

**IN THE UNITED STATES DISTRICT COURT  
FOR THE WESTERN DISTRICT OF NORTH CAROLINA  
CHARLOTTE DIVISION  
CIVIL ACTION NO. 3:25-CV-00065-KDB-DCK**

**ALEXIS DOUGHERTY, ET AL.,**

**Plaintiffs,**

**v.**

**BOJANGLES' RESTAURANTS,  
INC.,**

**Defendant.**

**MEMORANDUM AND ORDER**

Plaintiffs are former employees of Defendant Bojangles' Restaurants, Inc. ("Bojangles"). In this action, they seek to recover monetary damages and injunctive relief for themselves and a class of current and former employees whose personal information was allegedly exposed during a "data breach" of Bojangles' computer systems during February and March 2024. Now before the Court is Defendant's Motion to Dismiss, (Doc. No. 24), which argues that Plaintiffs lack standing to assert their claims. Having carefully reviewed the Complaint, the parties' arguments and the relevant authorities, the Court finds that Plaintiffs have not sufficiently pled an actual or imminent misuse of their personal data traceable to the Bojangles data breach, as is required to establish standing to pursue their claims. Therefore, Defendant's Motion will be granted and this action dismissed.

**I. LEGAL STANDARD**

A motion to dismiss based on Federal Rule of Civil Procedure 12(b)(1) addresses whether the court has subject-matter jurisdiction to hear the dispute, *see* Fed. R. Civ. P. 12(b)(1), and Plaintiff bears the burden of proving that subject matter jurisdiction exists. *Evans v. B. F. Perkins*

*Co.*, 166 F.3d 642, 647 (4th Cir. 1999). “[F]ederal courts are courts of limited jurisdiction, constrained to exercise only the authority conferred by Article III of the Constitution and affirmatively granted by federal statute.” *In re Bulldog Trucking, Inc.*, 147 F.3d 347, 352 (4th Cir. 1998) (quotation omitted); *see Gunn v. Minton*, 568 U.S. 251, 256 (2013); *Kokkonen v. Guardian Life Ins. Co. of Am.*, 511 U.S. 375, 377 (1994). There is no presumption that a federal court has subject-matter jurisdiction. *See Pinkley, Inc. v. City of Frederick*, 191 F.3d 394, 399 (4th Cir. 1999). However, “when a defendant asserts that the complaint fails to allege sufficient facts to support subject matter jurisdiction, the trial court must apply a standard patterned on Rule 12(b)(6) and assume the truthfulness of the facts alleged.” *Kerns v. United States*, 585 F.3d 187, 193 (4th Cir. 2009). To determine whether subject matter jurisdiction is proper, the Court may consider evidence beyond the pleadings. *Evans*, 166 F.3d at 647.

A court cannot exercise subject-matter jurisdiction “over an individual who does not have standing.” *Whipple v. Marcuse*, No. 3:24-CV-00325, 2024 WL 3761276, at \*1 (W.D.N.C. Aug. 12, 2024) (quoting *AtlantiGas Corp. v. Columbia Gas Transmission Corp.*, 210 F. App’x 244, 247 (4th Cir. 2006)). Federal courts are limited by Article III of the United States Constitution to deciding actual “cases” or “controversies.” U.S. Const. art. III § 2. If a plaintiff lacks standing, then there is no case or controversy, and the court lacks subject-matter jurisdiction over his claims. *Spokeo, Inc. v. Robins*, 578 U.S. 330, 338 (2016) (“Standing to sue is a doctrine rooted in the traditional understanding of a case or controversy.”). The “‘irreducible constitutional minimum’ of standing consists of three elements. 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*, 578 U.S. 330 at 338. Indeed, “Article III standing requires a concrete injury even in the context of a statutory violation.” *Id.* at 341;

*TransUnion LLC v. Ramirez*, 594 U.S. 413 (2021) (to establish injury in fact, plaintiff’s allegations must be sufficient to show he suffered a concrete harm).

