

The Intangible Concrete Injury: A 2024 Update of Post-*TransUnion* Decisions on Standing for Data Breach Class Actions

WRITTEN BY

Deanna Markowitz Willson

Jurisprudence on Article III standing requires a plaintiff to demonstrate an injury in fact, which must be both (1) concrete and (2) actual **or** imminent.^[1] For a plaintiff seeking redress in a data breach case, sufficiently pleading and proving the “injury in fact” standing requirement often proved elusive. Although a framework has developed relating to these elements, the application of this framework has yet to yield consistent results.

This article focuses on the element of concreteness. Subsequent articles will provide additional analysis on the element of actual or imminent injury as well as other considerations concerning pursuing claims in response to a data breach.

In 2021, two key decisions provided guidance on the concrete and actual or imminent elements in the data breach context.^[2] First, in *TransUnion v. Ramirez*, the Supreme Court held that an intangible injury can be concrete, but only if the asserted harm has a “close relationship” to a harm “traditionally” recognized as providing a basis for a lawsuit in American courts.^[3] Second, in *McMorris v. Carlos Lopez & Assocs.*, the Second Circuit outlined factors to be considered when evaluating whether an alleged future harm is imminent enough to confer standing.^[4] Unfortunately, in the two-and-a-half years since, the courts have not uniformly applied and interpreted the various factors and considerations outlined in *TransUnion* and *McMorris*. The question still remains: after a data breach, who has an injury in fact?

The Requirement to Show a Concrete Injury – Tangible or Intangible

To have Article III standing to sue in federal court, a plaintiff must show, among other things, that they suffered concrete injury in fact.^[5] The *TransUnion* Court confirmed that the concreteness requirement must be met for a plaintiff claiming injury by a defendant’s statutory violation, which was FCRA in the *TransUnion* case.^[6] Establishing that an alleged harm is concrete is relatively easy when the plaintiff claims a tangible harm such as the typical allegation of suffering a physical injury or economic loss.^[7] Examples of tangible harms that satisfy the concrete injury requirement for data breach cases include the need to pay for a credit-monitoring service^[8] and loss of access to a credit card for even a few days.^[9] The assertion of an intangible injury by a plaintiff is more complicated.

If the core injury is intangible, unlike the more common physical or monetary tangible harms, there needs to be a close common-law analog to the injury alleged.^[10] Indeed, the evaluation for whether the intangible harm is a concrete harm for standing purposes centers on “whether the alleged injury to the plaintiff has a ‘close

relationship' to a harm 'traditionally' recognized as providing a basis for a lawsuit in American courts."^[11] The Supreme Court acknowledged in *TransUnion* that "public disclosure of private information" is "traditionally recognized as providing a basis for lawsuits in American courts."^[12] Relying on *TransUnion*, the Second and Third Circuits have held that exposure of a plaintiff's personally identifiable information to unauthorized third parties, due to hacks of their employer, was sufficiently analogous to the common-law claim of public disclosure of private facts.^[13] Accordingly, the plaintiffs in those cases satisfied the requirement of alleging a concrete, intangible harm.

The analogous common law claim employed in data breach cases for the concreteness element is frequently, but not always,^[14] public disclosure of private information. However, the standard to establish that the common law claim is analogous varies widely among cases. The standard varies even within cases evaluating the same analogous common law claim. In addition, when drawing an analog to the common law claim of public disclosure of private information, there is a secondary focus as it pertains to the "public disclosure" aspect. For both, there is no consensus regarding what is required to satisfy the intangible harm requirement for standing.

1. Pleading of the Analogous Common Law Claim

Three Circuit decisions exhibit the varying requirements courts have applied when determining whether a plaintiff has articulated a concrete injury under an analogous common law claim. Although each analysis, like nearly everything with standing, is fact-specific, there is a distinct difference for a plaintiff to establish a concrete, intangible injury under these different holdings.

- Second Circuit: The plaintiff does not need to assert the analogous common law claim nor does the state law need to even recognize that particular common law claim.^[15]
- Seventh Circuit: The plaintiff's alleged harm was not closely related to the common law claim because his allegations were "missing an element essential to liability."^[16]
- Tenth Circuit: The plaintiff does not have to "plead and prove the tort's elements to prevail. But to proceed, she had to at least allege a similar harm."^[17]

2. Factual Requirements for Public Disclosure

The Circuit courts are also not uniform regarding the extent of the analogous disclosure necessary for the "public disclosure of private information" common law claim to be deemed sufficiently analogous.

