[Cite as *Jessica v. Ohio Dept. of Job & Family Servs.*, 2025-Ohio-2604.]

IN THE COURT OF APPEALS OF OHIO

TENTH APPELLATE DISTRICT

Jessica Short,	:	
Plaintiff-Appellant,	:	No. 24AP-423 (Ct. of Cl. No. 2023-00771JD)
v.	:	(REGULAR CALENDAR)
Ohio Department of Job and Family Services,	:	
Defendant-Appellee.	:	

D E C I S I O N

Rendered on July 24, 2025

On brief: *DannLaw, Marc E. Dann*, and *Brian D. Flick*; *Zimmerman Law Offices, P.C.*, and *Thomas A. Zimmerman, Jr.*, for appellant. **Argued**: *Andrew M. Engel.*

On brief: *Keating Muething & Klekamp, PLL, Stacy A. Cole, Bryce J. Yoder*, and *John E. Dahm*; [*Dave Yost*, Attorney General,] and *Heather M. Lammardo*, for appellee. **Argued**: *Stacy A. Cole.*

APPEAL from the Court of Claims of Ohio

MENTEL, J.

{¶ 1} Plaintiff-appellant, Jessica Short, appeals from a judgment of the Court of Claims of Ohio granting the Civ.R. 12(B)(6) motion filed by defendant-appellee, Ohio Department of Job and Family Services ("ODJFS"). For the reasons that follow, we reverse.

I. Facts and Procedural History

{¶ 2} On December 19, 2023, Ms. Short filed a complaint against ODJFS on behalf of herself and a class of similarly situated individuals asserting claims for negligence,

breach of implied contract, breach of fiduciary duty, and invasion of privacy. The events giving rise to the complaint concerned a data breach at Ohio's unemployment compensation system. ODJFS administers Ohio's unemployment compensation system and Ms. Short received unemployment benefits from ODJFS.

{¶ 3} On July 24, 2023, ODJFS issued a news release stating its "information technology team discovered and fixed a security flaw that fraudsters attempted to exploit in Ohio's unemployment system." (Compl. Ex. 1.) ODJFS explained it had experienced "an increased number of attempts to fraudulently access the state's unemployment system" and locked "more than 28,000 [unemployment] accounts with suspicious activity" as a precaution. (Compl. Ex. 1.) ODJFS estimated it paid out $189,184.62 in "bogus claims" as a result of the data breach. (Compl. Ex. 1.)

{¶ 4} On August 25, 2023, ODJFS sent Ms. Short a letter notifying her of the data breach. The notice letter explained ODJFS discovered "potentially fraudulent activity" occurring in its unemployment system and determined "criminals were exploiting a security flaw in the system to 'take over' the accounts of legitimate unemployment claimants." (Compl. Ex. 2.) ODJFS informed Ms. Short her unemployment account "may have been accessed by unauthorized individuals" during the data breach and stated the "information involved included [her] name, social security number, address and work, claim and application history." (Compl. Ex. 2.) ODJFS indicated it had "corrected the flaw" and offered Ms. Short a complimentary one-year membership in an identity theft protection service "[a]s a precaution." (Compl. Ex. 2.) ODJFS also informed Ms. Short of "other precautionary measures [she could] take to protect [her] personal information, including placing a Fraud alert and/or Security Freezes on her credit files" and "review[ing] [her] financial account statements and credit reports for fraudulent or irregular activity on a regular basis." (Compl. Ex. 2.)

{¶ 5} In the complaint, Ms. Short explained she provided ODJFS with her personally identifiable information ("PII") in order to receive unemployment benefits. Ms. Short alleged ODJFS "assumed legal and equitable duties" to protect and safeguard the PII in its possession. (Compl. at ¶ 6.) Ms. Short claimed ODJFS "failed to take proper measures to safeguard" her and the class members' PII "from foreseeable cybersecurity threats," and that ODJFS "allowed criminals to hack its systems and steal Plaintiff's and Class Members'

sensitive and confidential information." (Compl. at ¶ 4.) Ms. Short alleged she personally suffered the following injuries as a result of ODJFS's conduct: (1) she "spent time reviewing credit reports, reviewing various credit alerts received by text and email, checking her financial information, and dealing with increased spam text messages and emails[,]" (2) she discovered "unauthorized and fraudulent charges on her bank account which required the bank to close out her accounts and reissue bank cards[,]" (3) she suffered "damages to and diminution in the value of [her] PII[,] (4) she suffered "lost time, annoyance, interference, and inconvenience because of the Data Breach, and [she] has anxiety and increased concerns for the loss of her privacy[,]" (5) she suffered "imminent and impending injury arising from the present and ongoing risk of fraud, identity theft, and misuse[,]" and (6) she will incur "future costs and expenses" for "[f]uture identity theft monitoring." (Compl. at ¶ 96-102.) Although Ms. Short noted that, "in some circumstances," ODJFS "temporarily deactivated claimants' accounts causing claimants a significant delay in receiving the benefits to which they were entitled," Ms. Short did not allege that she personally experienced a delay in receiving her unemployment benefits. (Compl. at ¶ 82.)

{¶ 6} Ms. Short's claims for negligence, breach of implied contract, breach of fiduciary duty, and invasion of privacy all concerned ODJFS's alleged failure to protect and safeguard the class members' PII and the resulting exposure of the PII. Ms. Short identified the potential class as including "[a]ll Ohio residents whose personal information was actually acquired or potentially accessed during the Data Breach." (Compl. at ¶ 110.) Ms. Short asked the court to certify the action as a class action and award her and the class compensatory damages and injunctive relief.

{¶ 7} On February 20, 2024, ODJFS filed a motion to dismiss the complaint pursuant to Civ.R. 12(B)(1) and/or 12(B)(6). ODJFS asked the court to dismiss the case either because the court lacked subject-matter jurisdiction, Ms. Short lacked standing, or because Ms. Short failed to state a claim upon which relief could be granted. On March 26, 2024, Ms. Short filed a memorandum in opposition to ODJFS's motion to dismiss.

{¶ 8} On June 10, 2023, the trial court issued a decision and entry granting ODJFS's motion to dismiss for lack of standing. The court acknowledged the case involved a "novel issue for Ohio state courts related to alleged identity theft resulting from data breaches." (Decision at 8.) The court relied on *Howe v. Cincinnati State Technical and*

Community College, Ct. of Claims No. 2022-00830JD (June 21, 2023) and *In re Science Applications Internatl. Corp. (SAIC) Backup Tape Data Theft Litigation*, 45 F.Supp.3d 25 (D.D.C. 2014) to conclude that Ms. Short alleged "only a risk of identity theft and, at this point, the likelihood that Plaintiff or members of the putative class [would] suffer harm remain[ed] speculative and dependent on the actions of unknown third parties–namely, the cybercriminals who exploited Defendant's system." (Decision at 10.) As such, the court stated it was " 'reluctant to grant standing where the alleged future injury depends on the actions of an independent third party.' " (Decision at 10, quoting *SAIC* at 25-26.) The court also found the fraudulent charges on Ms. Short's bank account, the time she spent monitoring her accounts, her increased anxiety, her future costs for identity theft monitoring, and the alleged diminution in the value of her PII failed to provide Ms. Short with standing. Because the court dismissed the case for lack of standing, the court did not analyze ODJFS's remaining arguments for dismissal.

II. Assignments of Error

{¶ 9} Ms. Short appeals, assigning the following error for our review:

> The trial court erred in granting Appellee's motion to dismiss.

