. Relying on a 2007 Report from the United States Government Accountability Office, the Court noted that most data breaches do not result in either identity theft or fraudulent charges. *Id.* at 1343. Moreover, even absent the GAO report, the Court explained that it would still conclude that "vague, conclusory allegations" of "actual misuse" were not enough to establish standing. *Id.* Instead, a plaintiff must show "specific evidence" of either "actual misuse of class members' data" or some other facts that would raise a substantial risk of certainly impending harm in the case. *Id.* at 1344.

*Tsao* similarly held that "efforts to mitigate the risk of identity theft caused by the data breach" are themselves insufficient to establish standing. *Id.* Mitigation efforts like the cancellation of credit cards in *Tsao* are "inextricably tied" to the plaintiff's "perception of the actual risk of identity theft." *Id.* Since "it is well established that plaintiffs 'cannot

manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending," these self-imposed harms are insufficient for standing. *Id.* (quoting *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 416, 133 S. Ct. 1138, 1151 (2013)).

The district court's certification order conflicts with both of these holdings. The district court certified both a nationwide and a California class composed of customers 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." Doc. 167 at 16. The court believed that this class definition would "avoid later predominance issues regarding standing and the inclusion of uninjured individuals." *Id.* The court reasoned that class members would be able to show "that they have had their data 'misused' . . . , either through experiencing fraudulent charges or it being posted on the dark web." *Id.* Moreover, it concluded that "individuals must have some injury in the form of out-of-pocket expenses or time spent to be a part of the class." *Id.*

The district court's reasoning cannot be reconciled with *Tsao*. Starting with the requirement of a substantial risk of injury, the district

court read *Tsao*'s instruction that a plaintiff will ordinarily need to show some "actual misuse" to mean that any action that could be labelled "misuse" is enough to establish standing. *Tsao*, 986 F.3d at 1344. But that is not what *Tsao* held. *Tsao* held that a plaintiff in a data breach case must show a substantial risk of such harm that is certainly impending. *Id.* Alleged "misuse" of data is therefore relevant only to the extent that it is the kind of "misuse" that poses a substantial risk of imminent harm. *See id.*

The mere fact of having one's information accessed in a data breach and posted on the dark web does not create a substantial risk of imminent harm. To begin, *Tsao* confirmed that the mere act of having information accessed does not meet this standard. While *Tsao* noted that the GAO Report that it relied on "is over a decade old," more recent research bolsters *Tsao*'s conclusion that a breach involving customer data does not present a substantial risk of harm. *Id.* at 1343. The U.S. Chamber of Commerce Technology Engagement Center and the Political and Economic Research Council published a detailed study on the risks of data breaches in 2019. *See* Data Flows, Technology, and the Need for National Privacy Legislation. Like the GAO report, this Report found

that "individuals involved in data breaches (overall) are not at an especially high risk for ID theft or fraud." *Id.* at 37. In fact, it found that "[o]nly a very small share of all breached records could possibly translate to annual incidents of ID theft." *Id.* Data show that there is "very little change in the rate of ID theft and fraud" even when there is a substantial increase in data breaches. *Id.* at 35.

The posting of information on the "dark web" does not change this analysis. Information that was part of a data breach should appear on the dark web at a higher rate than other information if data-breach perpetrators routinely relied on the dark web to market personal information. But that is not what the data show. The U.S. Chamber Report compared the rate at which personal data appeared on the dark web between two groups with credit monitoring. The first group obtained credit monitoring because of a data breach, and the second group consisted of individuals who had obtained direct-to-consumer credit monitoring. *Id.* at 43. The Report found "no practical difference . . . in the rate of whether Dark Web data was detected from the consumer between the two groups." *Id.* at 47. This suggests that consumers who have their data breached and put on the dark web are not at a materially

greater risk of imminent identity theft or fraudulent charges than other individuals. For this reason, the Eighth Circuit has held that allegations that "illicit websites are selling [the plaintiffs'] Card Information to counterfeiters and fraudsters" did not show the kind of misuse that could establish standing. *In re SuperValu, Inc.*, 870 F.3d 763, 770 (8th Cir. 2017). In *Tsao*, this Court was "persuaded" by that decision. 986 F.3d at 1343. In today's modern world, there are simply too many data breaches that never result in any actual harm to the consumer, including breaches that result in information being placed on the dark web, for the mere occurrence of a data breach to ground Article III standing.

The district court's effort to cure the standing problems in this case by defining the class to include only individuals who had incurred expenses or lost time in response to the data breach also runs headlong into *Tsao*. Indeed, *Tsao* expressly rejected the idea that this kind of self-imposed harm could overcome the absence of a substantial risk of injury. Actions taken because of "fears of hypothetical future harm that is not certainly impending" have no role in establishing standing. *Id.* at 1344 (quoting *Clapper*, 568 U.S. at 416, 133 S. Ct. at 1151).

