



IN THE
Court of Appeals of Indiana

Jason Hensley,
Appellant-Plaintiff

v.

Lewis Brothers Bakeries, Inc.,
Appellee-Defendant



June 30, 2025

Court of Appeals Case No.
24A-PL-2246

Appeal from the Vanderburgh Superior Court

The Honorable Thomas A. Massey, Judge

Trial Court Cause No.
82D07-2405-PL-2926

Opinion by Chief Judge Altice
Judges Brown and Taviton concur.

Altice, Chief Judge.

Case Summary

- [1] In a targeted attack, cybercriminals obtained personal identifiable information (PII), including full names and Social Security numbers, of past and former employees of Lewis Brothers Bakeries, Inc. (LBB), which LBB saved unencrypted on its computer network. Jason Hensley, a former employee of LBB whose PII was compromised in the data breach, filed this putative class action against LBB on behalf of himself and all others similarly situated, seeking injunctive relief and damages.
- [2] LBB filed an Ind. Trial Rule 12(b)(6) motion to dismiss based on lack of standing. The trial court granted the motion, agreeing with LBB that Hensley's alleged injuries did not meet the threshold for standing because Hensley did not allege that the data breach had resulted in any actual misuse of the stolen PII. Concluding that Hensley has alleged sufficient harm at the pleading stage to confer standing, we reverse and remand for further proceedings.
- [3] We reverse and remand.

Facts¹ & Procedural History

- [4] LBB is a large bakery company headquartered in Indiana with distribution throughout the United States. As a condition of employment, it requires employees to entrust it with highly sensitive PII. LBB assured employees that

¹ The facts are based on the allegations in the complaint.

such information would be kept safe and confidential and deleted after it was no longer needed. LBB retained such information on its computer network even after an employee relationship ended.

- [5] On March 25, 2024, LBB began experiencing unauthorized access to its network that resulted in certain files being stolen and encrypted by hackers. LBB discovered the data breach on April 1, 2024, and launched an investigation with the assistance of third-party forensic specialists. It was determined that the compromised data included individuals' full names, Social Security numbers, and other sensitive information.
- [6] On May 9, 2024, LBB sent notices to individuals whose PII was involved in the data breach and offered to cover twelve months of credit monitoring and identity protection services through Experian. LBB advised recipients to remain vigilant against incidents of identity theft and fraud by reviewing account statements, monitoring credit reports for suspicious activity, and enrolling in the complimentary monitoring services being offered by LLB.
- [7] Hensley's PII was among the PII accessed and stolen in the data breach. He alleges that the hackers targeted and obtained the highly sensitive PII, specifically Social Security numbers with full names, because of the PII's value in exploiting and stealing the identities of individuals. Hensley believes that his PII, as well as that of the proposed class members, was subsequently sold on the dark web following the data breach, as that is the modus operandi of cybercriminals that commit attacks of this type.

[8] As a result of the data breach, Hensley has spent considerable time dealing with the data breach and attempting to mitigate his heightened risk of identity theft and fraud that will last for many years. And he anticipates spending time and money on an ongoing basis to mitigate and address harms caused by the data breach well into the future. In addition to lost time, annoyance, and inconvenience, Hensley has experienced anxiety and increased concerns for the loss of his privacy, especially his Social Security number being in the hands of criminals. He has also been subjected to a large increase in spam/phishing emails and calls.

[9] Hensley, on behalf of himself and those similarly situated, filed this putative class action against LBB on May 16, 2024, seeking injunctive relief and damages based on theories of negligence, negligence per se, breach of contract, and unjust enrichment. Hensley alleged that he and the proposed class members suffered the following injuries as a result of LBB's actions: invasion of privacy; theft of PII; lost or diminished value of PII; lost time and opportunity costs associated with attempting to mitigate the consequences of the data breach; loss of the benefit of the bargain; and the continued risk to their PII, which remains unencrypted and available for unauthorized third parties to access and abuse and remains backed up in LBB's possession and is subject to further unauthorized disclosures so long as LBB fails to undertake appropriate and adequate measures to protect it.

[10] On July 12, 2024, LBB moved to dismiss Hensley’s complaint for lack of standing.² On September 12, 2024, after a hearing, the trial court granted LBB’s motion to dismiss. The trial court’s ruling was based exclusively on Hensley’s failure to allege that the data breach had resulted in any actual misuse of his PII. Without actual misuse, the court agreed with LBB that Hensley’s alleged injuries, including mitigation efforts and intangible harms, were not sufficient to meet the required threshold for standing. The trial court dismissed the action without prejudice, noting that Hensley “may in the future suffer an actual injury from the misappropriation of his PII.” *Appellant’s Appendix* at 9.

