**UNITED STATES DISTRICT COURT**
**MIDDLE DISTRICT OF FLORIDA**
**JACKSONVILLE DIVISION**

In re Brinker Data Incident Litigation

Case No. 3:18-cv-686-J-32MCR

---

**ORDER**

This case requires the Court to determine what constitutes an injury in fact for Article III standing for individuals whose information was stolen in a data breach. Eight named plaintiffs bring this class action on behalf of themselves and all similarly situated customers whose payment card and other personal information were stolen by criminal hackers from Defendant Brinker International, Inc.—the company that owns, operates, and franchises Chili's Grill and Bar.

## I. BACKGROUND

### A. Facts

According to the Second Amended Consolidated Complaint ("the complaint"), beginning in March 2018, hackers accessed Brinker's data network and installed malware on point-of-sale ("POS") systems [1] at many Chili's

---

[1] According to the complaint:

A POS system is an on-site device, much like an electronic cash register,

restaurants, which Brinker owns, develops, operates, and franchises. (complaint, Doc. 39 ¶¶ 25, 101). Brinker publicly announced the breach on May 12, 2018, stating:

> On May 11th, 2018, we learned that payment card information of some of our Guests who visited certain Chili's® Grill & Bar corporate-owned restaurants have been compromised in a data incident. Currently, we believe the data incident was limited to between March – April 2018; however, we continue to assess the scope of the incident.
>
> Upon learning of this incident, we immediately activated our response plan. We are working with third-party forensic experts to conduct a thorough investigation to determine the details of what happened. Law enforcement has been notified of this incident and we will continue to fully cooperate.
>
> While the investigation is still ongoing, we believe that malware was used to gather payment card information, including credit or debit card numbers and cardholder names, from our payment-related systems for in-restaurant purchases at certain Chili's restaurants.
>
> We deeply value our relationships with our Guests and our priority remains doing what is right for them. We are committed to sharing additional information on this ongoing investigation. More details can be found at: http://brinker.mediaroom.com/ChilisDataIncident.

(Id. ¶ 102).

---

> which manages transactions from consumer purchases, both by cash and card. When a payment card is used at a POS terminal, "data contained in the card's magnetic stripe is read and then passed through a variety of systems and networks before reaching the retailer's payment processor." The payment processor then passes the payment information on to the financial institution that issued the card and takes the other steps needed to complete the transaction.

(Doc. 39 ¶ 75) (citations omitted).

Brinker acknowledges that it relies on information systems, and "Chili's has long touted its technological innovation . . . ." (Id. ¶¶ 60, 62). Chili's daily payment card transactions are in the "tens of thousands . . . ." (Id. ¶ 72). When Brinker processes payment card transactions, it collects "the cardholder name, the account number, expiration date, card verification value ("CVV"), and PIN data for debit cards. Brinker stores th[is] Customer Data in its POS system and transmits this information to a third party for processing and completion of the payment." (Id. ¶ 64).

The amount of data breaches involving the theft of retail payment card information has been rising over the past several years, and "[m]ost of the massive data breaches occurring within the last several years involved malware placed on POS systems used by merchants." (Id. ¶¶ 74–75). These breaches include other national restaurant chains, such as P.F. Chang's, Arby's, Chipotle, and Wendy's. (Id. ¶ 103). "Given the numerous reports indicating the susceptibility of POS systems and consequences of a breach, Brinker was well-aware, or should have been aware, of the need to safeguard its POS systems." (Id. ¶ 80). Plaintiffs allege that despite this knowledge, Brinker failed to comply with industry standards for information security, including the Payment Card Industry Data Security Standard ("PCI DSS"). (Id. ¶¶ 81–90). And, "Brinker failed to implement adequate data security measures to protect its POS networks from the potential danger of a data breach and failed to implement

and maintain reasonable security procedures and practices . . . ." (Id. ¶ 106). Specifically, "Brinker operated POS systems with outdated operating systems and software; failed to enable point-to-point and end-to-end encryption; and, failed to take other measures necessary to protect its data network." (Id. ¶ 98).