III. Analysis

{¶ 10} Ms. Short's sole assignment of error asserts the trial court erred by granting ODJFS's motion to dismiss for lack of standing. " 'Standing' is defined at its most basic as '[a] party's right to make a legal claim or seek judicial enforcement of a duty or right.' " *Ohio Pyro, Inc. v. Ohio Dept. of Commerce*, 2007-Ohio-5024, ¶ 27, quoting *Black's Law Dictionary* 1442 (8th Ed. 2004). "Before an Ohio court can consider the merits of a legal claim, the person or entity seeking relief must establish standing to sue." *Id. Accord State ex rel. Ohio Gen. Assembly v. Brunner*, 2007-Ohio-3780, ¶ 15, quoting *Cuyahoga Cty. Bd. of Commrs. v. State,* 2006-Ohio-6499, ¶ 22 (noting " '[a] preliminary inquiry in all legal claims is the issue of standing' "). Whether a party has established standing to bring an action is a question of law that we review de novo. *Moore v. Middletown*, 2012-Ohio-3897, ¶ 20, citing *Cuyahoga Cty. Bd. of Commrs.* at ¶ 23.

{¶ 11} Standing depends on "whether the plaintiffs have alleged such a personal stake in the outcome of the controversy that they are entitled to have a court hear their

case." *ProgressOhio.Org, Inc. v. JobsOhio*, 2014-Ohio-2382, ¶ 7. At a minimum, common-law standing requires the litigant to demonstrate that he or she has suffered (1) an injury (2) that is fairly traceable to the defendant's allegedly unlawful conduct and (3) is likely to be redressed by the requested relief. *Ohioans for Concealed Carry, Inc. v. Columbus*, 2020-Ohio-6724, ¶ 12, citing *Moore* at ¶ 22. "These three factors–injury, causation, and redressability–constitute 'the irreducible constitutional minimum of standing.' " *Moore* at ¶ 22, quoting *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560 (1992).

{¶ 12} An injury involves " 'an invasion of a legally protected interest which is (a) concrete and particularized and (b) "actual or imminent, not 'conjectural' or 'hypothetical.' " ' " *Cool v. Frenchko*, 2022-Ohio-3747, ¶ 23 (10th Dist.), quoting *Lujan* at 560. An injury is particularized when the injury "is not bourne by the population in general, but affects the plaintiff in a personal and individual way." *Ohio Democratic Party v. LaRose*, 2020-Ohio-4664, ¶ 19 (10th Dist.), citing *Spokeo, Inc. v. Robins*, 578 U.S. 330, 339 (2016). An injury is fairly traceable to a defendant's conduct when "the conduct complained of [is] causally connected to the injury." *Bourke v. Carnahan*, 2005-Ohio-5422, ¶ 10 (10th Dist.), citing *Lujan* at 560. Finally, it must be likely, as opposed to merely speculative, that a favorable decision will redress the injury. *Id.*, citing *Lujan* at 560-61.

{¶ 13} A court "must determine whether standing exists by examining the state of affairs at the time the action commenced." *United States Bank Natl. Assn. v. Gray*, 2013-Ohio-3340, ¶ 20 (10th Dist.), citing *Deutsche Bank Natl. Trust Co. v. Najar*, 2013-Ohio-1657, ¶ 57 (8th Dist.). "Standing is an indispensable part of the plaintiff's case" and the plaintiff must prove standing "with the manner and degree of evidence required at the successive stages of litigation." *Id.*, citing *Lujan* at 561. *See also Huff v. Telecheck Servs.*, 923 F.3d 458, 462 (6th Cir. 2019) (noting that the "burden of establishing standing rests with [the plaintiff]" and "he must provide the allegations or evidence required at each stage of the litigation"). Standing does not depend on the merits of the plaintiff's claim; rather, "standing turns on the nature and source of the claim asserted by the plaintiffs." *Moore*, 2012-Ohio-3897, at ¶ 23.

{¶ 14} While Ms. Short sought to bring the present action as a class action, Ms. Short needed to establish her own individual standing to sue. *See Hamilton v. Ohio Sav. Bank*, 82 Ohio St.3d 67, 74 (1998). " '[E]ven named plaintiffs who represent a class must allege

and show that they personally have been injured, not that injury has been suffered by other unidentified members of the class to which they belong and which they purport to represent.' " *Woods v. Oak Hill Community Med. Ctr.*, 134 Ohio App.3d 261, 269 (4th Dist. 1999), quoting *Simon v. E. Kentucky Welfare Rights Org.*, 426 U.S. 26, 40 (1976), fn. 20. *See also Fallick v. Nationwide Mut. Ins. Co.*, 162 F.3d 410, 423 (6th Cir. 1998) (stating that "[a] potential class representative must demonstrate individual standing vis-[à]-vis the defendant; he [or she] cannot acquire such standing merely by virtue of bringing a class action").

{¶ 15} "Lack of standing challenges a party's capacity to bring an action and is properly raised by a Civ.R. 12(B)(6) motion to dismiss for failure to state a claim upon which relief can be granted." *Cramer v. Javid*, 2010-Ohio-5967, ¶ 10 (10th Dist.), citing *Brown v. Columbus City Schools Bd. of Edn.*, 2009-Ohio-3230, ¶ 4 (10th Dist.). *Accord Wilkins v. Village of Harrisburg*, 2015-Ohio-5472, ¶ 38 (10th Dist.) (stating a "motion to dismiss for lack of standing is properly brought pursuant to Civ.R. 12(B)(6)"). A lack of standing is a fundamental flaw that requires dismissal. *Bourke*, 2005-Ohio-5422, at ¶ 10; *Bank of Am., N.A. v. Kuchta*, 2014-Ohio-4275, ¶ 23.

{¶ 16} A Civ.R. 12(B)(6) motion to dismiss for failure to state a claim upon which relief can be granted is procedural and tests the sufficiency of the complaint. *Rudd v. Ohio State Hwy. Patrol*, 2016-Ohio-8263, ¶ 11 (10th Dist.). When ruling on a Civ.R. 12(B)(6) motion to dismiss, the trial court must presume all factual allegations in the complaint are true, construe the complaint in a light most favorable to the plaintiff, and make all reasonable inferences in favor of the plaintiff. *Brown v. Ohio Dept. of Rehab. & Corr.*, 2013-Ohio-4012, ¶ 6 (10th Dist.), citing *Mitchell v. Lawson Milk Co.*, 40 Ohio St.3d 190, 192 (1988). A trial " 'court is confined to the averments set forth in the complaint and cannot consider outside evidentiary materials' " when considering a Civ.R. 12(B)(6) motion. *Morrissette v. DFS Servs., LLC*, 2011-Ohio-2369, ¶ 20 (10th Dist.), quoting *Hutchinson v. Beazer East, Inc.*, 2006-Ohio-6761, ¶ 14 (8th Dist.). While a trial court must presume all factual allegations contained in the complaint are true, the court need not accept as true any unsupported and conclusory legal propositions advanced in the complaint. *Rudd* at ¶ 12, citing *Morrow v. Reminger & Reminger Co., LPA*, 2009-Ohio-2665, ¶ 7 (10th Dist.).