[11] Hensley appeals the dismissal.

Standard of Review

[12] Motions to dismiss for lack of standing may be brought under T.R. 12(B)(6) for failure to state a claim on which relief can be granted. *Hoosier Contractors, LLC v. Gardner*, 212 N.E.3d 1234, 1239 (Ind. 2023). When evaluating such a motion, courts must accept as true the factual allegations in the complaint, consider them in the light most favorable to the plaintiff, and draw every reasonable inference in favor of the plaintiff. *See id.* Further, on appeal, we review de novo the legal question of whether a party has standing. *Id.* at 1238.

² LBB also moved for dismissal based on Hensley’s alleged failure to state a claim pursuant to each of his four causes of action. LBB does not reassert these arguments on appeal.

Discussion & Decision

[13] “The threshold issue of standing determines whether a litigant is entitled to have a court decide the substantive issues of a dispute.” *Id.* (quoting *Solarize Ind., Inc. v. S. Ind. Gas & Elec. Co.*, 182 N.E.3d 212, 216 (Ind. 2022)). The standing requirement ensures that courts avoid engaging in “abstract speculation” and that courts act only in “real cases.” *Id.* Indiana law is clear that standing requires an injury, which is met when the plaintiff shows that he “has suffered or is in immediate danger of suffering a direct injury as a result of the complained-of conduct.” *Id.* (cleaned up); *see also Alexander v. PSB Lending Corp.*, 800 N.E.2d 984, 989 (Ind. Ct. App. 2003) (“The standing requirement assures that litigation will be actively and vigorously contested, as plaintiffs must demonstrate a personal stake in the litigation’s outcome in addition to showing that they have sustained, or are in immediate danger of sustaining, a direct injury as a result of the defendant’s conduct.”), *trans. denied.*

[14] We have little difficulty holding that Hensley adequately alleged that LBB’s actions, or lack thereof, have directly harmed him and/or placed him in immediate danger of harm. First, it is important to understand what this case is not. Hensley is not suing LBB exclusively to enforce a statutorily created right or to address violations of duties owed broadly to the community at large. *Cf. Hoosier Contractors*, 212 N.E.3d at 1236, 1242 (holding that plaintiff did not have standing to sue contractor for procedural violations of consumer-protection statutes where plaintiff was not actually damaged by the alleged deceptive acts, as he paid contractor nothing and hired a different company to repair his roof

for less money). Rather, he asserts common law claims of negligence and breach of contract arising as a result of his past employment relationship with LBB. In other words, he has a personal stake in the outcome of the litigation.

[15] Based on LBB's failure to protect **his** PII (as well as that of the class members), Hensley has alleged that bad actors targeted and obtained this sensitive information, including his Social Security number and full name. In his complaint, Hensley documents the risks of future identity theft involved in having this type of highly sensitive information stolen and likely available for purchase on the dark web. Indeed, "[i]t stands to reason that data compromised in a targeted attack is more likely to be misused." *Webb v. Injured Workers Pharmacy, LLC*, 72 F.4th 365, 375-76 (1st Cir. 2023) (citing a collection of cases); *see also Remijas v. Neiman Marcus Grp., LLC*, 794 F.3d 688, 693 (7th Cir. 2015) ("Why else would hackers break into a store's database and steal consumers' private information? Presumably, the purpose of the hack is, sooner or later, to make fraudulent charges or assume those consumers' identities."). And the risk of future misuse is certainly heightened where the compromised data is particularly sensitive, as in this case. *See In re Equifax Inc. Customer Data Sec. Breach Litig.*, 999 F.3d 1247, 1262 (11th Cir. 2021) (recognizing "the unequivocal damage that can be done with this type of data"); *Krupa v. TIC Int'l Corp.*, 2023 WL 143140, at *2 (S.D. Ind. Jan. 10, 2023) ("Having one's social security number stolen seems an obvious harm. If it were not a harm, why should [anyone] take any data security measures?"). There is nothing speculative about the risk of harm Hensley now faces; it is substantial.