## II. FACTS AND PROCEDURAL HISTORY

Bojangles is a fast-food chain that owns and operates over 800 locations throughout the United States. Doc. No. 1 (“Complaint”) ¶21. Plaintiffs Alexis Dougherty, James Higgins, Peter Bungert, Leonardo Yon, Dennis Calabrese, Jessie Ruiz-Jacobs, Lily Nicole Portee, Christie Starnes, and Kassandra Blankenship are former Bojangles employees. *Id.* ¶¶ 41, 59, 71, 89, 103, 112, 130, 149, 155. They allege that Bojangles gathers various types of highly sensitive personal identifiable information (“PII”) and protected health information (“PHI”) (together “PII/PHI”) from its employees, including names, addresses, Social Security Numbers, driver’s license information, passport information, government issued ID numbers, state ID numbers, financial information (including debit and credit card numbers and financial account numbers),<sup>1</sup> health insurance information, and medical information. *Id.* ¶¶ 22, 28. Further, Plaintiffs allege that Bojangles then stores and maintains that PII/PHI for years, without implementing reasonable cybersecurity safeguards or protocols. *Id.* ¶ 3.

In February 2024, Bojangles was the victim of a cyberattack (the “Data Breach”), which Plaintiffs allege was carried out by the cybercriminal group “Hunters.” *Id.* ¶¶ 26, 37. In a Notice sent on November 19, 2024, to those who may have been impacted, Bojangles stated it had determined “that certain files were viewed and downloaded by an unknown actor between February 19, 2024 and March 12, 2024.” *Id.* ¶ 27. Each of the Plaintiffs received the Notice, and

---

<sup>1</sup> Significantly, however, Plaintiffs do not detail the specific types of PII/PHI each provided, with the exception that some of the Plaintiffs allege either that they provided their Social Security numbers to Bojangles or that the Notice they received said their Social Security numbers may have been impacted. *See id.* ¶¶ 60, 90, 104, 148, 159.

claims that their PII and or PHI is at risk. *Id.* ¶¶ 47, 61, 77, 91, 104, 118, 136, 148, 155. Eight of the nine Plaintiffs do not allege any specific identity theft or other data misuse resulting from the Data Breach; rather, they claim injury based on the threat of harm as a result of the potential sale of their information on the Dark Web, an increase in spam and scam phone calls, diminution in the value of personal information, time spent mitigating the potential impact of the Data Breach, and emotional distress. *See id.* ¶ 40. (alleging that Plaintiffs’ “stolen PII/PHI has already been published—or will be published imminently—by cybercriminals on the Dark Web”). Plaintiff Jessie Ruiz-Jacobs alleges fraudulent charges on his debit card but, importantly, does not allege that he provided the debit card number to Bojangles as part of his employment. *Id.* ¶ 98.

On January 30, 2025, Plaintiffs sued Bojangles on behalf of themselves and the putative class of all those potentially impacted by the Data Breach, alleging the following claims: (i) negligence, (ii) negligence per se, (iii) breach of implied contract, (iv) invasion of privacy, (v) unjust enrichment, (vi) breach of fiduciary duty, (vii) Violation of North Carolina Unfair and Deceptive Trade Practices Act, and (viii) declaratory judgment. Bojangles filed its Motion to Dismiss on April 1, 2025. The motion is fully briefed and ripe for the Court’s decision.

### **III. DISCUSSION**

There is no dispute among the Parties that Plaintiffs’ PII/PHI may have been impacted by the Data Breach. Yet, as discussed below, to properly pursue their claims Plaintiffs must allege more than the fact of the Data Breach and the potential threat of resulting damages. That is, the legal question before the Court is whether any of the Plaintiffs has sufficiently alleged facts that plausibly establish that they suffered a concrete injury that is fairly traceable to the Data Breach. The Court finds that Plaintiffs’ allegations fall short, ultimately only describing the possibility of future harm that is inherent in every data security incident, but cannot support the Article III

standing necessary to pursue a federal lawsuit. Therefore, Plaintiffs' Complaint will be dismissed pursuant to Federal Rule of Civil Procedure 12(b)(1).