During the data breach, each of the named plaintiffs paid for food and services at a Chili's restaurant with their credit or debit card. Marlene Green-Cooper dined at a Chili's in Florida in April 2018, and "[w]ithin days thereafter" noticed three unauthorized charges on the credit card she had used at Chili's. (Id. ¶¶ 28(1)–29(1)). Green-Cooper was issued a new credit card and during the time she waited for a new card she lost the ability to accrue cash back rewards. (Id. ¶¶ 28(1)–28(2)).[2] Green-Cooper continues to monitor her account daily for unauthorized charges. (Id. ¶ 29(1)).

In April 2018, Shenika Thomas used her debit card at a Chili's in Texas. (Id. ¶ 29(2)). In early May 2018, Thomas incurred three fraudulent charges totaling more than $100 on her debit card. (Id. ¶ 30). Thomas was issued a new debit card, and she, too, continues to monitor her account to prevent further misuse. (Id.).

Fred Sanders used his credit card at a Chili's in Virginia in mid-April 2018, and roughly one month later he discovered fraudulent charges totaling

[2] Plaintiffs have two paragraphs numbered "28" and two numbered "29." This Order denotes them as 28(1) and 28(2).

$3,300. (Id. ¶ 32). Sanders spent time disputing the charges with his bank, lost the opportunity to accrue cash back rewards while awaiting a replacement card, and placed fraud alerts with all three credit reporting agencies. (Id. ¶¶ 32–33).

Between March and April 2018, Daniel Summers, Christopher Lang, Peter Alamillo, and Michael Franklin all used credit or debit cards at various Chili's locations in California. (Id. ¶¶ 34–44). One month after using his debit card at Chili's, Summers incurred a fraudulent charge of $1,093.91, spent time disputing the charge with his bank, and was notified by Brinker that his personally identifiable information ("PII") might have been compromised. (Id. ¶¶ 34–36). After Lang used his debit card at Chili's, Chili's notified him that his PII was at risk because of the data breach. (Id. ¶¶ 37–38). Alamillo used his debit card at Chili's, which subsequently sent him a notice of the data breach, and he has spent time monitoring his accounts for fraudulent activity. (Id. ¶¶ 39–41). After using a payment card three times in two months at Chili's, Franklin experienced fraudulent charges on his account, spent time speaking with his bank, and lost the chance to accrue rewards points while awaiting a replacement card. (Id. ¶¶ 44–46).

In April 2018, Eric Steinmetz used his debit card at a Chili's in Nevada. After learning of the breach, Steinmetz "procured his consumer disclosures from all three credit reporting agencies," "incurred transportation costs of gasoline in driving to Wells Fargo to cancel his debit card and obtain a temporary card[,]"

and "lost time dealing with issues related to the [data breach] . . . ." (Id. ¶¶ 47–49).

Plaintiffs allege that they would not have dined at Chili's had they known "it lacked adequate computer systems and data security practices to safeguard" customers' information. (Id. ¶ 50). Plaintiffs further allege that the value of their customer data has diminished, they lost time, have been inconvenienced, and "have concerns for the loss of their privacy." (Id. ¶¶ 53–54). Additionally, Plaintiffs face a "substantially increased risk of fraud, identity theft, and misuse resulting from" the data breach. (Id. ¶ 55).

**B. Procedural Posture**

On October 30, 2018, the Court consolidated several related cases with this one, and directed Plaintiffs to file an amended consolidated complaint. (Doc. 31). Plaintiffs filed the operative Second Amended Consolidated Class Action Complaint, (Doc. 39), which alleges fourteen causes of action.[3] The eight named plaintiffs seek certification of a Nationwide Class, which is defined as: "All persons residing in the United States who made a credit or debit card purchase at any affected Chili's location during the period of the Data Breach. . . ." (Doc. 39 ¶ 129). In the alternative, Plaintiffs propose separate Statewide classes, which are defined as: "All persons residing in [California,

[3] Plaintiffs mistakenly have two Counts numbered "XII." This order refers to the second Count XII as XII(b).

