

[PUBLISH]

In the
United States Court of Appeals
For the Eleventh Circuit

No. 21-13146

MARLENE GREEN-COOPER,
individually and on behalf of all others similarly situated, et al.,
Plaintiffs,

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

versus

BRINKER INTERNATIONAL, INC.,

2

Opinion of the Court

21-13146

Defendant-Appellant.

Appeal from the United States District Court
for the Middle District of Florida
D.C. Docket No. 3:18-cv-00686-TJC-MCR

Before WILSON, BRANCH, and TJOFLAT, Circuit Judges.

TJOFLAT, Circuit Judge:

Brinker International, Inc. (“Brinker”), the owner of Chili’s restaurants, faced a cyber-attack in which customers’ credit and debit cards were compromised. Chili’s customers have brought a class action because their information was accessed (and in some cases used) and disseminated by cybercriminals. Below, the District Court certified the class, and Brinker appeals that decision. We vacate in part and remand for further proceedings.

I.

Between March and April 2018, hackers targeted the Chili’s restaurant systems and stole both customer card data and personally identifiable information.¹ Plaintiffs explain that hackers then took that data and posted it on Joker Stash, an online marketplace

¹ Different locations were affected at different periods within this timeframe.

for stolen payment data. The plaintiffs explain that, based on Brinker's internal reporting, the information for all 4.5 million cards the hackers accessed in the Brinker system were found on Joker Stash.

There are three named plaintiffs in this case: Shenika Theus, Michael Franklin, and Eric Steinmetz.² Theus is a Texas resident who used her card at Chili's in Texas on or about March 31, 2018. She experienced five unauthorized charges on the card she had used at Chili's and canceled the card as a result, disputing the charges that were not hers. She now spends time monitoring her account to make sure there is no further misuse.

Franklin is a California resident who made two Chili's purchases in the relevant timeframe, one on or about March 17, 2018, and one on or about April 22, 2018. Franklin experienced two unauthorized charges on his account, so he canceled that credit card, spoke for hours on the phone with bank representatives, and went to the Chili's locations he had visited to collect receipts for his transactions.³ His bank canceled the affected card.

² These plaintiffs, originally filing individual actions, moved to consolidate their cases. The District Court granted that motion.

³ The locations Franklin visited were affected by the data breach between March 30, 2018–April 22, 2018, and March 22, 2018–April 21, 2018, respectively. Franklin visited the first Chili's on or about March 17, 2018, 13 days before the affected period, and he visited the second Chili's on or about April

Steinmetz is a Nevada resident who used his credit card at a Nevada Chili's on or about April 2, 2018. Steinmetz called the Chili's national office, the local Chili's chain, credit reporting agencies, and his bank as a result of the data breach. He canceled the card he used at Chili's but never experienced fraudulent charges.

Pertinent to this appeal,⁴ these three plaintiffs moved to certify two classes under Federal Rules of Civil Procedure 23(a) and 23(b)(3),⁵ seeking both injunctive and monetary relief: 1) a nationwide class (or alternatively a statewide class) for negligence and 2) a California statewide class for California consumer protection claims based on its unfair business practices state laws. They were defined as follows:

1. 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 (the "Nationwide Class").
2. All persons residing in California who made a credit or debit card purchase at any affected Chili's

22, 2018, one day after the affected period for the second Chili's. His card had also previously been compromised in a Whole Foods data breach in 2017.

⁴ Plaintiffs originally brought a variety of other claims that are not before us. We do not address them here.

⁵ Plaintiffs proffered a declaration from a damages expert to establish that a common methodology for calculating damages for individual class members existed.

21-13146

Opinion of the Court

5

location during the period of the Data Breach (the “California Statewide Class”).

The District Court then certified the nationwide class for the negligence claim as follows:

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 “Nationwide Class”).

The District Court also certified a separate California class under the state unfair competition laws:

All persons residing in California 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 “California Statewide Class”).

We then permitted Brinker to appeal these class certifications pursuant to Federal Rule of Civil Procedure 23(f).

II.

We review a district court’s certification of a class under Federal Rule of Civil Procedure 23 for abuse of discretion. *Hines v. Widnall*, 334 F.3d 1253, 1255 (11th Cir. 2003). A district court

abuses its discretion when it certifies a class that does not meet the requirements of Rule 23. *See id.* (“In order to certify a class under the FRCP, all of the requirements of Rule 23(a) must be met, as well as one requirement of Rule 23(b).”).

Class certification under Rule 23(b)(3), like in this case, is only appropriate if “the trial court is satisfied, after a rigorous analysis, that the prerequisites of Rule 23(a) have been satisfied” and that “the questions of law or fact common to class members predominate over any questions affecting only individual members” through “evidentiary proof.” *Comcast Corp. v. Behrend*, 569 U.S. 27, 33, 133 S. Ct. 1426, 1432 (2013) (internal quotation marks and citations omitted). Rule 23 is more than “a mere pleading standard. A party seeking class certification must affirmatively demonstrate his compliance with the Rule—that is, he must be prepared to prove [the existence of the elements of Rule 23].” *Wal-Mart Stores, Inc. v. Dukes*, 564 U.S. 338, 350, 131 S. Ct. 2541, 2551 (2011).