{¶ 17} A trial court properly dismisses a complaint for failure to state a claim upon which relief can be granted when it appears beyond doubt from the complaint that the plaintiff can prove no set of facts entitling him or her to relief. *Rudd* at ¶ 11, citing *O'Brien v. Univ. Community Tenants Union, Inc.*, 42 Ohio St.2d 242 (1975), syllabus. "[A]s long as there is a set of facts, consistent with the plaintiff's complaint, which would allow the plaintiff to recover, the court may not grant a defendant's motion to dismiss." *York v. Ohio State Highway Patrol*, 60 Ohio St.3d 143, 145 (1991). An appellate court reviews a trial court's dismissal pursuant to Civ.R. 12(B)(6) under a de novo standard of review. *State ex rel. Ohio Civ. Serv. Emps. Assn. v. State*, 2016-Ohio-478, ¶ 12.

A. Risk of Identity Theft or Fraud

{¶ 18} We first address Ms. Short's contention she suffered an injury due to the imminent "risk of fraud, identity theft, and misuse resulting from her PII being placed in the hands of unauthorized third parties." (Compl. at ¶ 101.)

{¶ 19} The trial court predominantly relied on two cases to conclude Ms. Short's risk of identity theft or fraud was too speculative to support standing: *Howe* and *SAIC*. Because *Howe* is an Ohio trial court decision and *SAIC* is a federal district court decision, neither decision amounts to binding authority on this court. *See Estate of Auckland v. Broadview NH, LLC*, 2017-Ohio-5602, ¶ 21 (10th Dist.), quoting *Keytack v. Warren*, 2006-Ohio-5179, ¶ 51 (11th Dist.) (stating that, as an appellate court in this state, " '[w]e are bound by the decisions of the Supreme Court of Ohio and generally, by past precedent produced by our own district' "); *State v. Sarigianopoulos*, 2013-Ohio-5772, ¶ 9 (7th Dist.) (noting that an appellate court can examine the "opinions of a trial court, and rely on them as persuasive legal authority if needed"); *Daniel E. Terreri & Sons v. Bd. of Mahoning County Commrs.*, 2003-Ohio-1227, ¶ 79 (7th Dist.) (noting Ohio courts are not prohibited from considering, "as persuasive authority, federal common law when Ohio caselaw is silent on the subject"). Whether a plaintiff has standing to sue based on a risk of identity theft or fraud resulting from a data breach appears to be an issue of first impression for the appellate courts of Ohio.

{¶ 20} In *Howe*, the plaintiffs filed suit against a college alleging cybercriminals targeted, accessed, and stole data files containing the plaintiffs' PII from the college's computer network. The plaintiffs alleged they were subject to a present and ongoing risk

of identity theft and fraud as a result. Relying on *SAIC*, the *Howe* court found the plaintiffs failed to allege an actual or imminent threat of injury because "the likelihood that Plaintiffs or members of the putative class [would] suffer harm [was] speculative and dependent on the actions of unknown third parties – namely the cybercriminals who stole files from [the college's] network." (June 21, 2023 Decision at 13.) As such, the *Howe* court dismissed the complaint for lack of standing.

{¶ 21} In *SAIC*, a thief broke into a car and stole the car's stereo, GPS system and several data tapes which were present in the car. The data tapes happened to contain personal information and medical records for millions of U.S. military members and their families. Although the defendant notified the affected service members about the stolen tapes and offered them one year of free credit monitoring, the court found the risk of identity theft resulting from the stolen tapes "speculative" because the risk was "entirely dependent on the actions of an unknown third-party – namely, the thief." *SAIC*, 45 F.Supp.3d at 25. The court noted it "[did] not know who [the thief] was, how much she knows about computers, or what she has done with the tapes. The tapes could be uploaded onto her computer" or they could be "lying in a landfill somewhere in Texas because she trashed them after achieving her main goal of boosting the car stereo and GPS." *Id.* The court explained it was reluctant to grant standing "where the alleged future injury depend[ed] on the actions of an independent third party." *Id.*, citing *Clapper v. Amnesty Intl. USA*, 568 U.S. 398 (2013).

{¶ 22} Thus, *SAIC* involved a theft of property which happened to include data tapes containing PII. Nothing in *SAIC* indicated the thief intentionally stole the data tapes in order to access the PII on the tapes. In contrast, here, the cybercriminals intentionally exploited a security flaw in ODJFS's network to "take over" legitimate unemployment accounts and defraud ODJFS. (Compl. Ex. 2.) Accordingly, the present case involves a far more targeted attack on the class members' PII than the property theft in *SAIC*. As such, we find *SAIC* distinguishable. Because *Howe* relied on *SAIC* for its holding, we find *Howe* distinguishable as well.

{¶ 23} Since the 2014 decision in *SAIC*, numerous federal circuit courts have addressed whether a risk of identity theft or fraud resulting from a data breach provides a plaintiff with standing to sue. Although some courts have suggested there is a split among

the federal circuits on the issue, whether standing exists depends on the specific factual allegations at issue in each case. *Compare Tsao v. Captiva MVP Restaurant Partners, LLC*, 986 F.3d 1332, 1340 (11th Cir. 2021) (analyzing cases and stating that the "Sixth, Seventh, Ninth, and D.C. Circuits have all recognized–at the pleading stage–that a plaintiff can establish injury-in-fact based on the increased risk of identity theft," while the "Second, Third, Fourth, and Eighth Circuits have declined to find standing on that theory"); *with McMorris v. Carl Lopez & Assocs., LLC*, 995 F.3d 295, 300 (2d Cir. 2021) (noting that while "[s]ome courts have suggested that there is a circuit split" on the issue, in actuality, "no court of appeals has explicitly foreclosed plaintiffs from establishing standing based on a risk of future identity theft"); *In re SuperValu, Inc.*, 870 F.3d 763, 769 (8th Cir. 2017) (noting the circuits seemingly dissimilar results "ultimately turned on the substance of the allegations before each court").

{¶ 24} Before we address the federal data breach cases, we note two United States Supreme Court decisions which are relevant to the injury-in-fact analysis: *Clapper*, 568 U.S. 398 and *TransUnion LLC v. Ramirez*, 594 U.S. 413 (2021). *See State ex rel. Walgate v. Kasich*, 2016-Ohio-1176, ¶ 23 (noting the "test for Article III standing, like the test for common-law standing in Ohio, requires an injury in fact, causation, and redressability"); *Ohio Democratic Party*, 2020-Ohio-4778, at ¶ 14. In *Clapper*, the court addressed a suit brought by organizations challenging the constitutionality of the Foreign Intelligence Surveillance Act of 1978, 50 U.S.C.S. § 1881a. The respondents alleged their work required them to engage in sensitive communications with individuals who they believed were likely targets of surveillance under § 1881a. The respondents claimed they suffered an injury in fact because there was "an objectively reasonable likelihood that their communications [would] be acquired under § 1881a at some point in the future." *Id.* at 401. The court noted "the well-established requirement that threatened injury must be 'certainly impending' " to be imminent. *Id.* at 401, quoting *Whitmore v. Arkansas*, 495 U.S. 149, 158 (1990).

{¶ 25} The court found the mere possibility the respondents' communications would be intercepted in the future involved a "highly attenuated chain of possibilities" which "rest[ed] on speculation about the decisions of independent actors." *Id.* at 410, 414. As such, the court found the respondents failed to "establish that injury based on potential future surveillance [was] certainly impending." *Id.* at 414. The respondents also alleged

they suffered a present injury because the risk of § 1881a-authorized surveillance caused them to take costly and burdensome measures to protect their communications. The court found no merit to this alleged injury, noting the respondents could not "manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that [was] not certainly impending." *Id.* at 416.