Florida, Virginia, Nevada, or Texas] who made a credit or debit card purchase at any affected Chili's location during the period of the Data Breach (the 'Statewide Classes')." (Doc. 39 ¶ 130).

The complaint charges six common law claims on behalf of the Nationwide Class, or in the alternative on behalf of each Statewide Class: breach of implied contract (Count I); negligence (Count II); negligence per se (Count III); unjust enrichment (Count IV); declaratory judgment (Count V); and breach of confidence (Count XIII). In addition to the common law causes of action, each Statewide Class alleges state statutory violations: Florida Deceptive and Unfair Trade Practices Act ("FDUTPA") (Count VI); Texas Deceptive Trade Practices-Consumer Protection Act ("Texas DTPA") (Count VII); Virginia Customer Data Breach Notification Act ("Virginia Notification Act") (Count VIII); Virginia Consumer Protection Act ("VCPA") (Count IX); California's Unfair Competition Law ("UCL") – Unlawful Business Practices (Count X); California's UCL – Unfair Business Practices (Count XI); California's UCL – Fraudulent/Deceptive Business Practices (Count XII); and Nevada's Consumer Fraud Act ("CFA") (Count XII (b)).

Currently pending before the Court is Defendant's Motion to Dismiss, (Doc. 48). Plaintiffs responded, (Doc. 53), Brinker replied, (Doc. 54), and Plaintiffs filed a sur-reply, (Doc. 57). On June 25, 2019, the Court held a hearing on the motion, the record of which is incorporated herein. (Doc. 63) Brinker has

moved to dismiss every count under Rule 12(b)(6) for failure to state a claim, and has moved to dismiss the case under Rule 12(b)(1), arguing that the named plaintiffs lack standing. (Doc. 48).

## II. STANDING

To satisfy the "'irreducible constitutional minimum' of standing," the "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." Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1547 (2016) (quoting Lujan v. Defs. of Wildlife, 504 U.S. 555, 560 (1992)). "To establish injury in fact, a plaintiff must show that he or she suffered 'an invasion of a legally protected interest' that is 'concrete and particularized' and 'actual or imminent, not conjectural or hypothetical.'" Id. at 1548 (quoting Lujan, 504 U.S. at 560). "[T]hreatened injury must be certainly impending to constitute injury in fact and . . . allegations of possible future injury are not sufficient." Clapper v. Amnesty Int'l USA, 568 U.S. 398, 409 (2013) (alterations adopted) (quotation marks omitted) (quoting Whitmore v. Arkansas, 495 U.S. 149, 158 (1990)). Only the injury in fact requirement is at issue here, and more specifically, whether Plaintiffs have alleged a concrete injury. The Court divides this analysis into two sections, actual injuries that have already occurred and future injuries.

**A. Actual Injury**

A concrete injury is one that is real and not abstract. Spokeo, 136 S. Ct. at 1548. Concrete injuries are not limited to tangible harms; "'intangible' injuries . . . may satisfy Article III's concreteness requirement." Muransky v. Godiva Chocolatier, Inc., 922 F.3d 1175, 1185 (11th Cir. 2019).[4] The injury need not be substantial; "a small injury, an identifiable trifle, is sufficient to confer standing." Id. (quotation marks omitted) (quoting Common Cause/Georgia v. Billups, 554 F.3d 1340, 1351 (11th Cir. 2009)). The injury in fact requirement "serves to distinguish a person with a direct stake in the outcome of a litigation—even though small—from a person with a mere interest in the problem. [The Supreme Court has] allowed important interests to be vindicated by plaintiffs with no more at stake in the outcome of an action than a fraction of a vote. . . ." United States v. Students Challenging Regulatory Agency Procedures (SCRAP), 412 U.S. 669, 690 (1973).