At the same time, “[m]erits questions may be considered to the extent—but only to the extent—that they are relevant to determining whether the Rule 23 prerequisites for class certification are satisfied,” so a district court does not have a free-ranging “authority to conduct a preliminary inquiry into the merits of a suit” at the class certification stage “unless it is necessary to determine the propriety of certification.” *Amgen Inc. v. Conn. Ret. Plans & Tr. Funds*, 568 U.S. 455, 466, 133 S. Ct. 1184, 1195 (2013) (internal quotation marks and citations omitted).

21-13146

Opinion of the Court

7

III.

On appeal, Brinker mounts three arguments: 1) the District Court’s class certification order violates our precedent on Article III standing for class actions; 2) the District Court improvidently granted certification because the class will eventually require individualized mini-trials on class members’ injuries; and 3) the District Court erred by finding that a common damages methodology existed for the class. We will address each in turn.

IV.

A.

We start from the basic principle that at the class certification stage only the named plaintiffs need have standing.⁶ *Cordoba v. DIRECTV, LLC*, 942 F.3d 1259, 1264 (11th Cir. 2019). Article III standing requires that 1) the plaintiff has experienced an injury that is concrete and particularized and actual or imminent, 2) the defendant’s conduct is the cause of the plaintiff’s injury, and 3) a

⁶ We may review both the allegations in the complaint and evidence in the record so far to determine whether the named plaintiffs in this case have established Article III standing for class certification purposes. *Cordoba v. DIRECTV, LLC*, 942 F.3d 1259, 1264, 1271 (11th Cir. 2019) (looking at the allegations of named plaintiff to determine whether he had standing); *Prado-Steiman ex rel. Prado v. Bush*, 221 F.3d 1266, 1280–81 (11th Cir. 2000) (evaluating both named plaintiffs’ allegations and the lack of evidence of injury in the record for some claims while analyzing Article III standing); *Griffin v. Dugger*, 823 F.2d 1476, 1482 (11th Cir. 1987) (“Under elementary principles of standing, a plaintiff must allege and show that he personally suffered injury.”).

decision by the court would likely redress the plaintiff's injury. *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 560–61, 112 S. Ct. 2130, 2136 (1992). As we'll explain, only Theus satisfies *Lujan*'s standing analysis.

We begin with the concrete injury analysis. For purposes of the concrete injury analysis under Article III, we have recognized three kinds of harm: 1) tangible harms, like “physical or monetary harms”; 2) intangible harms, like “injuries with a close relationship to harms traditionally recognized as providing a basis for lawsuits in American courts”;⁷ and, finally, 3) a “material risk of future harm” when a plaintiff is seeking injunctive relief. *TransUnion LLC v. Ramirez*, 141 S. Ct. 2190, 2204, 2210 (2021). And the Supreme Court most recently clarified in *TransUnion* that a mere risk of future harm, without more, does not give rise to Article III standing for recovery of damages, even if it might give rise to Article III standing for purposes of injunctive relief. *Id.* at 2210. We will take each of the named plaintiff's standing analysis in turn.

While each plaintiff puts forth a variety of allegations of harm in an effort to establish Article III standing, we need only

⁷ Constitutional harms, like violations of the First Amendment, and reputational harms, neither of which is at issue here, are examples of traditional harms for purposes of Article III standing. *TransUnion LLC v. Ramirez*, 141 S. Ct. 2190, 2204 (2021). Stigmatic harm is another example of intangible injury giving rise to Article III standing. *Laufer v. Arpan LLC*, 29 F.4th 1268, 1273 (11th Cir. 2022). Informational injuries can also give rise to Article III standing as intangible harms. *TransUnion*, 141 S. Ct. at 2214.

address one: hackers took these individuals' data and posted it on Joker Stash.

We said in *Tsao* that a plaintiff whose personal information is subject to a data breach can establish a concrete injury for purposes of Article III standing if, as a result of the breach, he experiences “misuse” of his data in some way. *See Tsao v. Captiva MVP Rest. Partners, LLC*, 986 F.3d 1332, 1343 (11th Cir. 2021). 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. *Id.* at 1343, 1344 (“[W]ithout specific evidence of *some* misuse of class members’ data, a named plaintiff’s burden to plausibly plead factual allegations sufficient to show that the threatened harm of future identity theft was ‘certainly impending’—or that there was a ‘substantial risk’ of such harm—will be difficult to meet.” (emphasis in original and citation omitted)).