{¶ 26} In *TransUnion* a class of individuals sued TransUnion, a credit reporting agency, over a product TransUnion designed to help businesses avoid transacting with individuals on the U.S. Treasury Department's Office of Foreign Assets Control ("OFAC") list. The OFAC list generally consisted of terrorists, drug traffickers, and other serious criminals and it was "generally unlawful to transact business with any person on the list." *Id.* at 419. TransUnion's product compared the first and last names of consumers to the names on the OFAC list. If a match occurred, TransUnion would place an alert on the consumer's credit report indicating the consumer's name was a "potential match" to a name on the OFAC list. *Id.* at 420. Because many law-abiding Americans share first and last names with individuals on the OFAC list, TransUnion's product produced many false positives. The parties stipulated that, of the 8,185 class members, 1,853 class members had misleading credit reports disseminated by TransUnion to third party businesses, while the remaining 6,332 class members did not have any misleading credit reports disseminated by TransUnion to third party businesses.

{¶ 27} The Supreme Court explained a harm is considered concrete for purposes of standing when the alleged injury "has a 'close relationship' to a harm 'traditionally' recognized as providing a basis for a lawsuit in American courts." *Id.* at 424, quoting *Spokeo, Inc.*, 578 U.S. at 341. Such traditional harms include "physical harms and monetary harms," as well as "[v]arious intangible harms." *Id.* at 425. The court noted examples of intangible harms include "reputational harms, disclosure of private information, and intrusion upon seclusion." *Id.* at 425.

{¶ 28} The court had "no trouble concluding that the 1,853 class members suffered a concrete harm that qualifie[d] as an injury in fact." *Id.* at 432. Because TransUnion provided third party businesses "with credit reports containing OFAC alerts that labeled the [1,853] class members as potential terrorists, drug traffickers, or serious criminals," these class members "suffered a harm with a 'close relationship' to the harm associated with

the tort of defamation." *Id.* at 432. However, the court found the remaining 6,332 class members had not suffered a concrete injury because TransUnion did not disseminate any information about the 6,332 class members to potential creditors. The court found " 'no historical or common law analog where the mere existence of inaccurate information, absent dissemination, amounts to concrete injury.' " *Id.* at 434, quoting *Owner-Operator Independent Drivers Assn., Inc. v. United States Dept. of Transp.*, 879 F.3d 339, 344-45 (D.C.Cir. 2018).

{¶ 29} Ms. Short contends the Second Circuit in *Bohnak v. March & McLennan Companies, Inc.*, 79 F.4th 276 (2d Cir. 2023) "recently articulated 'the proper framework for evaluating whether an individual whose PII is exposed to unauthorized actors [in a data breach], but has not (yet) been used for injurious purposes such as identity theft,' " has standing to sue. (Appellant's Brief at 10, quoting *Bohnak*.) ODJFS notes that, although *Bohnak* had been decided when Ms. Short filed her memorandum in opposition to ODJFS's motion to dismiss, Ms. Short did not cite *Bohnak* in the trial court. ODJFS claims this court should "decline to consider Ms. Short's arguments based on *Bohnak* for the first time on appeal." (Appellee's Brief at 16.)

{¶ 30} "Issues raised for the first time on appeal are deemed to have been waived or forfeited through failure to assert them before the trial court." *Premiere Radio Networks, Inc. v. Sandblast, L.P.*, 2019-Ohio-4015, ¶ 7 (10th Dist.). Here, however, the parties thoroughly raised and addressed the *issue* of standing in the trial court.[1] Thus, no new *issue* has been raised on appeal. This court may consider any legal authority it finds persuasive, including the Second Circuit's decision in *Bohnak*, to resolve the issue of standing in the present case. *See Lawyers Coop. Pub. Co. v. Muething*, 65 Ohio St.3d 273, 275 (1992) (explaining that, while the plaintiff "raised for the first time [on appeal] the argument of the applicability" of a specific statute, the statute concerned the "affirmative defense of statute of limitations" which "was clearly raised in the trial court," so the plaintiff's failure to raise the specific statute in the trial court did not "prevent that party from obtaining a decision on [that] particular issue"); *Berrios-Romero v. Estado Libre Asociado De. Puerto*

[1] Additionally, "standing can be raised for the first time on appeal." *Bank of Am., N.A. v. Stewart*, 2014-Ohio-723, ¶ 38 (7th Dist.), fn. 1.

Rico et al., 641 F.3d 24, 27 (1st Cir. 2011) (noting a "decision of a sister court is a proper matter of judicial notice," because the court is taking "judicial notice of law, not of facts").

{¶ 31} The plaintiff in *Bohnak* alleged unauthorized actors targeted the defendant's computer system and accessed her PII during a data breach. The court initially applied *TransUnion* to find the plaintiff's risk of identity theft or fraud resulting from the data breach constituted a concrete injury. The *Bohnak* court noted that, "[s]imilar to the publication of misleading information about some of the plaintiffs in *TransUnion*, the core injury here—exposure of Bohnak's private PII to unauthorized third parties—bears some relationship to a well-established common-law analog: public disclosure of private facts." *Bohnak* at 285. *Accord Clemens v. ExecuPharm Inc.*, 48 F.4th 146, 157 (3d Cir. 2022), quoting *TransUnion* at 425 (finding the plaintiff's risk of identity theft or fraud resulting from a data breach was a concrete injury "because the harm involved [was] sufficiently analogous to harms long recognized at common law like the 'disclosure of private information' "); *Allen v. Wenco Mgt., LLC*, 696 F.Supp.3d 432, 437 (N.D.Ohio 2023), quoting *Bohnak* at 285 (noting "courts have held that a privacy injury stemming from a data breach 'bears some relationship to a well-established common-law analog: public disclosure of private facts' ").

{¶ 32} The complaint alleged unauthorized actors "accessed" and "stole[]" the class members' PII from ODJFS's system and used the PII to defraud ODJFS out of $189,184.62. (Compl. at ¶ 35.) Ms. Short also alleged the PII "was subsequently offered for sale on the dark web following the Data Breach."[2] (Compl. at ¶ 36.) "When standing is challenged in

[2] While the news release and notice letter demonstrated the hackers broke into ODJFS's system, took over legitimate unemployment accounts, and used those legitimate accounts to defraud ODJFS out of money, there was nothing in the news release or notice letter indicating the hackers stole Ms. Short's PII or that the hackers offered the information for sale on the dark web. However, Ohio is a notice pleading state. *Ohio Neighborhood Preservation Assn.*, 2023-Ohio-1281, ¶ 10. "The purpose of a notice pleading standard is to provide defendants with" " 'fair notice of the nature of the action.' " *Id.*, quoting *Boyland v. Giant Eagle*, 2017-Ohio-7335, ¶ 16 (10th Dist.). Unlike Ohio, federal courts use a heightened pleading standard. *See Ashcroft v. Iqbal*, 556 U.S. 662 (2007); *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544 (2009). Under the federal pleading standard, " '[f]actual allegations must be enough to raise a right to relief above the speculative level' and to 'state a claim to relief that is plausible on its face.' " *Keys v. Humana, Inc.*, 684 F.3d 605, 608 (6th Cir. 2012), quoting *Twombly* at 555, 570. *See also Tobin v. Interlinc Mtge. Servs., LLC*, 2025 U.S. Dist. LEXIS 79039 *8 (W.D.Ky. Apr. 25, 2025), fn. 2 (explaining the "standard for pleading in federal court is not notice pleading," because federal courts "require[] a stricter 'plausibility' pleading standard"). The Supreme Court of Ohio has expressly refused to adopt the heightened federal pleading standard. *See State ex rel. Ware v. Booth*, 2024-Ohio-2102, ¶ 5, fn. 1, citing *Maternal Grandmother, ADMR v. Hamilton Cty. Dept. of Job & Family Servs.*, 2021-Ohio-4096, ¶ 21-28 (DeWine, J., concurring in judgment only) (stating that the Supreme Court "has never adopted th[e] [heightened federal pleading] standard"