An individual is not required to suffer monetary harm to have a concrete injury for Article III standing. SCRAP, 412 U.S. at 686 ("[S]tanding [i]s not confined to those who c[an] show 'economic harm.'"); cf., e.g., Doe v. Chao, 540 U.S. 614, 624–25 (2004) (finding that individuals who were adversely affected but suffered no monetary harm "ha[ve] injury enough to open the courthouse

[4] A petition for rehearing en banc is currently pending before the Eleventh Circuit in Muransky.

door, but without more ha[ve] no cause of action for damages . . . ."). In Chao, the Supreme Court addressed whether a plaintiff who suffered an "adverse affect" from a violation of the Privacy Act of 1974 needed to sustain actual damages to recover the $1,000 statutory minimum. Id. at 618–20. The Court found that the plaintiff had standing based on his allegations "that he was 'torn . . . all to pieces' and 'greatly concerned and worried' because of the disclosure of his Social Security number and its potentially 'devastating' consequences." Id. at 641 (Ginsburg, J., dissenting). However, the Supreme Court held that the plaintiff could not recover the $1,000 statutory minimum because he did not sustain an out of pocket expense. Id. at 627. Thus, although the cause of action required a plaintiff to have incurred monetary damages to prevail, monetary damages were not necessary to "open the courthouse door." Id. at 624–25.

Here, Plaintiffs Green-Cooper, Thomas, Sanders, Summers, and Franklin had unauthorized charges on their cards. (Doc. 39 ¶¶ 29, 30, 32, 5, 44–45). As a result of needing to replace their compromised cards, Green-Cooper, Sanders, and Franklin lost the ability to accrue cash back or point rewards. (Doc. 39 ¶¶ 28, 33, 46). Except for Lang and Alamillo, all Plaintiffs spent time disputing fraudulent charges, cancelling their credit or debit cards, monitoring their accounts for additional fraudulent activity, or placing fraud alerts on their credit files. (Doc. 39 ¶¶ 29, 30, 32, 33, 35, 45, 49). As alleged, these are

personalized, concrete injuries that are neither "conjectural [n]or hypothetical." Lujan, 504 U.S. at 560.

Defendants rely heavily on Torres v. Wendy's Company (Torres I), 195 F. Supp. 3d 1278, 1282–83 (M.D. Fla. 2016) for the proposition that monetary harm is required for Article III standing. (Doc. 48 at 7–9). This reliance is misplaced. In Torres I, the plaintiff alleged that he had two fraudulent debit card charges because of a data breach against Wendy's. Id. at 2180, 1283. The district court found no standing, relying on Resnick v. Avmed, Inc., 693 F.3d 1317 (11th Cir. 2012) and several district court cases from other districts. Torres I, 195 F. Supp. 3d at 1282–83. In Resnick, the Eleventh Circuit held: "Plaintiffs allege that they have become victims of identity theft and have suffered monetary damages as a result. This constitutes an injury in fact under the law." Resnick, 693 F.3d at 1323. Torres I interpreted this holding to require monetary harm. 195 F. Supp. 3d at 1283. However, Resnick held that identity theft plus monetary harm is sufficient for an injury in fact; it did not say that both are necessary. The Eleventh Circuit, like the Supreme Court, has frequently found an injury in fact despite an absence of monetary harm. E.g., Muransky, 922 F.3d at 1192 (determining that "[t]he effort . . . put into doing away with [an untruncated] receipt would suffice for standing."); Pedro v. Equifax, Inc., 868 F.3d 1275, 1280 (11th Cir. 2017) (finding that lost time attempting to resolve credit issues is a concrete injury); Billups, 554 F.3d at

1351 (having to produce a photo ID to vote is a concrete injury); Fla. State Conference of NAACP v. Browning, 522 F.3d 1153, 1166 (11th Cir. 2008) (finding that the injury of devoting resources from an organization's other activities is sufficient for standing).