All three plaintiffs maintain that their credit card and personal information was “exposed for theft and sale on the dark web.” That allegation is critical. The fact that hackers took credit card data and corresponding personal information from the Chili’s restaurant systems and affirmatively posted that information for sale on Joker Stash is the misuse for standing purposes that we said was missing in *Tsao*.⁸ And it establishes both a present injury—

⁸ In *Tsao*, we said that a plaintiff had not established standing based on a state common-law negligence claim after a data breach where he alleged only that

credit card data and personal information floating around on the dark web—and a substantial risk of future injury—future misuse of personal information associated with the hacked credit card. We hold that this is a concrete injury that is sufficient to establish Article III standing.⁹

he had canceled his credit card and faced an increased risk of identity theft because the credit card system at a restaurant he visited had been hacked. *Tsao*, 986 F.3d at 1344. We said that because Tsao had not accompanied his allegations of increased risk of identity theft with allegations of misuse of any credit card data taken by the hackers in the restaurant breach, he could not meet Article III standing requirements. *Id.*

⁹ We decided *Tsao* before *TransUnion* was published, but we see the two as consistent. *TransUnion* established that a common-law analogue analysis is required when plaintiffs allege a statutory violation. We did not conduct that analysis in *Tsao* in the context of a state common-law negligence claim. See *TransUnion*, 141 S. Ct. at 2208. But we think that the common-law analogue analysis is *sui generis* to legislature-made statutory violations because the Supreme Court has not applied it to any other kind of intangible harm. For instance, constitutional harms, reputational harms, informational harms, and stigmatic harms are all intangible injuries that give rise to Article III standing, and the Supreme Court has never conducted the common-law analogue analysis in determining whether these kinds of harms establish Article III standing. See *Church of the Lukumi Babalu Aye, Inc. v. City of Hialeah*, 508 U.S. 520, 531, 113 S. Ct. 2217, 2225 (1993) (infringement of free exercise); *Meese v. Keene*, 481 U.S. 465, 473, 107 S. Ct. 1862, 1867 (1987) (reputational harms); *TransUnion*, 141 S. Ct. at 2214 (identifying informational injuries as intangible harms); *Laufer*, 29 F.4th at 1272–73 (recognizing that under Supreme Court precedent both stigmatic and emotional harms have sufficed to establish Article III standing). So, we adhere to the reasoning of *Tsao* today. See *United States v. Gillis*, 938 F.3d 1181, 1198 (11th Cir. 2019) (explaining the prior panel precedent rule).

B.

Although all three plaintiffs adequately allege a concrete injury sufficient for Article III standing, Franklin and Steinmetz’s allegations face a fatal causation issue, even at this stage of litigation.¹⁰

The Third Amended Complaint alleged that Franklin visited two Chili’s restaurants during March and April of 2018; one in Carson, California, and one in Lakewood, California. The at-risk timeframe for the Chili’s in Carson was subsequently determined to be March 30, 2018, to April 22, 2018. Franklin visited the Carson Chili’s on March 17, 2018—well outside the affected period. The District Court correctly concluded that “Franklin’s first transaction would not qualify him for the class without additional evidence, as he dined several days outside the affected time range.”

The at-risk timeframe for the Chili’s in Lakewood was March 22, 2018, to April 21, 2018. Franklin visited the Lakewood Chili’s on April 22, 2018—a day shy of the affected period. Falling outside the affected period poses a traceability problem for Franklin’s allegations. Without any allegation that he dined at a Chili’s during the time that *that* Chili’s was compromised in the data breach, Franklin fails to allege that his injury was “fairly . . . trace[able] to the challenged action of the defendant.” *Lujan*, 504

¹⁰ Theus visited a Chili’s location during the breach period for that location. As such, her alleged injuries are fairly traceable to the Chili’s data breach.

U.S. at 560, 112 S. Ct. at 2136 (alterations in original) (internal quotation marks and citation omitted).¹¹

The Third Amended Complaint also alleged that Steinmetz dined at the North Las Vegas Chili's on April 4, 2018. The at-risk time frame for the North Las Vegas Chili's was subsequently determined to be April 4, 2018, to April 21, 2018. Therefore, if Steinmetz's alleged dining date is true, he falls within the affected period. The record, however, shows that the allegation was slightly—but importantly—off the mark. Steinmetz stated in response to an interrogatory and in his deposition that he dined at the North Las Vegas Chili's on April 2, 2018.¹²

Much like with Franklin, therefore, Steinmetz does not have standing because the date he dined at Chili's is right outside of the affected date range for that Chili's. The proof required for a plaintiff to establish standing varies depending on the stage of litigation.

¹¹ The District Court found that “while [Franklin's Lakewood Chili's transaction was] one day outside the [affected] range,” Brinker's chart indicating the affected time periods for various Chili's locations indicated that the end date of the affected period “could not [be] validate[d].” Therefore, the District Court included Franklin as part of the class due to that wiggle room in the affected date range. But this was error. Although the Brinker chart included a “[c]ould not validate date” disclaimer for its April 22, 2018, end date for the Carson Chili's, the chart did not include such a disclaimer for the Lakewood Chili's.

¹² Steinmetz initially stated in his deposition that he dined at the Chili's on April 3, 2018, but later corrected himself when faced with documentation to the contrary that he dined there on April 2.