a motion to dismiss, the court must presume all the *factual* allegations in the complaint are true." (Emphasis in original.) *State ex rel. Ames v. Portage Cty. Bd. of Revision*, 2021-Ohio-4486, ¶ 13. Accordingly, accepting the factual allegations of the complaint as true, the core injury at issue in the present case concerned the acquisition and exposure of the class members' personal information by cybercriminals. This injury bears a close relationship to a common law claim for invasion of privacy. *See Cotton v. Ohio Dept. of Rehab. & Corr.*, 2014-Ohio-2619, ¶ 11 (10th Dist.), quoting *Housh v. Peth*, 165 Ohio St. 35 (1956), paragraph two of the syllabus (stating that an actionable claim for invasion of privacy involves the " 'unwarranted appropriation or exploitation of one's personality, the publicizing of one's private affairs with which the public has no legitimate concern, or the wrongful intrusion into one's private activities in such a manner as to outrage or cause mental suffering, shame or humiliation to a person of ordinary sensibilities' "); *Roe v. Heap*, 2004-Ohio-2504, ¶ 53 (10th Dist.). *See also TransUnion, LLC* at 433 (noting the harm need only bear a "close relationship" to a harm traditionally recognized as providing a basis for a lawsuit in American courts, "an exact duplicate" is not required).

{¶ 33} Accordingly, we find the risk of identity theft or fraud to be a concrete injury in the present case. The risk of identity theft or fraud was also particular to the plaintiffs, because the risk affected the plaintiffs in a personal way. *See Ohio Democratic Party*, 2020-Ohio-4778, at ¶ 19.

{¶ 34} We next consider whether the risk of identity theft or fraud was an actual or imminent injury. A future injury is imminent if it "is 'certainly impending,' or there is a 'substantial risk' that the harm will occur." *Susan B. Anthony List v. Driehaus*, 573 U.S. 149, 158 (2014), quoting *Clapper*, 568 U.S. at 409, 414, fn. 5. *See Clemens*, 48 F.4th at 152 (noting that "a plaintiff need not wait until he or she has actually sustained the feared harm in order to seek judicial redress, but can file suit when the risk of harm becomes imminent") (emphasis omitted); *McMorris*, 995 F.3d at 300, quoting *Susan B. Anthony List* at 158 (explaining that requiring plaintiffs to allege "they have already suffered identity theft or

established in *Iqbal* and *Twombly*). Accordingly, Ohio's "notice pleading" standard "does not require that the claim have 'facial plausibility.' " *S&T Bank, Inc. v. Advance Merchant Servs., LLC*, 2024-Ohio-4757, ¶ 55 (1st Dist.). Thus, at this stage of the litigation, we must accept as true Ms. Short's factual allegations indicating the hackers stole the PII and posted it for sale on the dark web. *Compare Quintero v. Metro Santurce, Inc.*, 2021 U.S. Dist. LEXIS 237071, *4, 6 (D.P.R. Dec. 9, 2021).

fraud as the result of a data breach would seem to run afoul of the Supreme Court's recognition that '[a]n allegation of future injury may suffice' ").

{¶ 35} The *Bohnak* court identified three, non-exhaustive factors courts use to determine whether a plaintiff whose PII was compromised in a data breach faces a substantial risk of identity theft or fraud. *Id.* at 288. First, courts consider whether "the data was compromised as the result of a targeted attack intended to get PII." *Id.* at 288. "Where a malicious third party has intentionally targeted a defendant's system and has stolen a plaintiff's data stored on that system, courts are more willing to find a likelihood of future identity theft or fraud sufficient to confer standing." *Id.* at 288. Second, courts consider whether some part of the compromised data "has been misused–even if a plaintiff's own data has not." *Id.* at 288, citing *McMorris* at 301. Examples of misuse include "fraudulent charges to the credit cards of *other* customers impacted by the same data breach, or evidence that a plaintiff's PII [was] available for sale on the Dark Web."[3] (Emphasis in original.) *Id.* at 288. Third, courts consider whether the exposed PII was of a "type 'more or less likely to subject plaintiffs to a perpetual risk of identity theft or fraud once it has been exposed.' " *Id.* at 288, quoting *McMorris* at 302. High-risk information "such as [SSNs] . . . especially when accompanied by victims' names–makes it more likely that those victims will be subject to future identity theft or fraud,' " while low-risk information that is "publicly available, or that can be rendered useless (like a credit card number unaccompanied by other PII), is less likely to subject plaintiffs to a perpetual risk of identity theft." *Id.* at 288, citing *McMorris* at 302.

{¶ 36} The plaintiff in *Bohnak* alleged "her PII was exposed as a result of a targeted attempt by a third party to access the data set" and that the "PII taken by the hackers include[d] her name and SSN." *Id.* at 288-89. The court noted the plaintiff "ha[d] not pulled off a hat trick with respect to the factors," since she "ha[d] not alleged any known misuse of the information in the dataset accessed in the hack." *Id.* at 289. However, because the factors are non-exhaustive, the court found the "allegations of a targeted hack that exposed Bohnak's name and SSN to an unauthorized actor [were] sufficient to suggest

[3] The Dark Web is " 'a portion of the Internet that is intentionally hidden from search engines and requires the use of an anonymizing browser to be accessed. It is most widely used as an underground black market where individuals sell illegal products like . . . sensitive stolen data that can be used to commit identity theft or fraud.' " *Clemens* at 150.

a substantial likelihood of future harm, satisfying the 'actual or imminent harm' component of an injury in fact." *Id.* at 289.

{¶ 37} Notably, the three imminence factors described in *Bohnak* are not unique to the *Bohnak* decision. Rather, these factors represent general principles distilled from the many federal courts to address when the threat of future identity theft or fraud resulting from a data breach is sufficiently imminent to confer standing. *See Clemens*, 48 F.4th at 153-54 (decided the year before *Bohnak* and noting that "[c]ourts rely on a number of factors in determining whether an injury is imminent . . . in the data breach context," including "whether the data breach was intentional," whether "the data was misused," and whether "the nature of the information accessed through the data breach could subject a plaintiff to a risk of identity theft"); *Webb v. Injured Workers Pharmacy, LLC*, 72 F.4th 365, 376 (1st Cir. 2023) (decided two months before *Bohnak* and noting the same three factors); *In re 21st Century Oncology Customer Data Sec. Breach Litigation (*hereinafter *21st Century)*, 380 F.Supp.3d 1243, 1254-55 (M.D.Fla. 2019) (decided years before *Bohnak* and noting the same three factors). *See also Santos-Pagan v. Bayamón Med. Ctr.*, 2024 U.S. Dist. LEXIS 179273, *13 (D.P.R. Sept. 30, 2024) (noting the "way in which a cyberattack is performed, and the ends pursued by the hackers, influence whether class action plaintiffs will have standing").