After the district court in Torres I dismissed the complaint for lack of standing, the plaintiff filed an amended complaint, alleging that his stolen identity caused him to incur a $3 late charge on his utility bill. Torres v. Wendy's Int'l, LLC (Torres II), No. 6:16-cv-210-Orl-40DCI, 2017 WL 8780453, at *1 (M.D. Fla. Mar. 21, 2017). Additionally, other named plaintiffs were added, and they alleged that they lost the opportunity to accrue cash back and rewards points as a result of the breach, id. at *2, as plaintiffs here have alleged. The Torres II court found both—the $3 charge and lost rewards points—as independently sufficient injuries that meet the standing requirement. Id.

Further, the Eleventh Circuit has discounted Defendant's argument that Plaintiffs must allege their fraudulent charges were unreimbursed. Resnick, 693 F.3d at 1324 ("AvMed contends that Plaintiffs' injuries are not cognizable under Florida law because the Complaint alleges only 'losses,' not 'unreimbursed losses.' This is a specious argument."). At this stage of the proceeding, the Court can infer that the charges were not reimbursed, and thus the injury—the fraudulent charges—can be redressed by a favorable decision by this Court. See In re U.S. Office of Pers. Mgmt. Data Sec. Breach Litig., 928

F.3d 42, 65 (D.C. Cir. 2019) (finding in a data breach case that the district court erred in requiring allegations that fraudulent costs went unreimbursed, stating: "At this stage of the litigation, all facts and reasonable inferences must be drawn in favor of [Plaintiffs], and the complaint provides no basis for disregarding the claimed financial losses based on OPM's speculation that [Plaintiffs] were indemnified."); cf. In re SuperValu, Inc., 870 F.3d 763, 773 (8th Cir. 2017) (stating that the failure to allege that fraudulent charges were unreimbursed did not impact Article III standing, but "could be fatal to the complaint under the 'higher hurdles' of Rules 8(a) and 12(b)(6).").

Defendants also argue that the lost opportunity to accrue cash back or point rewards on payment cards while the cards were being replaced is not a concrete injury. (Doc. 48 at 19 (citing Tsao v. Captiva MVP Restaurant Partners, LLC, No. 8:18-cv-1606-T-02SPF, 2018 WL 5717479, at *2 (M.D. Fla. Nov. 1, 2018))).[5] Courts within this district are divided on whether the loss of the ability to accrue credit card rewards constitutes an injury in fact. Compare Torres II, 2017 WL 8780453, at *2 ("Plaintiffs have alleged they have suffered actual injuries, including the loss of credit card reward points and loss of cash-back rewards. These allegations are sufficient at this stage to plead standing."),

[5] The plaintiffs in Tsao filed an appeal. Currently, a motion to stay the appeal until after mediation is pending before the Eleventh Circuit.

with Tsao, 2018 WL 5717479, at *2 (finding the loss of cash back rewards as a speculative injury insufficient for standing). In Tsao, the court held

> As to damages, [the plaintiff] points to his lost time in alerting his bank of the potential compromise to two credit reward cards, the loss of his cash back reward accrual from the time he cancelled his cards to the time they were reissued, and the inconvenience, hassle, and nuisance of monitoring the situation caused by the data breach. These allegations amount to speculation of future, potential injury at best. De minimus non curat lex.[6]

Id. This Court aligns itself with Torres II on the "loss of rewards" issue. Also, Tsao is otherwise distinguishable. In Tsao, the plaintiffs did not allege that their information was stolen, only that it had been "exposed." 2018 WL 5717479, at *1. And, Tsao found that the plaintiff had failed to allege an injury because "[n]ot once d[id] he allege that his credit cards were used in any way by a thief or that his identity was stolen." Id. at *2. But here, several plaintiffs alleged they had fraudulent charges on their payment cards because of the breach. (Doc. 39 ¶¶ 29, 30, 32, 35, 44). This Court finds that all named plaintiffs (except for Lang and Alamillo), have sufficiently alleged a concrete actual injury and therefore have standing.