21-13146

Opinion of the Court

13

Lujan, 504 U.S. at 561, 112 S. Ct. at 2136 (“Since [the standing elements] are not mere pleading requirements but rather an indispensable part of the plaintiff’s case, each element must be supported in the same way as any other matter on which the plaintiff bears the burden of proof, *i.e.*, with the manner and degree of evidence required at the successive stages of the litigation.”). At the class certification stage, “it may be necessary for the court to probe behind the pleadings” to assess standing. *Gen. Tel. Co. of Sw. v. Falcon*, 457 U.S. 147, 160, 102 S. Ct. 2364, 2372 (1982).

Where, as here, the facts developed in discovery firmly contradict the allegation in the complaint, the District Court cannot rely on the complaint’s factual allegation. Plaintiffs make no argument and provide no additional facts to cast doubt on Steinmetz’s discovery admissions that he dined at Chili’s *outside* of the at-risk time period. He therefore cannot fairly trace any alleged injury to Brinker’s challenged action. *See Lujan*, 504 U.S. at 560, 112 S. Ct. at 2136.

C.

Having determined that one named plaintiff has standing, we turn to the class definitions because Rule 23(b)(3)’s predominance analysis implicates Article III standing. *Cordoba*, 942 F.3d at 1272–73 (“In some cases, whether absent class members can establish standing may be exceedingly relevant to the class certification analysis required by Federal Rule of Civil Procedure 23.”). The predominance inquiry is especially important in light of *TransUnion*’s (and *Cordoba*’s) reminder that “every class member must

have Article III standing in order to recover individual damages” because a district court must ultimately weed out plaintiffs who do not have Article III standing before damages are awarded to a class. *TransUnion*, 141 S. Ct. at 2208; *Cordoba*, 942 F.3d at 1264 (“At some point before it may order any form of relief to the putative class members, the court will have to sort out those plaintiffs who were actually injured from those who were not.”).

Turning to the class definitions the District Court certified, we have the following:

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 “Nationwide Class”).

...

All persons residing in California 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 “California Statewide Class”).

The District Court explained that its class definitions “avoid later predominance issues regarding standing and the inclusion of

uninjured individuals because now individuals are not in the class unless they have had their data ‘misused’ per the Eleventh Circuit’s *Tsao* decision, either through experiencing fraudulent charges or it being posted on the dark web.” So, under the class definitions, the District Court thought that the phrase “data accessed by cybercriminals” meant either that an individual had experienced fraudulent charges or that the hacked credit card information had been posted on the dark web. And, to make sure to clear any standing bar imposed by *Tsao*, the District Court added an additional requirement that the individuals in the class must have tried to mitigate the consequences of the data breach.

While the District Court’s interpretation of the class definitions surely meets the standing analysis we have outlined above for named plaintiff Theus, we note that the phrase in the class definitions “accessed by cybercriminals” is broader than the two delineated categories the District Court gave, which were limited to cases of fraudulent charges or posting of credit card information on the dark web. Therefore, we think it wise to remand this case to give the District Court the opportunity to clarify its predominance finding. It may either refine the class definitions to only include those two categories and then conduct a more thorough predominance analysis,¹³ or the District Court may instead conduct a

¹³ The District Court centered its predominance analysis around the fact that it thought it had created class definitions in which all members of the class had standing. And, while that calculus is part of the predominance inquiry, *Cordoba*, 942 F.3d at 1276, refining the class definitions is not necessary or

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 under *Tsao*, who have simply had their data accessed by cybercriminals and canceled their cards as a result. *See Cordoba*, 942 F.3d at 1274 (“The essential point, however, is that at some time in the course of the litigation the district court will have to determine whether each of the absent class members has standing before they could be granted any relief.”).

On remand, the District Court should also determine the viability of the California class afresh. As discussed *supra* part IV.B, Franklin does not have standing to bring the alleged causes of action against Brinker, including the causes of action based in California state law. Without a named plaintiff with standing to bring the California claims, the California class cannot survive.

V.

With standing sorted out, we are left with Brinker’s final claim that individualized damages claims will predominate over

sufficient to satisfy the predominance inquiry as to standing under *Cordoba*. In the predominance analysis, a district court must determine whether “each plaintiff will likely have to provide some individualized proof that they have standing.” *Id.* at 1275. The District Court here did not determine whether its class definitions would require individualized proof of standing, especially as to time or effort expended to mitigate the consequences of the data breach. So, remand is appropriate to afford the District Court the opportunity to perform that analysis.

the issues common to the class under Rule 23(b)(3). As a starting point, “the presence of individualized damages issues does not prevent a finding that the common issues in the case predominate.” *Allapattah Servs., Inc. v. Exxon Corp.*, 333 F.3d 1248, 1261 (11th Cir. 2003). Individualized damages issues predominate if “computing them will be so complex, fact-specific, and difficult that the burden on the court system would be simply intolerable” or if “significant individualized questions go[] to liability.” *Brown v. Electrolux Home Prods., Inc.*, 817 F.3d 1225, 1240 (11th Cir. 2016) (internal quotation marks omitted) (citing *Klay v. Humana, Inc.*, 382 F.3d 1241, 1260 (11th Cir. 2004), *abrogated in part on other grounds by Bridge v. Phoenix Bond & Indem. Co.*, 553 U.S. 639, 128 S. Ct. 2131 (2008)). And “[i]ndividualized damages issues are of course least likely to defeat predominance where damages can be computed according to some formula, statistical analysis, or other easy or essentially mechanical methods.” *Sacred Heart Health Sys., Inc. v. Humana Mil. Healthcare Servs., Inc.*, 601 F.3d 1159, 1179 (11th Cir. 2010) (internal quotation marks and citation omitted).

