UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF FLORIDA
JACKSONVILLE DIVISION

SHENIKA THEUS, individually and on behalf of all others similarly situated,

Plaintiffs,

Case No. 3:18-cv-686-TJC-MCR

v.

BRINKER INTERNATIONAL, INC.,

Defendant.

ORDER

This data breach case is before the Court on the matter of class certification. Plaintiff Shenika Theus sues Defendant Brinker International, Inc.—owner of the chain restaurant Chili's—in connection with a spring 2018 incident in which a hacker allegedly stole customers' credit and debit card data and posted it for sale on Joker's Stash, a dark web marketplace. See Doc. 95 (Third Amended Complaint). The Court previously certified the following class for Theus's negligence claim:

> 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.

Doc. 167 at 16, 37.[1] The Court determined that this definition would ensure standing for all members and satisfy Federal Rule of Civil Procedure 23(b)(3)'s requirement that questions common to the class predominate over individualized questions because the definition would require class members to have experienced fraudulent charges or to have had their data posted on the dark web, and that they would have suffered some out-of-pocket expenses. Id. at 16.

Brinker appealed, and the United States Court of Appeals for the Eleventh Circuit held that the phrase "had their data accessed by cybercriminals" encompasses more than fraudulent charges and data posts on the dark web. See Green-Cooper v. Brinker Int'l, Inc., 73 F.4th 883, 892 (11th Cir. 2023). The Eleventh Circuit remanded for this Court to reconsider Rule 23(b)(3) predominance. Id. Specifically, the Eleventh Circuit instructed the Court to either (1) "refine the class definition[] to only include [people who have experienced fraudulent charges or had their data posted on the dark web]" or (2) reanalyze the original class definition "based on the understanding that the

[1]The Court also certified a California subclass. Doc. 167 at 37–38. On appeal, the Eleventh Circuit held that the California class representative lacked standing and directed the Court to determine the viability of the California subclass. Green-Cooper, 73 F.4th at 890-91, 893. The Court dismissed the California class representative's claims, Doc. 193 at 4, and Theus subsequently withdrew her request to certify a California subclass, Doc. 195 at 2–3.

class definition[] . . . may include uninjured individuals[.]" Id. The Eleventh Circuit also instructed the Court to analyze whether the class definition—original or as revised—"would require individualized proof of standing, especially as to time or effort expended to mitigate the consequences of the data breach." Id. at 892 n.13. Finally, the Eleventh Circuit held that posting data on the dark web is "misuse" of data and a concrete injury for standing purposes, and that Theus's proposed method of calculating damages—which is based on average losses from mitigation efforts—suffices at the class certification stage. Id. at 889-90, 893-94.

On remand, the Court directed supplemental briefing limited to the Rule 23(b)(3) predominance issue (Doc. 193 at 4) and held a hearing on April 17, 2025, the transcript of which is incorporated by reference. See Doc. 207. In her supplemental brief, Theus proposed revising the class definition to 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) and resultingly had their data posted on Joker's Stash.

Doc. 195 at 2, 7, 10. But at the hearing, Theus abandoned her proposed definition, stating that while she thought she was following the spirit of the Eleventh Circuit's mandate and trying to narrowly define the class, she realized in retrospect that her proposed definition was being viewed differently. She

instead agrees the Court is confined to the two options permitted by the Eleventh Circuit's mandate.[2] As discussed at the hearing, the Court refines the class definition as indicated by the Eleventh Circuit:[3]

> 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 March and April 2018 data breach who: (1) experienced fraudulent charges or had data posted on the dark web in connection with the data breach; and 2) incurred reasonable expenses or time spent in mitigation of the fraudulent charges or data posting.

Applying the Eleventh Circuit's ruling to this refined definition, Rule 23(b)(3) predominance is not satisfied.

---

[2]"When an appellate court issues a clear and precise mandate, the district court is obligated to follow the instruction. . . . A district court when acting under an appellate court's mandate, cannot vary it, or examine it for any other purpose than execution; or give any other or further relief; or review it, even for apparent error, upon a matter decided on appeal; or intermeddle with it, further than to settle so much as has been remanded." Winn-Dixie Stores, Inc. v. Dolgencorp, LLC, 881 F.3d 835, 843 (11th Cir. 2018) (quoted authority omitted). Here, the Eleventh Circuit mandated that this Court reanalyze Rule 23(b)(3) predominance for the originally certified class or for that class refined to include only individuals who had experienced fraudulent charges or had their data posted on the dark web. Green-Cooper, 73 F.4th at 892. As plaintiff belatedly recognized, proposing an entirely new definition and beginning the class certification analysis afresh was simply not an option.