On the one hand, many courts do not struggle to determine that an allegation of unauthorized disclosure pursuant to a data breach is satisfactorily analogous to public disclosure of private information. When there was actual "exposure of personally identifying information" on the dark web, the plaintiff's alleged harm was sufficiently concrete and easily analogous to the tort of public disclosure.^[18] Yet, the Second Circuit has affirmatively held that the private information does not need to be published or publicly available for the tort to be analogous. The *Bohnack* Court (2023) found that a third-party obtaining private information in a targeted hack is close enough to "public disclosure," even if such information was not published.^[19] The *Salazar* Court (2024) went further and held that intentional disclosure to a third-party by the defendant, although the defendant did not inform the plaintiff that such disclosure was occurring, was a sufficiently analogous public disclosure.^[20]

Conversely, in factually similar cases, the Third (2024) and Tenth (2022) Circuits also held that "[w]hen the communication of personal information only occurs between a debt collector and an intermediary tasked with

contacting the consumer, the consumer has not suffered the kind of privacy harm traditionally associated with public disclosure.”^[21] More generally, the Seventh Circuit (2023) held that without the publication of private information, a plaintiff has not suffered an injury similar to the public disclosure tort.^[22] This was echoed in a Florida district court opinion (2022) that denied standing because “Plaintiffs fail to allege that Defendant or the hacker(s) communicated their private information to the public at large.”^[23]

The interpretation that requires publicization to meet the “analogous common law claim” requirement for intangible injuries seems to negate the fact that the next element of the “injury in fact” analysis permits an injury to be imminent rather than have actually occurred. The evaluation of the second element (actual or imminent) for establishing an injury in fact for standing will be assessed in depth in the next article.

[1] *Thole v. U.S. Bank N.A.*, 590 U.S. 538, 140 S. Ct. 1615, 1618, 207 L.Ed.2d 85 (2020). There is a third requirement: the injury must be particularized, which is not typically in dispute for these decisions. To “satisfy the particularity requirement” an injury must be “distinct from the body politic”. *Strubel v. Comenity Bank*, 842 F.3d 181,

188 (2d Cir. 2016). But when a plaintiff in a data breach case specifically alleges that the plaintiff’s personal information was compromised during a data breach that

impacted a finite number of people, the injury will always be “distinct from the body politic.”

[2] See our prior articles on *TransUnion* and standing in data breach cases [here](#) and [here](#).

[3] *TransUnion LLC v. Ramirez*, 594 U.S. 413, 417, 141 S. Ct. 2190, 2200, 210 L. Ed. 2d 568 (2021) (providing examples of concrete injuries: “such as physical harm, monetary harm, or various intangible harms including (as relevant here) reputational harm”).

[4] *McMorris v. Carlos Lopez & Assocs.*, 995 F.3d 295, 301-03 (2d Cir. 2021).

[5] *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560–561, 112 S.Ct. 2130, 2136 -37, 119 L.Ed.2d 351.

[6] *TransUnion*, 594 U.S. at 427 (“Only those plaintiffs who have been concretely harmed by a defendant’s statutory violation may sue that private defendant over that violation in federal court.”); see also *Bohnak v. Marsh & McLennan Companies, Inc.*, 79 F.4th 276, 283 (2d Cir. 2023) (explaining that “*TransUnion* is the touchstone for”

assessing the concreteness requirement).

[7] See *TransUnion*, 594 U.S. at 425 (“If a defendant has caused physical or monetary injury to the plaintiff, the plaintiff has suffered a concrete injury in fact under Article III.”).

[8] *Baysal v. Midvale Indem. Co.*, 78 F.4th 976, 977 (7th Cir. 2023), reh’g denied, No. 22-1892, 2023 WL 6144390 (7th Cir. Sept. 20, 2023) (referencing *Remijas v. Neiman Marcus Group, LLC*, 794 F.3d 688 (7th Cir. 2015)).