*TransUnion* governs this Court's consideration of how to apply "the Article III requirement that the plaintiff's injury in fact be concrete" in the context of a class action. 594 U.S. at 424 (cleaned up); *Sikes v. Sree Hotels, LLC*, No. 3:24-CV-00679-KDB-DCK, 2024 WL 5130865, at \*1–3 (W.D.N.C. Dec. 16, 2024). In *TransUnion*, the named plaintiff brought a class action, alleging that TransUnion, a credit reporting agency, had violated the Fair Credit Reporting Act by failing to use reasonable procedures before placing a misleading alert in his credit file that labeled him as a potential terrorist, drug trafficker, or serious criminal and sending him mailings with formatting errors. *Id.* at 419–21. The district court certified a class of more than 8,000 people who had the same misleading alert added to their credit files and had also received similar mailings. A jury then awarded each class member statutory and punitive damages.

The Supreme Court reversed the awards, holding that only class members whose credit reports had been provided to third-party businesses had suffered sufficient "concrete harm" to support standing. *Id.* at 417. The Court rejected the argument that the other class members had "suffered a concrete injury for Article III purposes because the existence of misleading ... alerts in their internal credit files exposed them to a material risk that the information would be disseminated in the future to third parties and thereby cause them harm." *Id.* at 435. In its Opinion, the Supreme Court emphasized that, put simply, "[n]o concrete harm, no standing." *Id.* at 417. It explained that while "[t]he most obvious" concrete injuries are "tangible harms, such as physical harms and monetary harms," "[v]arious intangible harms can also be concrete," depending on whether they have "a close relationship to harms traditionally recognized as providing a basis for lawsuits in American courts." *Id.* at 425.

Then, most important here, the Court applied those principles to class actions, observing that “standing is not dispensed in gross.” *Id.* at 431. It stated that federal courts lack “the power to order relief to any uninjured plaintiff, class action or not,” *id.* (quoting *Tyson Foods, Inc. v. Bouaphakeo*, 577 U.S. 442, 466 (2016) (Roberts, C.J., concurring)), and that, as a result, “[e]very class member must have Article III standing in order to recover individual damages,” *id.* Moreover, “plaintiffs must demonstrate standing for each claim that they press and for each form of relief that they seek.” *Id.* Finally, the Court also made clear that the form of relief sought matters when assessing the sufficiency of the alleged harm. While “a person exposed to a risk of future harm may pursue forward-looking, injunctive relief to prevent the harm from occurring,” *id.* at 435, “the risk of future harm on its own does not support Article III standing for [a] damages claim,” *id.* at 441.

Therefore, following *TransUnion*, it is clear that to recover damages from Defendant, “[e]very class member must have Article III standing” “for each claim that they press,” requiring proof that the challenged conduct caused each of them a concrete harm. 594 U.S. at 431. It is equally clear that, to establish their standing to recover damages, the plaintiffs cannot rely on a “mere risk of future harm.” *Id.* at 437. Instead, *TransUnion* requires a sufficient factual showing for each class member to claim damages. *See id.* at 431 (explaining that standing must be demonstrated for every class member with “specific facts”).

Consistent with *TransUnion*, courts in the Fourth Circuit have concluded that in the context of class actions alleging claims arising from a “data breach,” plaintiffs must allege facts that show “*actual misuse* of [their] [personal information] disclosed by the data breach.” *Sikes*, 2024 WL 5130865, at \*1–3 (quoting *Capiau v. Ascendum Mach., Inc.*, No. 3:24-CV-00142-MOC-SCR, 2024 WL 3747191, at \*4 (W.D.N.C. Aug. 9, 2024)) (emphasis in original); *see Beck v. McDonald*,

848 F.3d 262, 272 (4th Cir. 2017) (“Actual misuse is the keystone of Article III injury in Fourth Circuit data breach case law.”). Therefore, “being subjected to a data breach isn’t in and of itself sufficient to establish Article III standing without a nonspeculative, increased risk of identity theft.” *O’Leary v. TrustedID, Inc.*, 60 F.4th 240, 244 (4th Cir. 2023).