At the class certification stage, all that the named plaintiffs had to prove was that a reliable damages methodology existed, not the actual damages plaintiffs sustained. Plaintiffs must demonstrate that a “model purporting to serve as evidence of damages in this class action . . . measure[s] only those damages attributable to that theory.” *Comcast*, 569 U.S. at 35, 133 S. Ct. at 1433. And “[t]he first step in a damages study is the translation of the *legal theory of*

the harmful event into an analysis of the economic impact *of that event.*” *Id.* at 38, 133 S. Ct. at 1435 (emphasis in original and citation omitted). Here, plaintiffs’ expert provided the District Court with a common methodology for calculating damages based on “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).”¹⁴ The plaintiffs’ expert used a damages methodology based on averages because the expert believed the “delta between class members’ damages is minimal irrespective of the type of card used or time spent.”

¹⁴ Plaintiffs’ expert does not purport to provide a damages methodology based on averages to determine actual damages for each plaintiff sustained as a result of the misuse of their personal information. Such inquiry into actual damages would surely be an individual inquiry. Rather, according to the expert, the out-of-pocket damages category includes:

such items as penalties paid by cardholders in connection with not being able to use their cards to pay bills on time, gasoline to go back to the retail establishment where the breach occurred or to the cardholder’s bank or local police station, postage and stationary, overnight replacement card shipping fees, bank charges to replace cards (while unusual this cost does occur on occasion), ATM fees to get access to cash, and hiring a third party to assist cardholder recovery and security efforts.

The expert stated that data breaches typically yield damages attributable to this category somewhere in the ballpark of \$38 per plaintiff.

In our analysis of a damages methodology based on averages, the focus is on “whether the sample at issue could have been used to establish liability in an individual action.” *Tyson Foods, Inc. v. Bouaphakeo*, 577 U.S. 442, 458, 136 S. Ct. 1036, 1048 (2016). In this case, each Chili’s customer fitting within the class definitions experienced a similar injury of a compromised card combined with some effort to mitigate the harm caused by the compromise. So, the damages methodology is not “enlarg[ing] the class members’ substantive rights” by giving class members an award for an injury they could not otherwise prove in an individual action. *Id.* (internal alterations, quotation marks, and citation omitted). Through the District Court’s rigorous analysis, it found that at the class certification stage the damages model was sufficient, and it would be a “matter for the jury” to decide actual damages at trial. *Id.* at 459, 136 S. Ct. at 1049. Any individual inquiry into particularized damages resulting from the data breach, such as damages recoverable due to uncompensated loss caused by compromised personal information, does not predominate over the three categories of common damages inquiries analyzed by the plaintiffs’ expert. We do not think, therefore, that the District Court’s determination on this point was an abuse of discretion, so we do not disturb it here.

VACATED IN PART AND REMANDED.

21-13146 BRANCH, J., Concurring and Dissenting in Part 1

BRANCH, J., Specially Concurring in Part and Dissenting in Part:

I write separately to address two issues discussed in the Majority Opinion: standing and damages. First, while I agree with the Majority that Shenika Theus is the only named Plaintiff with standing, I disagree with the Majority’s concrete injury analysis. Second, I dissent from the Majority’s approval of Plaintiffs’ damages methodology. I address each of these issues in turn.

I. STANDING

Beginning with standing, the Majority and I agree on several points. First, I agree that two of the three named Plaintiffs do not have standing. *See Cordoba v. DIRECTV, LLC*, 942 F.3d 1259, 1264 (11th Cir. 2019) (explaining that only named plaintiffs need to demonstrate standing at the class certification stage). Specifically, I agree that Michael Franklin and Eric Steinmetz lack standing because they failed to establish that their alleged injuries were “fairly . . . trace[able] to the challenged action of the defendant.” *Lujan v. Defs. Of Wildlife*, 504 U.S. 555, 560 (1992) (quotation omitted). Second, with respect to Shenika Theus, the remaining named Plaintiff, I agree that Theus can establish standing—but I arrive at that conclusion for different reasons than the Majority articulates. Accordingly, my standing discussion proceeds in two parts. I first explain why I part ways with the Majority’s approach and then address why Theus nonetheless establishes a concrete injury.

2 BRANCH, J., Concurring and Dissenting in Part 21-13146

A.

To begin, I turn to my disagreement with the Majority’s concrete injury analysis, which rests on two erroneous conclusions about what Plaintiffs have alleged in their third amended consolidated class action complaint (“TAC”) (the operative complaint in this case). The Majority’s first conclusion rests on an allegation that is simply not contained in the TAC, and the Majority’s second conclusion rests on an allegation that, when viewed in light of all the TAC’s allegations, does not establish a concrete injury.