The district court's attempt to evade the limitations of *Tsao*, if affirmed, will invite a deluge of wasteful litigation in this Circuit. Since data breaches are common but harm resulting from a data breach is rare, courts have consistently rejected attempts to invoke the jurisdiction of the federal courts without a showing of the kind of misuse that creates an imminent risk to a consumer. *See Tsao*, 986 F.3d at 1343. The district court's approach, however, would permit a plaintiff to invoke the jurisdiction of the federal courts by citing any action labeled a "misuse" even if there was never a risk of imminent harm. That lax approach to standing would draw data breach suits to this Circuit, creating substantial costs both for the courts and for defendants. And these burdens cannot be justified by any vindication of the rights of plaintiffs: the district court's approach would be necessary only when a plaintiff could not show any misuse that presents a risk of imminent harm.

## II. The district court's classes will require individual proceedings on class membership that will predominate over common issues.

Putting aside the district court's failure to understand what is necessary to show standing after a data breach, the district court's class definitions will ensure that individualized issues predominate over common issues. This Court has decertified a class where "each plaintiff

will likely have to provide some individualized proof that they have standing." *Cordoba*, 942 F.3d at 1275. And here, although it attempted to tailor the classes to meet the requirements for standing, the district court failed to recognize that this case will unavoidably require precisely such individual mini-trials to determine class membership. The district court's order defines each of the classes to include only individuals who spent funds or time responding to the data breach. Determining whether a plaintiff meets this standard would require an individual adjudication of whether that plaintiff took any action in response to the breach. *See TransUnion*, 141 S. Ct. at 2208 (explaining that each plaintiff "must demonstrate standing for each claim that they press"). Those individual inquiries would predominate over any common issues in violation of Rule 23.

## III. The imposition of damages based only on "averages" unconnected to harm actually suffered by particular plaintiffs violates the Rules Enabling Act and Supreme Court precedent.

Plaintiffs failed to meet their burden on predominance in this case for a second reason as well: they have failed to identify any method for establishing damages that can be done on a common basis without altering the substantive rights of the defendant. This Court has long held

that the predominance inquiry prohibits class certification where individual issues concerning damages will predominate over other issues. *See Sacred Heart Health Sys., Inc. v. Humana Mil. Healthcare Servs., Inc.*, 601 F.3d 1159, 1178–79 (11th Cir. 2010). Claims involving "extensive individualized inquiries on . . . issues of . . . damages" cannot be resolved through a class action. *Sikes v. Teleline, Inc.*, 281 F.3d 1350, 1366 (11th Cir. 2002) *abrogated on other grounds by Bridge v. Phoenix Bond & Indem. Co.*, 553 U.S. 639, 128 S. Ct. 2131 (2008). But to avoid this problem, the district court approved a method of damages that will alter the substantive rights of the parties.

The district court found that individual issues of damages would not predominate because an "averages method" could be employed to determine damages. Doc. 167 at 7. Under this method, class members would receive awards based on the damages incurred by an average class member without showing that the individual class member had sustained any corresponding injury. The district court explained that "all class members would receive a standard dollar amount for lost opportunities to accrue rewards points (whether or not they used a rewards card), the value of cardholder time (whether or not they spent

any time addressing the breach), and out-of-pocket damages (whether or not they incurred any out-of-pocket damages)." *Id.*

This kind of "averages method" cannot be used to evade individualized issues related to damages. Rule 23 is an exception to the ordinary requirement that each individual plaintiff's claim must be proven through a separate proceeding. But it does not—and cannot—permit a plaintiff to recover an award without showing that the individual plaintiff is entitled to that award.

The Supreme Court has rejected this kind of "averages" proof of classwide damages in a class action proceeding. In *Wal-Mart Stores, Inc. v. Dukes*, 564 U.S. 338, 367, 131 S. Ct. 2541, 2561 (2011), the Court rejected an attempt to recover through "Trial by Formula." There, the class-action plaintiffs proposed to prove their claims by having a special master determine "liability for sex discrimination and the backpay owing as a result" for a "sample set of the class action members." *Id.* To determine the award to "the entire class," "[t]he percentage of claims determined to be valid would then be applied to the entire remaining class, and the number of (presumptively) valid claims thus derived would be multiplied by the average backpay award in sample set . . . without

further individualized proceedings." *Id.* The Court "disapprove[d]" of "that novel project," noting that "the Rules Enabling Act forbids interpreting Rule 23 to 'abridge, enlarge or modify any substantive right.'" *Id.* (quoting 28 U.S.C. § 2072(b)). Since the defendant must be able to present "defenses to individual claims," this scheme to avoid individual proceedings could not proceed.

The proposed damages methodology endorsed by the district court presents a similar attempt to recover based on averages untethered to the circumstances of any individual claim. The district court acknowledged that the model looked to the "standard dollar amount" of various potential harms and provided an award "whether or not" each plaintiff had actually suffered those harms. Doc. 167 at 7. This Court should reject this "novel project." *Dukes*, 564 U.S. at 367, 131 S. Ct. at 2561.