One way for a data breach plaintiff to establish actual misuse—and thus Article III injury—is to credibly plead “that their data [has] been used in a fraudulent manner” as a consequence of the breach. *Stamat v. Grandizio Wilkins Little & Matthews, LLP*, No. CV SAG-22-00747, 2022 WL 3919685, at \*5 (D. Md. Aug. 31, 2022) (citing *Hutton v. Nat’l Bd. of Examiners in Optometry, Inc.*, 892 F.3d 613, 622 (4th Cir. 2018)); *Capiau*, 2024 WL 3747191, at \*3. For example, depending on the specific allegations in a particular case, the use of or attempt to use a plaintiff’s personal information to open a credit card account without their authorization, or receipt of spam communications related to the data breach may be sufficient to establish data misuse and standing. *See Hutton*, 892 F.3d at 621–23; *Capiau*, 2024 WL 3747191, at \*3; *Krottner v. Starbucks Corp.*, 628 F.3d 1139, 1141 (9th Cir. 2010) (two months after theft of Plaintiff’s laptop someone attempted to open a new account using his social security number); *See also In re Marriott Int’l, Inc., Customer Data Sec. Breach Litig.*, 440 F. Supp. 3d 447, 459 (D. Md. 2020) (complaint “contains allegations of actual misuse by some of the plaintiffs”); *Bank of Louisiana v. Marriott Int’l, Inc.*, 438 F. Supp. 3d 433, 440 (D. Md. 2020) (complaint alleges that “payment card information actually has been accessed, and used in a fraudulent manner”).

However, in other circumstances involving data exposure, courts have dismissed claims based on a lack of standing. *See Beck*, 848 F.3d at 274-75 (Theft of laptop containing personal information insufficient to establish actual harm or substantial risk of imminent harm); *Kimbriel v. ABB, Inc.*, No. 5:19-CV-215-BO, 2019 WL 4861168, at \*3 (E.D.N.C. Oct. 1, 2019) (plaintiffs

merely alleged their information was used to conduct a credit inquiry); *Krohm v. Epic Games, Inc.*, 408 F. Supp. 3d 717, 720 (E.D.N.C. 2019) (“plaintiff’s complaint contains no facts showing, or even suggesting, that his personal data has been used as a result of the cyber vulnerability”); *Stamat*, 2022 WL 3919685, at \*5–6 (finding Plaintiff alleged no actual misuse of his personal data and that “all potential harms and misuses of his data remain hypothetical”).

With respect to a plaintiff’s claims of future harm and pursuit of forward-looking, injunctive relief, standing may be found even if harm has not already occurred so long as the risk of harm is “sufficiently imminent and substantial.” *TransUnion*, 594 U.S. at 435-36 (citing *Clapper v. Amnesty Int’l USA*, 568 U.S. 398, 414 n.5 (2013)). See *DaimlerChrysler Corp. v. Cuno*, 547 U.S. 332, 345 (2006) (an asserted injury is “imminent” when it is “certainly impending”); *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 564–65, n.2 (1992) (same); *Whitmore v. Arkansas*, 495 U.S. 149, 158 (1990) (“A threatened injury must be ‘certainly impending’ to constitute injury in fact.”); *Beck*, 848 F.3d at 277–78 (“The most that can be reasonably inferred from the Plaintiffs’ allegations regarding the likelihood of another data breach ... is that the Plaintiffs *could* be victimized by a future data breach. That alone is not enough.”). Also, “to have standing to pursue damages based on a risk of future harm, plaintiffs must demonstrate a *separate* concrete harm ‘caused by their exposure to the risk itself.’” *Webb*, 72 F.4th at 372 (quoting *TransUnion*, 594 U.S. at 436). Relatedly, in the Fourth Circuit, a plaintiff’s claim of “emotional upset” and “fear [of] identity theft and financial fraud” resulting from a data breach is not an “adverse effect” sufficient to confer Article III standing. *Beck*, 848 F.3d at 271–73.