The Majority first concludes that Plaintiffs have alleged that the “hackers took [their] data and posted it on Joker Stash” (an online marketplace for stolen payment data).¹ Plaintiffs’ TAC, however, contains no such allegation. Instead, Plaintiffs’ allegations concern only the risk of “potential fraud and identity theft” based on “expos[ure]” of Plaintiffs’ data due to the data breach—*i.e.*, the risk of future harm. Accordingly, I respectfully disagree with the Majority’s conclusion that the named Plaintiffs have alleged that their credit card information was posted on the dark web.

¹ The Majority concludes that the posting of one’s credit card information on the dark web is sufficient to establish a concrete injury for all three named Plaintiffs. To be clear, my dissent does not address whether an allegation that hackers stole Plaintiffs’ data and posted it for sale on the dark web sufficiently establishes a concrete injury. I write separately because, even assuming such an allegation was sufficient for concreteness, Plaintiffs have simply not made that allegation in this case.

21-13146 BRANCH, J., Concurring and Dissenting in Part 3

As to its second conclusion, the Majority points to Plaintiffs’ TAC allegation that their personal information was “exposed for theft and sale on the dark web” as “critical” to establishing a concrete injury. Because Plaintiffs’ allegations about mere “exposure” to the theft and sale of their information simply point to an increased risk of identity theft and risk of future harm, however, I disagree that this concern establishes a concrete injury. I address the TAC,² the motion for class certification, and the class certification hearing in turn.³

Starting with the TAC, Plaintiffs’ allegations concern only the risk of future harm. Plaintiffs describe their injury as “imminent and certainly impending” (*i.e.*, futuristic) and fraud and identity theft as “potential” (*i.e.*, a mere risk). And allegations relating to the risk of future harm are insufficient to establish a concrete injury under Article III. *TransUnion LLC v. Ramirez*, 141 S. Ct. 2190, 2210–11 (2021) (explaining that mere risk of future harm without more does not give rise to Article III standing for recovery of damages); *Tsao v. Captiva MVP Rest. Partners, LLC*, 986 F.3d 1332, 1339 (11th Cir. 2021) (“[A] plaintiff alleging a threat of harm does not have Article III standing . . .”); *Muransky v. Godiva Chocolatier, Inc.*, 979 F.3d 917, 927–28 (11th Cir. 2020). Indeed, we have

² The Majority confines its concrete injury analysis to the TAC.

³ The district court and the parties on appeal rely on post-pleading litigation developments—like the motion for class certification and the class certification hearing—for their standing arguments.

4 BRANCH, J., Concurring and Dissenting in Part 21-13146

held that “[e]vidence of a mere data breach does not, standing alone, satisfy the requirements of Article III standing” and that allegations of an “increased risk” of identity theft based on a data breach are likewise insufficient. *Tsao*, 986 F.3d at 1344; *Muransky*, 979 F.3d at 933 (explaining that the allegation that the plaintiff “and members of the class continue to be exposed to an elevated risk of identity theft” is the “kind of conclusory allegation [that] is simply not enough” for an Article III injury). Thus, because the Majority rests its concrete injury analysis on an allegation that amounts to the mere risk of future harm, I cannot join the Majority’s concrete injury analysis.

The motion for class certification and the class certification hearing do not help Plaintiffs in establishing a concrete injury either. Plaintiffs’ motion for class certification largely echoes the TAC’s allegations, stating that “Plaintiffs . . . experienced the . . . harm of having their Customer Data exposed to fraudulent use” and that the “evidence will establish that [Brinker’s] conduct exposed [their customer data] to unauthorized third parties.” The motion makes no reference to Joker Stash—or any other site on the dark web—and states only once in passing that Plaintiffs’ customer data “ha[d] been exposed and found for sale on the dark web,” without any allegation of which of the Plaintiffs’ data was exposed or where such data was “found.” But, as I explain below, this passing statement does not pass muster in light of Plaintiffs’ admissions at the class certification hearing.

21-13146 BRANCH, J., Concurring and Dissenting in Part 5

During the hearing on class certification, Plaintiffs stated that they had “uncontroverted evidence that the data that was taken from Brinker’s system was posted for sale and sold on the dark web.” According to Plaintiffs, at least 4.5 million cards were affected by the data breach and, according to documents they obtained from Fiserv (Brinker’s processor), those 4.5 million cards—*i.e.*, one hundred percent of the cards used at Brinker’s locations during the affected time period—were posted on Joker Stash. Despite these assertions at the hearing, however, when the district court asked Plaintiffs’ counsel whether she knew if any of the three named Plaintiffs’ cards were actually on the dark web, Plaintiffs’ counsel responded: “[*W*]e *do not know* that at this point.” Accordingly, by counsel’s own admission, the record fails to support the conclusion that the named Plaintiffs’ credit card information was either posted or sold on the dark web as a result of the data breach. To the contrary, Plaintiffs admitted that they did not know if their credit card information was on the dark web.