{¶ 38} For instance, in *Galaria v. Nationwide Mut. Ins. Co.*, 663 Fed.Appx. 384 (6th Cir. 2016), the court found the plaintiffs had standing to sue Nationwide after "hackers broke into Nationwide's computer network and stole the personal information of Plaintiffs and 1.1 million others." *Id.* at 386. The court found "no need for speculation where Plaintiffs allege[d] that their data ha[d] already been stolen and [was] now in the hands of ill-intentioned criminals. . . . Where a data breach targets personal information, a reasonable inference can be drawn that the hackers will use the victims' data for the fraudulent purposes alleged in Plaintiffs' complaints." *Id.* at 388. *See also Attias v. CareFirst, Inc.*, 865 F.3d 620, 628 (D.C.Cir. 2017) (explaining that because "an unauthorized party ha[d] already accessed personally identifying data on CareFirst's servers," no "long sequence of uncertain contingencies involving multiple independent actors ha[d] to occur before the plaintiffs in th[e] case [would] suffer any harm; a

substantial risk of harm exist[ed] already, simply by virtue of the hack and the nature of the data that the plaintiffs allege[d] was taken").

{¶ 39} In *Remijas v. Neiman Marcus Group, LLC*, 794 F.3d 688 (7th Cir. 2015), the court found the plaintiffs faced an imminent risk of identity theft or fraud after hackers attacked a department store's computer system, stole customers' credit card information, and a portion of the class incurred fraudulent charges on their credit cards. The court noted, "[w]hy else would hackers break into a store's database and steal consumers' private information? Presumably, the purpose of the hack [was], sooner or later, to make fraudulent charges or assume those consumers' identities." *Id.* at 693. *See also Webb*, 72 F.4th at 376 (finding the plaintiffs alleged an imminent risk of identity theft or fraud because the cybercriminals " 'infiltrated IWP's patient records systems' and 'stole[] PII,' " at least "some of the stolen PII ha[d] already been misused to file a fraudulent tax return in [one plaintiff's] name," and the PII included " 'patients' names and [S]ocial [S]ecurity numbers' "); *Hutton v. Natl. Bd. of Examiners in Optometry, Inc.*, 892 F.3d 613, 622 (4th Cir. 2018) (finding the plaintiffs alleged an imminent threat of identity theft or fraud because they "allege[d] that their data ha[d] been stolen, accessed, and used in a fraudulent manner").

{¶ 40} In *Clemens*, a known hacker group "named CLOP accessed Clemens's sensitive information," the hacker group "published Clemens's data on the Dark Web, a platform that facilitates criminal activity worldwide," and the data was "the type of data that could be used to perpetrate identity theft or fraud" because it included financial information, social security numbers, and full names. *Id.* at 157-58. As such, the *Clemens* court found the plaintiffs faced a substantial risk of identity theft or fraud resulting from the data breach.

{¶ 41} In contrast, other federal courts have found the risk of identity theft or fraud resulting from a data breach too speculative to support standing. For instance, in *Reilly v. Ceridian Corp.*, 664 F.3d 38, 40 (3d Cir. 2011), a hacker "infiltrated" a company's computer system and "potentially gained access to personal and financial information," but it was not "known whether the hacker read, copied, or understood" the personal data stored on the system. *Id.* at 40. The court determined the plaintiffs "alleged no misuse, and therefore, no injury. Indeed, no identifiable taking occurred; all that [was] known [was] that a firewall

was penetrated." *Id.* at 44. Accordingly, because the hackers did not target or misuse the data in *Reilly*, the court found the risk of identity theft to be "nothing more than speculation." *Id.* at 43.

{¶ 42} In *McMorris*, the plaintiffs alleged they were subject to a risk of identity theft or fraud after a company employee accidently sent an email containing the plaintiffs' PII to other employees of the same company. The court noted that, "[f]ar from being a 'sophisticated' or 'malicious' cyberattack 'carried out to obtain sensitive information for improper use,' " the situation in *McMorris* involved "the inadvertent disclosure of PII due to an errant email sent to approximately 65 employees." *Id.* at 303, citing *In re United States OPM Data Sec. Breach Litigation*, 928 F.3d 42 (D.C.Cir. 2019). As such, the court found the plaintiffs failed to demonstrate "a substantial risk of future identity theft or fraud," because the plaintiffs "never alleged that their data was intentionally targeted or obtained by a third party outside of [the company]." *Id.* at 303.

{¶ 43} In *Beck v. McDonald*, 848 F.3d 262 (4th Cir. 2017), a thief stole a laptop containing the plaintiffs' personal information from a medical center. *Id.* at 267. The medical center notified the plaintiffs about the incident and offered them a year of free credit monitoring. *Id.* The Fourth Circuit found the plaintiffs failed to allege a substantial risk of future identity theft because the plaintiffs had "no evidence that the [personal] information . . . ha[d] been accessed or misused" or that the thief "stole the laptop with the intent to steal their private information." *Id.* at 274. As such, the court found the chance of identity theft or fraud resulting from the stolen laptop involved the "same 'attenuated chain of possibilities' rejected by the Court in *Clapper*." *Id.* at 275. *See also In re SuperValu, Inc.*, 870 F.3d at 770 (finding the plaintiffs lacked standing because, although hackers stole the plaintiffs' credit card information, the stolen card information did not include "any personally identifying information, such as social security numbers, [or] birth dates," and a government report cited in the complaint demonstrated "there [was] little to no risk that anyone [would] use the Card Information stolen in these data breaches to open unauthorized accounts in the plaintiffs' names"); *Tsao*, 986 F.3d at 1343 (finding it "unlikely that the information allegedly stolen in the [data] breach, standing alone, raise[d] a substantial risk of identity theft," because the cybercriminals accessed credit and debit card information but not any PII).

{¶ 44} We find the reasoning of the federal circuit courts, regarding when the threat of future identity theft or fraud resulting from a data breach becomes imminent, to be persuasive. Applying the imminence factors to the present case, we find all the factors satisfied. The first factor concerns whether the data was compromised as part of a targeted attack intended to obtain the PII. Here, ODJFS's notice letter acknowledged the hackers exploited a security flaw in ODJFS's computer system that allowed the hackers to " 'take over' the accounts of legitimate unemployment claimants." (Compl. Ex. 2.) Ms. Short alleged the hackers "targeted and obtained Plaintiff's and Class Members' PII" and alleged the "PII was accessed and stolen in the Data Breach." (Compl. at ¶ 12, 35.) Accepting these factual allegations as true, they demonstrate the hackers targeted and stole the plaintiffs' PII.

{¶ 45} The second factor concerns whether some part of the data has been misused, even if the plaintiff's own data has not. The factual allegations demonstrated the hackers misused the data to file "bogus claims" and obtain $189,184.62 from ODJFS. (Compl. Ex. 1.) Even if the hackers did not use Ms. Short's unemployment account to defraud ODJFS, the hackers certainly misused some of the class members legitimate unemployment accounts to defraud ODJFS.

{¶ 46} Ms. Short also alleged she "believes . . . her PII, and the PII of Class Members, was subsequently offered for sale on the dark web following the Data Breach" by the "cybercriminals that perpetrated the hack." (Compl. at ¶ 12, 36.) While Ms. Short alleged she "believes" the hackers offered her PII for sale on the dark web, "pleading facts based upon the pleaders 'information and belief' is expressly authorized by Civ.R. 11." *Prime Invest., LLC v. Altimate Care, LLC*, 2022-Ohio-1181, ¶ 31 (10th Dist.). *See* Civ.R. 11; *Carasalina LLC v. Bennett*, 2014-Ohio-5665, ¶ 36 (10th Dist.) (observing that "[i]f a party makes an allegation or factual contention on information or belief, then the party must have the opportunity to investigate the truth of that allegation or factual contention"). Accordingly, the complaint also indicated the hackers misused the data by posting it for sale on the dark web. *See Clemens*, 48 F.4th at 157 (finding the plaintiff faced "a substantial risk of identity theft or fraud by virtue of her personal information being made available on underground websites," because "many of those who visit the Dark Web . . . do so with nefarious intent"); *21st Century*, 380 F.Supp.3d at 1255.