Plaintiffs’ allegations of harm as a consequence of the Data Breach fall squarely in the “might be a problem” rather than the “is already a problem” category. As noted above, Plaintiffs claim that there is an ongoing *threat* of identity theft based on what they allege is the publication



or “imminent” publication of their PII/PHI on the “Dark Web,” but they do not allege facts that establish that “imminence” (as the months pass further away from the date of the Data Breach) or any actual harm, such as the attempt to open credit card accounts or other misuse of social security numbers.

Further, an allegation of an increase in spam calls since the Data Breach cannot alone support standing without a specific connection to the breach (which is not alleged here). *Compare Burger v. Healthcare Mgmt. Sols., LLC*, No. 23-1215, 2024 WL 473735, at \*6 (D. Md. 2024) (“[G]eneric allegation[s] of increased spam calls and emails, if [] injur[ies] at all, fail[] to plausibly show that [the plaintiffs’] alleged injuries were the result of [the] [d]efendant’s conduct.” (internal quotation marks omitted)); *with Capiau*, 2024 WL 3747191 at \*2 (named plaintiff alleged that he received emails, text messages, and calls from someone pretending to be the CEO of the company that was hacked). In fact, there is no specific allegation that any of the Plaintiffs provided their cell phone numbers to Bojangles (which were then taken in the Data Breach) so they cannot show how their alleged increase in spam calls are sufficiently connected to the Data Breach. *See Holmes v. Elephant Ins. Co.*, No. 22-487, 2023 WL 4183380, at \*6 (E.D. Va. June 26, 2023) (finding alleged increase in spam calls not fairly traceable to data breach where “plaintiffs do not allege that the PI in this Data Breach included cell phone numbers”). Plaintiffs’ allegations of diminution in the value of personal information, time spent mitigating the potential impact of the Data Breach, and emotional distress are similarly insufficient. *See Panighetti v. Intelligent Bus. Sols., Inc.*, No. 1:23CV209, 2025 WL 1796454, at \*4 (M.D.N.C. June 30, 2025) (“Emotional upset” is itself insufficient to support standing).

Finally, Plaintiff Jessie Ruiz-Jacobs' allegations that he experienced fraudulent charges on his debit card would support standing as actual harm, if he could plausibly establish that the charges are traceable to the Data Breach. A "plaintiff must 'clearly ... allege facts demonstrating each element' of standing, including traceability." *See Springmeyer v. Marriott Int'l, Inc.*, No. 20-867, 2021 WL 809894, at \*2 (D. Md. Mar. 3, 2021) (quoting *Spokeo*, 578 U.S. at 337). However, Mr. Ruiz-Jacobs does not allege that he provided his debit card number to Bojangles as part of his employment. *Id.* ¶ 98. In the absence of that allegation, there is no means to connect the fraudulent charges on his debit card to the Data Breach. *See Blood v. Labette Cnty. Med. Ctr.*, No. 22-4036, 2022 WL 11745549, at \*5 (D. Kan. Oct. 20, 2022) (finding that allegations of stolen Social Security numbers and unauthorized charges to bank accounts cannot establish traceability because the allegations did not include a "plausible, non-speculative connection"). Therefore, Plaintiff Jessie Ruiz-Jacobs cannot establish the traceability necessary for standing.

In sum, Plaintiffs have failed to establish a concrete injury as a result of the Data Breach sufficient to give them standing to pursue their claims in this Court, and the Motion to Dismiss will be granted.

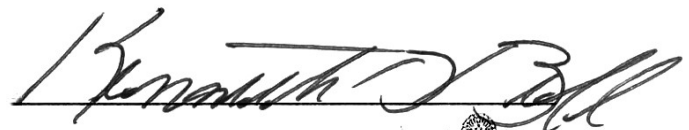
#### IV. ORDER

##### NOW THEREFORE IT IS ORDERED THAT:

1. Defendant's Motion to Dismiss (Doc. No. 24) is **GRANTED**; and
2. The Clerk is directed to close this matter in accordance with this Order.

##### SO ORDERED ADJUDGED AND DECREED.

Signed: September 30, 2025



Kenneth D. Bell  
United States District Judge