In sum, considering Plaintiffs’ admission that they do not know whether their data was posted or sold on the dark web, I cannot join the Majority’s concrete injury analysis—which rests on conclusions that are simply unsupported by the record. *See Lujan*, 504 U.S. at 561 (explaining that the proof required for standing varies “with the manner and degree of evidence required at the successive stages of the litigation”); *Gen. Tel. Co. of Sw. v. Falcon*, 457 U.S. 147, 160 (1982) (explaining that “it may be necessary for the

6 BRANCH, J., Concurring and Dissenting in Part 21-13146

court to probe behind the pleadings” to assess standing at the class certification stage).

B.

Although I disagree with the Majority’s concrete injury analysis, I nonetheless agree that Theus has suffered a concrete injury (and therefore has standing) for a different reason: she has established financial harm. In her deposition, Theus explained that her transactions at Chili’s, which occurred during the restaurant’s at-risk time frame,⁴ caused her to incur unauthorized charges on her account that led to an overdraft fee and a bank-imposed card replacement fee. These unreimbursed, out-of-pocket expenses that Theus incurred are the type of “pocketbook injur[ies] [that are] . . . prototypical form[s] of injury in fact.” *Collins v. Yellen*, 141 S. Ct. 1761, 1779 (2021); *TransUnion*, 141 S. Ct. at 2204 (explaining that “traditional tangible harms, such as . . . monetary harms” are “obvious” harms that “readily qualify as concrete injuries under Article III”). Accordingly, I conclude—for different reasons than the Majority—that Theus has alleged a concrete harm sufficient for standing.

II. Damages Methodology

I now turn to the damages issue and conclude that the district court erred by accepting the damages methodology offered by

⁴ As the Majority points out, Theus does not suffer the same traceability problem that Franklin and Steinmetz do.

21-13146 BRANCH, J., Concurring and Dissenting in Part 7

Plaintiffs’ expert for two reasons. First, the methodology fails to tie a damages amount to an injury actually suffered by a plaintiff. And second, the district court improperly relied on *Tyson Foods, Inc. v. Bouaphakeo*, 577 U.S. 442, 459–61 (2016).

In support of their motion for class certification, Plaintiffs offered an expert declaration to explain their damages methodology. Plaintiffs’ expert set forth a “damages methodology applicable on a class-wide basis” by calculating four “damages elements”: (1) the value of any lost opportunity to accrue rewards points; (2) the value of stolen payment card data; (3) the value of cardholder time; and (4) out-of-pocket damages.

The district court rejected Brinker’s argument that the expert’s methodology was overinclusive and not accurately tailored to the facts. It explained that “[u]nder [the expert’s] damages methodology, 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 time addressing the breach), and out-of-pocket damages (whether or not they incurred any out-of-pocket damages).” The court continued: “[Plaintiffs’ expert] employs an averages method to compute damages, reasoning that the delta between class members’ damages is minimal[,] irrespective of the type of card used or time spent.” It explained that “[a]s with any averages calculation, over or under inclusivity is going to be a risk,” and noted that “the Supreme Court” in *Tyson Foods* “has approved the use of averages methods to calculate damages.” The district

8 BRANCH, J., Concurring and Dissenting in Part 21-13146

court concluded that “at this point [the expert’s] testimony [was] offered to show that a reliable damages calculation methodology exists, not to calculate class members’ damages.”

Applying Rule 23(a)’s predominance requirement, the district court determined that Plaintiffs’ damages expert offered a common method of calculating damages that, despite including “payment cards that may have been breached prior to the Data Breach,” “shows for class certification purposes that a common method of addressing causation and damages exists.” The court opined:

Most data breaches are very similar to one another, such that a jury may find that a relative average reduction in damages for every class member that has been subjected to other data breaches is appropriate. As discussed above, the Supreme Court has approved the use of averages methods to calculate damages, *see Tyson Foods*, 577 U.S. [at] 459–61, and the same rationale could apply here.

Nevertheless, the district court caveated that “if it becomes obvious at any time that the calculation of damages (including accounting for multiple data breaches) will be overly burdensome or individualized, the [c]ourt has the option to decertify the class.”

Brinker argues that the district court erred by concluding that Plaintiffs’ “proposed damages methodology permissibly eliminated individualized issues.” Brinker contends that because it is “entitled to scrutinize each individual claim at trial by referring to

21-13146 BRANCH, J., Concurring and Dissenting in Part 9

each individual class member’s individual circumstances,” Plaintiffs have not met Rule 23’s requirement that common issues predominate over individual ones. Plaintiffs argue that the “district court did not abuse its discretion in finding [that they] met this standard.”

To certify a class under Rule 23(b)(3), a district court must determine that “questions of law or fact common to class members predominate over any questions affecting only individual members.” Fed. R. Civ. P. 23(b)(3). This predominance determination includes questions relating to damages. *See Tyson Foods*, 577 U.S. at 453–54; *Agmen Inc. v. Conn. Ret. Plans & Tr. Funds*, 568 U.S. 455, 460 (2013). As the Majority points out, individual damages issues predominate “if computing them will be so complex, fact-specific, and difficult that the burden on the court system would be simply intolerable” or if “significant individualized questions go[] to liability.” *Brown v. Electrolux Home Prods., Inc.*, 817 F.3d 1225, 1240 (11th Cir. 2016) (quotations omitted). Accordingly, in our analysis of a damages methodology based on averages, the focus is on “whether the sample at issue could have been used to establish liability in an individual action.” *Tyson Foods*, 577 U.S. at 458.