{¶ 47} The third factor concerns whether the data is of a type more or less likely to subject the plaintiffs to a perpetual risk of identity theft or fraud once exposed. The information involved in the data breach included Ms. Short's name, social security number, address, and her work, claim, and application history. Such information constitutes high risk information which makes it more likely Ms. Short will be subject to identity theft or fraud in the future. *See Bohnak* at 288, quoting *McMorris* at 302 (noting exposed PII which includes a social security number and the individual's name " 'makes it more likely that those victims will be subject to future identity theft or fraud' ").

{¶ 48} Thus, accepting the factual allegations of the complaint as true and making all reasonable inferences in Ms. Short's favor, we find Ms. Short alleged an imminent risk of identity theft or fraud resulting from the data breach. Accordingly, because Ms. Short alleged a concrete, particularized, and imminent injury, the risk of identity theft or fraud constituted an injury in fact.[4]

{¶ 49} ODJFS notes that well over a year has passed since Ms. Short filed her complaint. ODJFS asks, "[i]f the risk of fraud and identity theft to Ms. Short had been 'imminent' and 'certainly impending,' would it not have already occurred?" (Appellee's Brief at 21.) ODJFS's contention in this regard lacks merit because courts determine whether standing exists at the time the action commenced. *Gray*, 2013-Ohio-3340, at ¶ 20. Additionally, when reviewing a Civ.R. 12(B)(6) motion to dismiss, a court is confined " 'to the averments set forth in the complaint and cannot consider outside evidentiary materials.' " *Morrissette*, 2011-Ohio-2369, at ¶ 20, quoting *Hutchinson*, 2006-Ohio-6761,

[4] In the complaint, Ms. Short alleged ODJFS's offer of one year of complimentary credit monitoring in the notice letter demonstrated her PII was "in fact affected, accessed, compromised, and exfiltrated from Defendant's computer systems." (Compl. at ¶ 60.) Courts have taken opposing views regarding the significance of a defendant's offer of free credit monitoring following a data breach. *Compare Galaria*, 663 Fed.Appx. at 388 (stating Nationwide "seem[ed] to recognize the severity of the risk [of identity theft], given its offer to provide credit-monitoring and identity-theft protection for a full year"); *with Beck*, 848 F.3d at 276 ("declin[ing] to infer a substantial risk of harm of future identity theft from an organization's offer to provide free credit monitoring services," because such an inference "would surely discourage organizations from offering these services to data-breach victims, lest their extension of goodwill render them subject to suit"). Because we have already found the risk of identity theft or fraud to be an injury in fact, we need not address the significance of ODJFS's offer of one year of free credit monitoring. *See also* R.C. 1349.19(B)(1) (requiring any "person that owns or licenses computerized data that includes personal information" in Ohio to disclose any breach of its security system to any "resident of this state whose personal information was, or reasonably is believed to have been, accessed and acquired by an unauthorized person if the access and acquisition by the unauthorized person causes or reasonably is believed will cause a material risk of identity theft or other fraud to the resident").

at ¶ 14. Whether or not Ms. Short suffered identity theft or fraud since filing the complaint is a matter outside of the complaint, and therefore not a proper consideration at this stage of the litigation. *See In re Zappos.com, Inc.*, 888 F.3d 1020, 1028 (9th Cir. 2018) (noting that whether identity theft occurred since the plaintiff filed the complaint involved "facts outside the Complaint[] . . ., which ma[de] [the defendant's] argument one that may be appropriate for summary judgment but not one that may support a facial challenge to standing at the motion to dismiss stage").

B. Mitigation Costs and Emotional Injury

{¶ 50} While a person exposed to a future harm may pursue "forward-looking, injunctive relief to prevent the harm from occurring," standing to pursue injunctive relief "does not necessarily mean that the plaintiff has standing to seek retrospective damages." *TransUnion LLC*, 594 U.S. at 435-36.[5] However, *TransUnion* recognized that a "risk of future harm" could "cause[] a *separate* concrete harm." (Emphasis in original.) *Id.* at 436. Thus, to establish standing to pursue damages in a data breach case, the complaint "must also plausibly allege a separate concrete, present harm caused 'by [the plaintiffs'] exposure to [the] risk [of future harm].' " *Webb* at 376, quoting *TransUnion, LLC* at 437.

{¶ 51} When a plaintiff incurs mitigation costs in response to a speculative threat, such costs do not satisfy the injury-in-fact requirement. *Attias*, 865 F.3d at 629, citing *Clapper*, 568 U.S. at 416-17. *See McMorris*, 995 F.3d at 303, quoting *Clapper*, 568 U.S. at 416 (explaining this "notion stems from the Supreme Court's guidance in *Clapper*, where it noted that plaintiffs 'cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending' "); *Remijas*, 794 F.3d at 694 (explaining that "[m]itigation expenses do not qualify as actual injuries where the harm is not imminent"). However, when a plaintiff incurs costs "to mitigate or avoid harm when a substantial risk of harm actually exists," such costs satisfy the injury in fact requirement. *Hutton*, 892 F.3d at 622, citing *Clapper* at 414, fn. 5. *See*

[5] Ms. Short asked the trial court to issue an injunction requiring ODJFS to "adopt, implement, and maintain adequate security measures to protect its customers' personal and financial information." (Compl., Prayer for Relief G.) The trial court did not address whether Ms. Short had standing to pursue her request for injunctive relief. Because the trial court did not address Ms. Short's request for injunctive relief, and because neither party addresses this issue on appeal, we will not address the request for injunctive relief in the first instance. *See Bell v. Teasley*, 2011-Ohio-2744, ¶ 15 (10th Dist.), citing *Gangale v. Bur. of Motor Vehicles*, 2002-Ohio-2936, ¶ 13 (10th Dist.). *See also Webb* at 378.

Bohnak, 79 F.4th at 286 (finding the plaintiff's " 'out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft' and 'lost time' and other 'opportunity costs' associated with attempting to mitigate the consequences of the data breach" were concrete harms "foreseeably arising from the exposure of Bohnak's PII to a malign outside actor"). Accordingly, these "two theories of injury-in-fact," i.e. the risk of identity theft or fraud and any associated mitigation costs, "stand or fall together." *In re Marriott Internatl., Inc.*, 440 F.Supp.3d 447, 460 (S.D.Md. 2020).

{¶ 52} Ms. Short alleged that upon receiving the notice letter she "spent time reviewing credit reports, reviewing various credit alerts received by text and email, [and] checking her financial information." (Compl. at ¶ 96.) Ms. Short alleged she and the class suffered "loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk." (Compl. at ¶ 81.) A plaintiff's "time spent responding to a data breach can constitute a concrete injury sufficient to confer standing, at least when that time would otherwise have been put to profitable use." *Webb*, 72 F.4th at 377. *See also Galaria* at 388 (finding the "time and money" plaintiffs spent "to monitor their credit, check their bank statements, and modify their financial accounts" following the data breach constituted concrete injuries, because plaintiffs incurred these costs "to mitigate an imminent harm"); *In re Equifax*, 999 F.3d 1247, 1262 (11th Cir. 2021) (noting that "when a plaintiff faces a sufficient risk of harm, the time, money, and effort spent mitigating that risk are also concrete injuries"). Accordingly, Ms. Short's lost time spent responding to the data breach was a concrete, present injury.