[6] The district court's statement "[d]e minimus non curat lex"—which means the law does not concern itself with trifles, BLACK'S LAW DICTIONARY (10th ed. 2014)—does not necessarily coincide with the Supreme Court's statement, and the Eleventh Circuit's reiteration, that even "an identifiable trifle" is a sufficient injury in fact to confer standing. Billups, 554 F.3d at 1351 (quotation marks omitted) (quoting SCRAP, 412 U.S. at 689 n.14).

**B. Future Injury**

Two named plaintiffs, Lang and Alamillo, failed to allege actual injuries and attempt to allege only future injuries. The extent of Lang's allegations are this: "Lang dined at a Chili's location in San Jose, California on April 1, 2018, paying for his purchases with a debit card. . . . On May 21, 2018, Chili's notified Mr. Lang that his PII was at risk as a result of the Data Breach." (Doc. 39 ¶ 37–38). Alamillo alleges that he received an email from Chili's informing him of the breach, he "has spent time and will continue to spend time monitoring his financial accounts for fraudulent activity[,]" and that the twelve months of free credit monitoring required him to provide his payment card information and to take affirmative steps to cancel the service after the twelve months to avoid being charged. (Doc. 39 ¶¶ 40–42). Whether these minimal allegations are sufficient to confer standing presents a closer call.

An increased risk of future harm is, in some circumstances, sufficient for standing. See Clapper, 568 U.S. at 414 n.5. To constitute a concrete injury, the risk of future harm must be certainly impending—not merely possible—and cannot be too speculative. Id. at 409–10; see also City of Miami Gardens v. Wells Fargo & Co., No. 18-13152, 2019 WL 3423228, at *6 (11th Cir. July 30, 2019) (finding that "[t]he delinquency of a single loan did not establish a certainly impending risk that the City [would] lose property-tax revenues or be forced to increase municipal spending to remediate blight."). In Clapper, the plaintiffs

alleged that a government surveillance program was unconstitutional. 568 U.S. at 407. The plaintiffs alleged that their jobs required privileged communications with people who might be subject to surveillance and that such surveillance would compromise the plaintiffs' ability to do their jobs. Id. at 405–07. However, the Supreme Court found that the plaintiffs' "objectively reasonable likelihood that their communications with foreign contacts [would] be intercepted . . . at some point in the future" was too speculative. Id. at 410. Although the Supreme Court acknowledged that a harm need not be "literally certain" to occur, and that standing can be sufficient "based on a 'substantial risk' that the harm will occur," the plaintiffs lacked any knowledge about the government's targeting practices and their allegations rested on a speculative chain of events that was not "certainly impending." Id. 410, 414 n.5.

In the data breach context, this Court looks with favor on Judge Scriven's analysis in In re 21st Century Oncology Customer Data Sec. Breach Litig., No. 8:16-MD-2737-MSS-AEP, 2019 WL 2151095, at *6 (M.D. Fla. Mar. 11, 2019) (compiling cases and determining that the "circuit split" on future harm standing in data breach cases is based on differing facts and not a disagreement of the law). In 21st Century Oncology, Judge Scriven parsed out three factors commonly relied upon in circuit court opinions determining whether a plaintiff has an injury in fact from the threat of future identity theft. Id. The first factor is the motive of the third-party who received the sensitive information. Id. In

cases where the plaintiffs alleged a criminal motive by hackers, the court was more likely to find a concrete injury. Id. The second factor is the type of information. Id. at *7. Where the compromised information contains PII—social security numbers, driver's license numbers, birthdates, etc.—the threat of future identity theft is much greater. Id. Third, is there evidence that a third-party has already accessed or fraudulently used the compromised information. Id. at *8. Allegations that the information has already been misused support a finding of an injury in fact. Id.