At the class-certification stage, “a model purporting to serve as evidence of damages . . . must measure only those damages attributable to” plaintiffs’ theory of liability in the case. *Comcast Corp. v. Behrend*, 569 U.S. 27, 35 (2013). “And for purposes of Rule 23, courts must conduct a rigorous analysis to determine whether that is so.” *Id.* (quotation omitted). As such, a court must not only

10 BRANCH, J., Concurring and Dissenting in Part 21-13146

evaluate whether a damages calculation “provide[s] a method to measure and quantify damages on a classwide basis,” but also whether such a methodology constitutes “a just and reasonable inference” or whether it is “speculative.” *Id.* Without this evaluation, “any method of measurement [could be] acceptable [at the class-certification stage] so long as it can be applied classwide, no matter how arbitrary the measurements may be.” *Id.* at 35–36. And “[s]uch a proposition would reduce Rule 23(b)(3)’s predominance requirement to a nullity.” *Id.* at 36.

Here, the district court approved a damages methodology that awards to all class members 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*).” In short, this methodology impermissibly permits plaintiffs to receive an award based on damages that they did not suffer—*i.e.*, an award that a plaintiff could not establish in an individual action. *Tyson Foods*, 577 U.S. at 458.

The Majority defends the use of representative evidence by asserting that each “customer fitting within the class definitions experienced a similar injury,” but this assertion cannot be true. As the district court acknowledged, Plaintiffs’ damages methodology could allow a plaintiff to be compensated for opportunities to accrue rewards points, the value of their time spent addressing the breach, and out-of-pocket damages, even though the plaintiff

21-13146 BRANCH, J., Concurring and Dissenting in Part 11

suffered *none* of those harms. Each of these damages elements relate to separate and distinct injuries that may not be common to all class members, meaning that certain plaintiffs may impermissibly recover damages that they otherwise would not be entitled to in an individual action. *See Comcast Corp.*, 569 U.S. at 35.

The district court acknowledged that “[a]s with any averages calculation, over or under inclusivity is going to be a risk,” but cited *Tyson Foods* to say that “the Supreme Court has approved the use of averages methods to calculate damages.” But *Tyson Foods* is inapposite to the facts of this case.

In *Tyson Foods*, the Supreme Court approved the use of “representative evidence” to prove that the amount of time employees spent “donning and doffing” their gear at a chicken plant, when added to their regular work hours, “amounted to more than 40 hours in a given week” in order to be entitled to recovery under the Fair Labor Standards Act. *Tyson Foods*, 577 U.S. at 454. Far from categorically “approv[ing] the use of averages methods to calculate damages,” as the district court asserted, the Supreme Court was careful to reject any request to “establish general rules governing the use of statistical evidence, or so-called representative evidence, in all class-action cases.” *Id.* at 455. Instead, the Court explained that “[w]hether a representative sample may be used to establish classwide liability will depend on the purpose for which the sample is being introduced and on the underlying cause of action.” *Id.* at 460. The Court noted that plaintiffs in that case “sought to introduce a representative sample to fill an evidentiary gap created

12 BRANCH, J., Concurring and Dissenting in Part 21-13146

by the employer’s failure to keep adequate records.” *Id.* at 456. And the Court concluded that reliance on this representative evidence “did not deprive [the employer] of its ability to litigate individual defenses,” reasoning that “[s]ince there were no alternative means for the employees to establish their hours worked,” the employer was left to attack the representative evidence itself. *Id.* at 457. The defense was thus “itself common to the claims made by all class members.” *Id.*

The justifications for using representative evidence that were present in *Tyson Foods* are simply not present here. In this case, the questions relevant to the damages inquiry include whether a given class member possessed a rewards card, spent time addressing a data breach, and suffered out-of-pocket losses. Unlike *Tyson Foods*, the evidence for the answers to those questions is not inaccessible or controlled by Brinker. To the contrary, that evidence would be known and controlled by the plaintiffs or is at least readily available through individualized examination. And unlike *Tyson Foods*, here, the use of damages averages would deprive Brinker of its ability to litigate individual defenses where a class members’ individual damages are discoverable.

Considering that, under Plaintiffs’ averages methodology, a plaintiff could be compensated for a harm he did not suffer and that *Tyson Foods* does not justify the use of averages under the facts of this case, I am left to conclude that the district court erred by accepting Plaintiffs’ damages methodology when certifying Plaintiffs’

21-13146 BRANCH, J., Concurring and Dissenting in Part 13

proposed classes. Accordingly, I dissent from the Majority's conclusion to the contrary.

★ ★ ★

In sum, while I agree with the Majority's bottom line that Theus is the only named Plaintiff with standing, I disagree with the Majority's concrete injury analysis, and I conclude that Theus suffered an injury by establishing financial harm. Additionally, I dissent from the Majority's approval of Plaintiffs' damages methodology.