[3]Because the Eleventh Circuit held that the language "data accessed by cybercriminals" will include uninjured plaintiffs, Green-Cooper, 73 F.4th at 892, and eliminating as many uninjured plaintiffs as possible from the outset is prudent, the Court declines to maintain or reanalyze the original, overbroad definition. In any case, that definition would raise the same predominance issues fatal to the refined definition, as discussed below.

"Common questions 'predominate' within the meaning of Rule 23(b)(3) when the substance and quantity of evidence necessary to prove the class claims won't vary significantly from one plaintiff to another." Tershakovec v. Ford Motor Co., 79 F.4th 1299, 1306 (11th Cir. 2023) (citation omitted). "The first step in assessing predominance is to identify the parties' claims and defenses and their elements and to categorize these issues as common questions or individual questions by predicting how the parties will prove them at trial." Id. (quoting Brown v. Electrolux Home Prods., Inc., 817 F.3d 1225, 1234 (11th Cir. 2016)). "A common issue is one that will likely be proved using the same evidence for all class members; an individualized issue, by contrast, is one that will likely be proved using evidence that 'varies from member to member'." Id. (quoting Brown, 817 F.3d at 1234). "If proving class member standing will require individualized proof, predominance is likely not satisfied." See Cordoba v. DIRECTV, LLC, 942 F.3d 1259, 1277 (11th Cir. 2019). Moreover, "predominance looks to whether 'significant questions concerning ultimate liability' remain after the resolution of any common issues." Carter v. City of Montgomery, 108 F.4th 1334, 1342 (11th Cir. 2024) (citing Vega v. T-Mobile USA, Inc., 564 F.3d 1256, 1274 (11th Cir. 2009)). The Eleventh Circuit has described the predominance test as follows:

> Where, after adjudication of the classwide issues, plaintiffs must still introduce a great deal of individualized proof or argue a number of individualized legal points to establish most or all of the

> elements of their individual claims, such claims are not suitable for class certification under Rule 23(b)(3). If common issues truly predominate over individualized issues in a lawsuit, then the addition or subtraction of any of the plaintiffs to or from the class should not have a substantial effect on the substance or quantity of evidence offered. Put simply, if the addition of more plaintiffs to a class requires the presentation of significant amounts of new evidence, that strongly suggests that individual issues (made relevant only through the inclusion of these new class members) are important. If, on the other hand, the addition of more plaintiffs leaves the quantum of evidence introduced by the plaintiffs as a whole relatively undisturbed, then common issues are likely to predominate.

Vega, 564 F.3d at 1270 (quoting Klay v. Humana, Inc., 382 F.3d 1241, 1255 (11th Cir. 2004), abrogated in part on other grounds by Bridge v. Phoenix Bond & Indem. Co., 553 U.S. 639 (2008)).

Common questions in this litigation are whether Brinker was negligent (including all factual questions related to Brinker's data use and protection practices and all legal questions related to the sufficiency of those practices) and the precise circumstances of the data breach (including when each Chili's location was affected within the breach period).

But individual questions abound. These include the details of each class member's Chili's transaction (including the date and location of the transaction and whether that location was affected on that date). Theus proposes using Brinker's transaction records to determine who ate at which locations during the period each location was affected. But even if this information is available, Theus has not produced evidence to show that every diner who used a credit or

debit card at affected restaurants during the relevant dates had their data taken. Even assuming they all did, other individualized questions predominate.

Another individual question is whether each member experienced fraudulent charges or had data posted on the dark web. Theus never submitted any evidence to demonstrate that any particular Chili's customer's credit or debit card was posted on the dark web.[4] Indeed, Theus's attorney did not know whether Theus' credit card information was posted on the dark web—the most she could say was that she believed Theus's card was in the tranche of cards offered for sale—but the evidentiary support for even that proposition is shaky. Theus's evidence amounts to one internet article (which Brinker rightly challenges on hearsay grounds) which describes an upcoming sales event on the Joker's Stash dark web credit card shop where 4.5 million credit card numbers "purportedly" taken in a breach of "nationwide chain restaurants" were to be offered for sale (the article does not mention Chili's or any other restaurant