Lang's and Alamillo's allegations are insufficient to demonstrate a future risk of harm beyond a speculative level. See id.; (Doc. 39 ¶ 37–38). Neither Lang nor Alamillo allege a "substantial risk" or "heightened risk" of future harm. See Clapper, 568 U.S. at 414 n.5; Muransky, 922 F.3d at 1188. Looking at the three factors developed in 21st Century Oncology, they fail to allege an injury in fact. Although the first factor—the motive of the hackers—supports Lang and Alamillo, the other two factors—the type of information stolen and whether it has been misused—do not. See 21st Century Oncology, 2019 WL 2151095, at *6–8. Lang and Alamillo do not allege that their information was actually compromised—only that it is at risk. Although Lang alleges that his "PII" was involved, which could include social security numbers, driver's license numbers, and the like, according to his own complaint this is not the type of information that Brinker collected. (Doc. 39 ¶ 64 (stating that Brinker collects the

cardholder name, card number, expiration date, and CVV or PIN)). Lastly, Lang and Alamillo's information, if even compromised, has not been misused. See 21st Century Oncology, 2019 WL 2151095, at *6–8. Thus, the three factors do not support finding an injury in fact for standing based on future harm. See id.

Additionally, Alamillo's allegation that "he has spent time and will continue to spend time monitoring his accounts for fraudulent activity" does not constitute an injury in fact for standing. See Clapper, 568 U.S. at 40–10; (Doc. 39 ¶ 41). Monitoring one's accounts for fraudulent activity is something many individuals do, regardless of whether they have been informed their information is at risk. And because the information collected is less likely to lead to identity theft than other types of information and it has not actually been misused, the threat of future injury, although possible, is not "certainly impending." See Clapper, 568 U.S. at 40–10; (Doc. 39 ¶ 41). Lang and Alamillo's minimal allegations assert only speculative future harm that does not rise to an Article III injury in fact. See Clapper, 568 U.S. at 410–414; City of Miami Gardens, 2019 WL 3423228, at *6. Because the other named plaintiffs have sufficiently alleged actual injuries, the Court declines to address whether they have also alleged a sufficient future injury.

## III. SUFFICIENCY OF THE COMPLAINT

Defendants move to dismiss every count in the complaint as failing to state a claim upon which relief can be granted. (Doc. 48). The parties primarily

rely on Florida law in discussing the common law claims, but then sporadically use other data breach cases that apply different states' laws. The parties fail to explain why Florida law (or any other state's law) should apply. The Court cannot determine whether the complaint states claims upon which relief can be granted if it does not know what law to apply to each count. Thus, the parties need to brief choice of law before the Court rules on the Rule 12(b)(6) portion of the motion to dismiss.

## IV. CONCLUSION

Accordingly, it is hereby

**ORDERED:**

1. Defendant Brinker International, Inc.'s Motion to Dismiss is **DENIED in part, GRANTED in part, and DEFERRED in part**.

    a. Defendant's Rule 12(b)(1) Motion to Dismiss (Doc. 48) is **GRANTED** as to Plaintiffs Christopher Lang and Peter Alamillo. Plaintiff Christopher Lang's and Peter Alamillo's claims are **DISMISSED without prejudice** for lack of standing.[7]

    b. The remainder of Defendant's Rule 12(b)(1) Motion to Dismiss is

[7] The Court would consider permitting a Third Amended Consolidated Complaint to allow Lang and Alamillo, if they have a good faith basis to do so, to allege additional facts in support of standing. However, any amendment would take place after the Court rules on the 12(b)(6) portion of the motion to dismiss, to avoid unnecessary repleading.

**DENIED**.

c. The Court **DEFERS** ruling on the Rule 12(b)(6) portion of the Motion to Dismiss.

2. Not later than **August 16, 2019**, the parties shall file a joint notice informing the Court whether they prefer to brief the choice of law issue now and have the Court rule on the Rule 12(b)(6) portion of the Motion to Dismiss, or if they prefer the Court defer ruling until the choice of law issue is fully briefed as part of the class certification motion. If the parties choose to brief choice of law now, they should propose a briefing schedule.

3. After determining how the Court will proceed on the 12(b)(6) portion of the Motion to Dismiss, the Court will enter a Case Management and Scheduling Order.

**DONE AND ORDERED** in Jacksonville, Florida this 1st day of August, 2019.

TIMOTHY J. CORRIGAN
United States District Judge

jb
Copies:

Counsel of record