Contrary to the suggestion of the district court, *Tyson Foods, Inc. v. Bouaphakeo*, 577 U.S. 442, 459–61, 136 S. Ct. 1036, 1048–49 (2016), did not generally "approve[] the use of averages methods to calculate damages." Doc. 167 at 7. Rather, *Tyson Foods* held that averages could be used in a class action proceeding only when they "could have been used

to establish liability in an individual action." *Id.* at 458, 136 S. Ct. at 1048. Permitting recovery based on an average that would not be sufficient in an individual action "would . . . violate[] the Rules Enabling Act by giving plaintiffs and defendants different rights in a class proceeding than they could have asserted in an individual action." *Id.*

*Tyson* confirms that the damages methodology relied on by the district court cannot be used in a class action proceeding. That model relies on averages that would have no role in an individual proceeding. For example, in a non-class case, a plaintiff who never used a rewards card could not point to "a standard dollar amount for lost opportunities to accrue rewards points" to recover damages, but here, the district court approved reliance on this average for all putative class members "whether or not" a plaintiff "used a rewards card." Doc. 167 at 7. This kind of average with no relationship to an individual's actual damages is exactly the kind of evidence that *Tyson* found would violate the Rules Enabling Act.

## IV. Improper class actions impose substantial costs on the business community.

The failure to rigorously police class actions imposes substantial harms on the business community and the public more broadly. If classes

are certified even when members of the class cannot show Article III injury, as in this case, then burdensome class action litigation driven by the interests of attorneys rather than claimants will only increase, without any countervailing benefit to class members. The consequences for the judicial system, as well as for businesses, their owners, customers, and employees will be extraordinarily damaging.

Class-action litigation costs in the United States are huge. They totaled a staggering $2.64 billion in 2019, continuing a rising trend that started in 2015. *See* 2020 Carlton Fields Class Action Survey, at 4 (2020), *available at* https://ClassActionSurvey.com. The cost to defend a single large class action can run into nine figures. *See* Adeola Adele, *Dukes v. Wal-Mart: Implications for Employment Practices Liability Insurance* 1 (July 2011) (noting defense cost of $100 million). And such actions can drag on for years even before a court takes up the question of class certification. *See* U.S. Chamber Institute for Legal Reform, *Do Class Actions Benefit Class Members? An Empirical Analysis of Class Actions*, at 1, 5 (Dec. 2013), *available at* http://bit.ly/3rrHd29 ("Approximately 14 percent of all class action cases remained pending four years after they

were filed, without resolution or even a determination of whether the case could go forward on a class-wide basis.").

The certification of a class also places immense pressure to settle on defendants. "Certification of a large class may so increase the defendant's potential damages liability and litigation costs that he may find it economically prudent to settle and to abandon a meritorious defense." *Coopers & Lybrand v. Livesay*, 437 U.S. 463, 476 (1978) *superseded by rule on other grounds as stated in Microsoft Corp. v. Baker*, 137 S. Ct. 1702 (2017).

This case provides a useful example of how failure to enforce the limits on class actions imposes costs with no countervailing benefit. Based on its misunderstanding of the requirement of "misuse" to show standing in a data breach case, the district court certified two classes that included any individual whose data was accessed in this breach and posted to the dark web who undertook some mitigation efforts. This decision would require Brinker to engage in expensive litigation even though a substantial number of class action plaintiffs will never suffer harm from the underlying data breach. These potential costs would be exacerbated by the district court's creation of a class that would require

separate litigation to determine class membership of each individual unnamed class member. Worse still, Brinker would face the prospect of damages imposed on the basis of "average" calculations without any individual plaintiff having to prove corresponding injury.

If not corrected by this Court, the decision below will only lead to increased litigation that could have been avoided, and litigation divorced from Article III cases or controversies and Rule 23's class certification requirements. These suits will only increase the already immense pressure to settle improperly brought class actions. This harms the entire economy because the costs of defending and settling abusive class actions are ultimately absorbed by consumers and employees through higher prices or lower wages.

## CONCLUSION

The decision of the district court should be reversed.

Dated: November 23, 2021 Respectfully submitted,

*/s/ Gilbert C. Dickey*

Gilbert C. Dickey
McGuireWoods LLP
201 North Tryon Street
Suite 3000
Charlotte, NC 28202
T: (704) 343-2396
F: (704) 444-8854
gdickey@mcguirewoods.com

Andrew R. Varcoe
Jennifer B. Dickey
U.S. Chamber Litigation Center
1615 H Street, NW
Washington, DC 20062
T: (202) 463-5337

*Counsel for Amicus Curiae*
*The Chamber of Commerce of the*
*United States of America*

## CERTIFICATE OF COMPLIANCE

I hereby certify that this brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5), the type style requirements of Fed. R. App. P. 32(a)(6), and the type-volume limitations of Fed. R. App. P. 29(a)(5) because it is proportionally spaced, has a typeface of 14-point Century font, and contains 4,242 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(f).

*/s/ Gilbert C. Dickey*
Gilbert C. Dickey

## CERTIFICATE OF SERVICE

I hereby certify that on November 23, 2021, the foregoing was electronically filed with the Clerk for the United States Court of Appeals for the Eleventh Circuit using the CM/ECF system. The system will serve all counsel of record.

*/s/ Gilbert C. Dickey*
Gilbert C. Dickey