{¶ 53} Although Ms. Short alleged she and the class sustained " 'out of pocket' costs incurred mitigating the materialized risk and imminent threat of identity theft," Ms. Short alleged she personally would incur "future costs and expenses" for future "identity theft monitoring." (Compl. at ¶ 81, 88, 102.) To the extent Ms. Short actually incurred out of pocket expenses to mitigate the risk of identity theft or fraud, such costs constitute a concrete injury. *See Bohnak* at 286. To the extent Ms. Short alleged only that she will incur costs for identity theft monitoring in the future, we note a plaintiff may obtain future damages when the damages are "limited to losses that the plaintiff is reasonably certain to incur from the injuries." *Bender v. Durrani*, 2024-Ohio-1258, ¶ 136 (10th Dist.). *See also Fisher v. Univ. of Cincinnati Med. Ctr.*, 2015-Ohio-3592, ¶ 22 (10th Dist.); *Hohn v. Ohio*

Dept. of Mental Retardation & Dev. Disabilities, 1993 Ohio App. LEXIS 6023, *13 (10th Dist. Dec. 14, 1993).

{¶ 54} In the complaint, Ms. Short alleged ODJFS's offer of one year of free credit monitoring was inadequate because it "fail[ed] to provide for the fact victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft and financial fraud." (Compl. at ¶ 59.) Ms. Short quoted from a U.S. Government Accountability Office report stating that " 'stolen data may be held for up to a year or more before being used to commit identity theft' " and that " 'once stolen data ha[s] been sold or posted on the Web, fraudulent use of that information may continue for years.' " (Compl. at ¶ 72.) Ms. Short alleged she and the class would have to "monitor their financial accounts for many years to mitigate the risk of identity theft" and would have to "sign[] up for credit and identity theft monitoring insurance, and monitor[] credit reports and accounts for unauthorized activity, which may take years to discover and detect." (Compl. at ¶ 87-88.) Viewing these allegations in a light most favorable to Ms. Short, we find Ms. Short alleged sufficient facts to demonstrate she will incur credit monitoring expenses in the future as a result of the data breach. *See Mason v. Wright Bros. Constr. Co.*, 2025 U.S. Dist. LEXIS 57386, *20 (E.D.Tn. Mar. 27, 2025) (finding that, because the plaintiff alleged he and the class would have to "pay for future credit and identity-theft monitoring for a minimum of seven years, which could cost two hundred dollars or more per year," the plaintiff "alleged facts that, if true, would entitle him to recover the reasonable and necessary cost of future credit monitoring").

{¶ 55} Ms. Short also alleged she experienced "anxiety and increased concerns for the loss of her privacy" as a result of the data breach. (Compl. at ¶ 100.) In *TransUnion* the court recognized a risk of future harm could cause "its own current emotional or psychological harm." *TransUnion, LLC* at 436, fn. 7. Thus, if a "plaintiff's knowledge of the substantial risk of identity theft causes [the plaintiff] to presently experience emotional distress . . . the plaintiff has alleged a concrete injury." *Clemens*, 48 F.4th at 156. Ms. Short's anxiety resulting from the data breach was a present emotional injury which supports standing. *See Landon v. TSC Acquisition Corp.*, 2024 U.S. Dist. LEXIS 237108, *20 (C.D.Ca. Nov. 1, 2024) (finding the allegations in the complaint sufficient to "allege

emotional damages at the motion to dismiss stage" because plaintiffs alleged the data breach "caused them to suffer 'fear, anxiety, and distress' ").

{¶ 56} Based on the foregoing, we find Ms. Short sufficiently alleged concrete, present harms resulting from the data breach. Ms. Short also claimed the injuries she and the class sustained "were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the PII" which "allowed criminals to hack its systems and steal Plaintiff's and Class Members' sensitive and confidential information." (Compl. at ¶ 4, 61.) Ms. Short sought monetary damages to compensate her for her injuries. Accordingly, Ms. Short adequately alleged her injuries were fairly traceable to ODJFS and were redressable. *See Galaria*, 663 Fed.Appx. at 390 (observing that, while the "hackers [were] the direct cause of Plaintiffs' injuries," the allegations of the complaint demonstrated that "but for Nationwide's allegedly lax security, the hackers would not have been able to steal Plaintiffs' data," which satisfied the traceability requirement); *Clemens*, 48 F.4th at 158 (finding the plaintiff adequately alleged traceability and redressability because she alleged the defendant's "failure to safeguard her information enabled [the hackers] to publish it on the Dark Web as part of the stolen dataset" and she sought "[monetary] damages to compensate for her losses"); *Webb*, 72 F.4th at 377 (finding traceability and redressability satisfied because the plaintiffs sought monetary damages and alleged defendant's "actions led to the exposure and actual or potential misuse of the plaintiffs' PII").

{¶ 57} Accordingly, Ms. Short had standing to pursue her claims against ODJFS based on her increased risk of identity theft or fraud and her lost time, mitigation costs, and emotional injury. Although Ms. Short alleged she suffered other injuries due to the data breach, including the fraudulent charges on her bank account and the diminution in the value of her PII, Ms. Short notes we "need only" address these other injuries if we determine she did not have standing based on the increased risk of identity theft or fraud. (Appellant's Brief at 21.) We agree. *See Attias*, 865 F.3d at 626, fn. 2 (explaining that, because the court found "all plaintiffs, including the Tringlers, ha[d] standing to sue CareFirst based on their heightened risk of future identity theft, [the court] need not address the Tringlers' separate argument as to *past* identity theft") (emphasis in original); *In re Zappos.com, Inc.*, 888 F.3d at 1030, fn. 15 (noting plaintiffs "need only one viable basis for standing," and because

the plaintiffs "sufficiently allege[d] standing from the risk of future identity theft, [the court would] not reach their other asserted bases for standing"); *Remijas*, 794 F.3d at 696 (explaining the court would not decide whether the plaintiffs other alleged injuries amounted to injuries in fact because the court already found the "injuries associated with resolving fraudulent charges and protecting oneself against future identity theft [were] sufficient to satisfy the first requirement of Article III standing"); *Webb*, 72 F.4th at 377. *See also Ohio Gen. Assembly*, 2007-Ohio-3780, at ¶ 22 (noting that because the relators had "standing to sue, as legislators who voted with the majority for Am.Sub.S.B. No. 117," the court "need not, and therefore [did] not, consider their other proffered bases for standing"); *Racing Guild, Local 304 v. Ohio State Racing Comm.*, 28 Ohio St.3d 317, 322 (1986). Because Ms. Short had standing to pursue her claims against ODJFS based on the imminent risk of identity theft or fraud and her lost time, mitigations costs, and emotional injury resulting from the data breach, we need not address whether Ms. Short's other claimed injuries provided her with standing.

{¶ 58} Based on the foregoing, we find the trial court erred by granting ODJFS's Civ.R. 12(B)(6) motion to dismiss based on Ms. Short's lack of standing. We therefore sustain Ms. Short's sole assignment of error.

IV. Conclusion

{¶ 59} Having sustained Ms. Short's sole assignment of error, we reverse the judgment of the Court of Claims of Ohio and remand the case to that court for proceedings consistent with this decision and law.

Judgment reversed;
cause remanded.

JAMISON, P.J. and EDELSTEIN, J., concur.