[9] *Id.*

[10] See, e.g., *Spokeo, Inc. v. Robins*, 578 U.S. 330, 340-41, 136 S.Ct. 1540, 1549, 194 L.Ed.2d 635 (2016).

[11] *Packer on behalf of 1-800-Flowers.Com, Inc. v. Raging Capital Management, LLC*, 105 F.4th 46, 51 (2d Cir. 2024) (quoting *TransUnion*, 594 U.S. at 424, 141 S.Ct. 2190).

[12] *TransUnion*, 594 U.S. at 425.

[13] *Bohnak*, 79 F.4th at 285 (holding: "The core of the injury Bohnak alleges here is that she has been harmed by the exposure of her private information—including her SSN and other PII—to an unauthorized malevolent actor. This falls squarely within the scope of an intangible harm the Supreme Court has recognized as 'concrete.'"); See also *Clemens v. ExecuPharm Inc.*, 48 F.4th 146, 155 n.5 (3d Cir. 2022) ("we are content for now that the exposure of the type of information that was alleged here—information employees would normally choose to keep to themselves and would reasonably not want to make publicly available—and the resulting substantial risk of

identity theft or fraud is a harm that bears at least a "close relationship" to harms traditionally recognized in privacy torts. Accordingly, the asserted injury supports Article III

standing—and whether a plaintiff has successfully made out claims under a particular cause of action is a separate question.") (internal citations omitted).

[14] For example, unlawful collection and disclosure of biometric information as equivalent to the tort of trespass. *Cothron v. White Castle System, Inc.*, 20 F.4th 1156, 1161 (7th Cir. 2021). Note, this case also held that some other violations of the Illinois Biometric Privacy Act are not actionable in federal court because the injury is neither concrete nor similar to a tort.

[15] *Bohnak*, 79 F.4th at 286:

We recognize that Bohnak does not in this case assert a common law claim for public disclosure of private facts, and it matters not whether New York common law recognizes a tort relating to publication of private facts. For the purposes of the "concreteness" analysis under *TransUnion*, what matters is that the intangible harm arising

from disclosure of one's PII bears a relationship to an injury with a "close historical or common-law analogue." And that analog need not be "an exact duplicate." (internal citations omitted).

The Second Circuit has also affirmatively held that not every element of the analogous common law claim needs to be plead. *Salazar v. Nat'l Basketball Ass'n*, 118 F.4th 533, 553 n.6 (2d Cir. 2024) ("We did not, in any of those cases, hold that *TransUnion* demands that a plaintiff adequately plead every element of a common-law analog to satisfy the concreteness requirement.")

[16] *Hunstein v. Preferred Collection and Management Services, Inc.*, 48 F.4th 1236, 1242 (11th Cir. 2022) (en banc).

[17] *Shields v. Professional Bureau of Collections of Maryland, Inc.*, 55 F.4th 823, 829 (10th Cir. 2022); see also *Barclift v. Keystone Credit Services, LLC*, 93 F.4th 136, 145 (3d Cir. 2024) ("We believe that if the Court wanted us to compare elements, it would have simply said so. So when asking whether a plaintiff's intangible injury is 'concrete,' we will examine the kind of harm at issue.").

[18] *Clemens v. ExecuPharm Inc.*, 48 F.4th 146, 155 (3d Cir. 2022).

[19] *Bohnak*, 79 F.4th at 286.

[20] *Salazar*, 118 F.4th at 544 (“Given the nature of the companies involved, intended and potential uses of the disclosed information, and resulting enhanced disclosure risks, we see little daylight between the nature of the harm Salazar alleges and the harm flowing from the public disclosure of private facts common-law analog.”).

[21] *Barclift*, , 93 F.4th at 146.; *Hunstein*, 48 F.4th at 1245; *Shields* , 55 F.4th at 829. (.

[22] *Nabozny v. Optio Sols. LLC*, 84 F.4th 731, 736 (7th Cir. 2023).

[23] See *Baron v. Syniverse Corp.*, 8:21-cv-2349-SCB-SPF, 2022 WL 6162696, *6 (M.D. Fla. Oct. 7, 2022).

RELATED INDUSTRIES + PRACTICES

- Privacy + Cyber