[4] In her brief, Theus appears to interpret the Eleventh Circuit's decision to establish as fact that all compromised cards were posted on Joker's Stash, see Doc. 195 at 6–7, while Brinker argues that no evidence identifies cardholders whose data was posted or supports the assertion that any breached data was posted at all, see Doc. 199 at 15–16. The Court reads the Eleventh Circuit's decision to hold only that the posting of data on the dark web is a concrete injury for standing purposes, not that such posting happened for all cardholders in this case. But even if Theus's interpretation is correct, the outcome is the same. At the very least, the question of individual mitigation is substantial and predominates over common questions.

chain) (see Doc. 197); and a series of emails from Brinker's credit card servicer (FISERV (formerly FirstData)) who worked with Brinker after it learned of the data breach, in which FISERV staff discuss the breach, with one person making a "back of the envelope calculation" that Chili's processed 5.5 million transactions in the relevant time which would "probably" translate to 4.5 million unique cards being exposed, and reporting that they were "working on pulling the at risk cards" (see Doc. 155-2 at FISV-Brinker 0000989-990, 0001064-65). This is not enough. Even if the "at risk cards" were all available, Theus fails to demonstrate that she can offer class-wide proof of fraudulent charges or posting of data on the dark web. Thus, this too becomes an individualized question.[5]

[5] Along with its post-remand brief, Brinker submitted a declaration and report from J. Andrew Valentine, a digital forensics expert, who opines that it would be impossible to determine which credit cards were offered for sale on Joker's Stash (which is now defunct) or to identify any customers whose credit card information was ultimately purchased by fraudsters from that site. He further explains that only purchasers would see any actual credit card data—the sales offer did not include the data itself, only generic descriptions of individual available cards, such as Visa Gold Credit card, price $5; Mastercard Standard Debit card, price $5. See Doc. 201-1. While the Court is not relying on this evidence, Theus did not move to strike it or ask to reply. At the hearing, her counsel explained that she did not believe this was a contested area in the litigation. But Brinker's response to plaintiff's initial motion for class certification raised questions as to plaintiff's ability to put forward a proposed class that was readily ascertainable, given plaintiff's failure to offer evidence that records existed. See Doc. 141 at 15-18. And, regardless, it remains plaintiff's burden to demonstrate—with evidence—that the class should be certified. See Brown, 817 F.3d at 1234 ("The party seeking class certification

A further individualized question relates to the expenses and time each class member spent in mitigation. While agreeing that Theus's damages expert had a satisfactory plan for offering class-wide analysis of the types and amounts of damages, the Eleventh Circuit was not satisfied that the Court's inclusion of mitigation in the class definition was enough to show whether individualized proof would be needed "as to time or effort expended to mitigate the consequences of the data breach" sufficient to demonstrate standing. Green-Cooper, 73 F.4th at 893 n.13. As to this, Theus has offered no suggestion at all. To the contrary, in both her brief and at the post-remand hearing, Theus encouraged the Court to put off any consideration of mitigation until after the class is certified. This would directly contravene the Eleventh Circuit's direction to the Court.

Under the refined class definition, the common questions do not predominate over the individual questions. Resolving the individual questions would require "a great deal of individualized proof." See Vega, 564 F.3d at 1270 (citing Klay, 382 F.3d at 1255). The proposed class encompasses up to approximately 4.5 million individuals. The addition of those individuals "requires the presentation of significant amounts of new evidence," see id., to establish the time-and-place details of each individual's transaction, the

---

has a burden of proof, not a burden of pleading.") (emphasis in original).

presence of fraudulent charges or dark web exposure, and individual mitigation efforts. The legitimacy of each individual's membership in the class—and Brinker's ultimate liability, if the negligence is established—turns on this evidence. Without proving the described details, each member could not establish standing or liability. Rule 23(b)(3) predominance is thus unsatisfied, and class certification is unavailable.

Accordingly, it is hereby

ORDERED:

1. Class certification is **DENIED**.

2. No later than **July 25, 2025,** plaintiff Shenika Theus shall file a notice stating whether she is prepared to go forward with the case on an individual basis. If she is, the Court will issue an amended case management and scheduling order; if not, the Court will enter an order of dismissal.

DONE AND ORDERED in Jacksonville, Florida, the 27th day of June, 2025.

Timothy J. Corrigan

TIMOTHY J. CORRIGAN
Senior United States District Judge

s/vng

Copies:

Counsel of record