[16] Further, Hensley has allegedly taken steps to mitigate his now-heightened risk of identity theft. The loss of time that he has already incurred in this regard is a compensable harm.³ See *McLaughlin v. Taylor Univ.*, 2024 WL 4274848, at *3 (N.D. Ind. Sept. 23, 2024) (recognizing that Indiana law allows as damages the value of lost time and concluding that “[t]he time and effort that data breach victims must expend is a real injury”); see also *Webster v. Bradford-Scott Data, LLC*, 2025 WL 560917, at *5 (N.D. Ind. Feb. 20, 2025) (observing that a plaintiff who has already lost time mitigating the risk of identity theft after a data breach has suffered an actual injury). And he has credibly alleged that he will need to take mitigation measures well into the future in light of the specific circumstances of this data breach.

[17] For these reasons, we conclude that Hensley has met Indiana’s requirements for standing at this stage of the proceedings. That is, his allegations establish that he has suffered and is in immediate danger of suffering a direct injury because of the data breach. The trial court erred by requiring allegations of actual misuse of Hensley’s PII. Under the circumstances of this case, Hensley should not have to wait until hackers commit identity theft, fraud, or other misuse to obtain standing.⁴

³ Recently, in a data breach case, another panel of this court found standing based solely on the plaintiff’s allegation that he had incurred out-of-pocket costs to mitigate his risk of identity theft. *McLinden v. Tangoe U.S., Inc.*, No. 24A-PL-1617, 2025 WL 1584889, at *3 (Ind. Ct. App. June 5, 2025).

⁴ LBB asserts that federal courts following *TransUnion LLC v. Ramirez*, 594 U.S. 413 (2021), have found “overwhelmingly that a plaintiff in a data breach case must allege some misuse of data or fraud to establish harm.” *Appellee’s Brief* at 9-10. We, of course, are not bound by cases addressing federal principles of standing.

[18] Reversed and remanded.⁵

Brown, J. and Tavitas, J., concur.

ATTORNEYS FOR APPELLANT

Lynn A. Toops
Amina A. Thomas
Arend J. Abel
Indianapolis, Indiana

ATTORNEYS FOR APPELLEE

Steven S. Hoar
Evansville, Indiana

Richard M. Haggerty
Devon, Pennsylvania

See Schulz v. State, 731 N.E.2d 1041, 1044 (Ind. Ct. App. 2000), *trans. denied*; *see also Hoosier Contractors*, 212 N.E.3d at 1243-46 (Goff, J., concurring in judgment, joined by Rush, C.J.) (explaining why we should hesitate before following restrictive federal standing doctrine too far). Moreover, the federal authorities are not as overwhelmingly consistent on the requirement of misuse as LBB suggests. *See, e.g., Bohmak v. Marsh & McLennan Companies, Inc.*, 79 F.4th 276, 279 (2d Cir. 2023) (finding standing in data breach case even though there was no allegation of misuse of stolen PII); *Webster*, 2025 WL 560917 (same); *Krupa*, 2023 WL 143140 (same); *Stamat v. Grandizio Wilkins Little & Matthews, LLP*, 2022 WL 3919685, at *6 (D. Md. Aug. 31, 2022) (“Actual misuse of data, however, is not strictly required to establish standing in the data breach context.”). And some federal courts have recognized that *TransUnion* (not a data breach case) should not be read to apply outside of the context of standing analysis for statutory causes of action. *See, e.g., Green-Cooper v. Brinker Int’l, Inc.*, 73 F.4th 883, 890 (11th Cir. 2023) (“*TransUnion* established that a common-law analogue analysis is required when plaintiffs allege a statutory violation.... But we think that the common-law analogue analysis is sui generis to legislature-made statutory violations because the Supreme Court has not applied it to any other kind of intangible harm.”), *cert. denied*, 144 S. Ct. 1457 (2024); *Krupa*, 2023 WL 143140, at *5 n.4 (“The Court reads *TransUnion* to affect standing analysis only for statutory causes of action.”).

⁵ While this appeal was pending, a federal court addressing the same LBB data breach at issue here, but with a different putative class, found that the plaintiffs have standing to pursue claims for damages based on their alleged injuries of invasion of privacy and mitigation expenses. *See Duffy v. Lewis Bros. Bakeries, Inc.*, 760 F. Supp. 3d 704, 718 (S.D. Ind. 2024) (“In short, Plaintiffs allege actual and concrete harms by alleging loss of privacy and mitigation costs commensurate with the substantial risk of identity theft and fraud, which are traceable to the Data Breach that Defendant failed to prevent, and redressable by this Court.”).