Data Breach Standing: How Plaintiffs May Find Their Footing After *TransUnion v. Ramirez*

CHRISTOPHER M. DEUCHER*

TABLE OF CONTENTS

I. INTRODUCTION 37
II. STANDING IN DATA BREACH CASES: THE PRE-*TRANSUNION* CIRCUIT SPLIT 39
A. *Six Circuits Recognize Data Breach Standing Due to the Risk of Future Harm* 40
B. *Four Circuits Consider Data Breaches, Alone, Insufficient for Standing* 41
III. *TRANSUNION*: A NEW LOOK AT FUTURE-HARM STANDING 42
IV. WAYS TO SHORE UP DATA BREACH STANDING NOTWITHSTANDING *TRANSUNION* 44
A. *The Further Narrowing of Risk of Future Harm Standing* 45
B. *Navigating the Post-*TransUnion *"Closely Related to Traditional Harm" Test* 49
C. TransUnion*'s Narrowing of Statutorily-Derived Standing* 51
V. CONCLUSION 52

I. INTRODUCTION

Imagine the following scenario: a hacker breaks into a large company's database and accesses its customers' private information including names, addresses, credit card numbers, and dates of birth. Almost undoubtedly, such a breach would set in motion a nightmare for the company's customers. As a result, customers initiate a class action lawsuit against the company for failing to sufficiently protect their private information. No fraud or identity theft has resulted from the data breach *yet*. Nevertheless, the plaintiffs assert that they have been harmed by the increased risk of future harm caused by the breach.

In our increasingly digital world, this scenario is far from unique. The phrase "data breaches" likely brings several headlines-making examples to mind, and they are only becoming more prevalent.[1] Yet, as this Note sets out,

* Note Editor, *Ohio State Law Journal*; J.D. Candidate, The Ohio State University Moritz College of Law, 2023. Thank you to my family for their support and encouragement. I would also like to thank Professor Margaret Kwoka and the *OSLJ Online* team. All errors are my own.

[1] Chris Morris, *Data Breaches Continue to Skyrocket in 2022*, NASDAQ (May 19, 2022), https://www.nasdaq.com/articles/data-breaches-continue-to-skyrocket-in-2022 [https://perma.cc/7KGB-SURW].

somewhat shockingly, data breach standing is no trivial matter.[2] A tricky question often arises: whether the breach itself constitutes a risk of future harm sufficient to demonstrate a concrete injury-in-fact. There is no "clear consensus" among courts considering this question.[3] Six circuits have held that the risk of future harm, alone, from a data breach is sufficient for standing while four have refused to do so.[4] This inconsistency stems from hazy Supreme Court guidance,[5] the unique facts of data breach cases,[6] and—most importantly—disagreement as to whether the risk of future harm from a breach is too speculative.[7]

Then came the Supreme Court's *TransUnion v. Ramirez* decision.[8] This case dealt three significant blows to data breach plaintiffs. First, *TransUnion* held that the risk of future harm, by itself, is insufficient for standing when seeking damages.[9] Second, it circumscribed *Spokeo*'s "close relationship" test—a test that could have been a promising avenue for data breach plaintiffs to assert standing.[10] Third, it confirmed that the Court will not recognize a congressionally-granted right of action in the absence of plaintiffs suffering a concrete injury.[11]

To be sure, *TransUnion* does not wholly resolve the circuit split because, in contrast to typical data breach cases, a portion of the plaintiffs' credit reports never left the TransUnion database.[12] Accordingly, future data breach plaintiffs will attempt to differentiate their risk of future harm as less speculative and a better fit with common law analogues than the harm suffered in *TransUnion*. However, data breach defendants will indubitably argue for courts to broadly apply *TransUnion*'s harm analysis to the data breach context. If defendants successfully convince courts to do so, data breach plaintiffs' prospects for standing will be on much shakier footing.

This Note discusses how data breach defendants and plaintiffs may navigate the post-*TransUnion* world of standing. It proceeds in five parts. Part II describes the pre-*TransUnion* circuit split on data breach standing. Part III examines *TransUnion*. Part IV explores the likely application of *TransUnion* in

---

[2] A recent empirical study found that among 16,773 cyber-related cases at least 2,223 were dismissed due to lack of standing. *See* Jay P. Kesan & Linfeng Zhang, *When Is a Cyber Incident Likely to Be Litigated and How Much Will It Cost? An Empirical Study*, 27 CONN. INS. L.J. 529, 565 (2021).

[3] Lee J. Plave & John W. Edison, *First Steps in Data Privacy Cases: Article III Standing*, 37 FRANCHISE L.J. 485, 487 (2018).

[4] *See infra* Sections II.A and II.B.

[5] *See infra* notes 28–29 and accompanying text.

[6] *See infra* notes 42–43 and accompanying text.

[7] *Compare* Attias v. Carefirst, Inc., 865 F.3d 620, 629 (D.C. Cir. 2017), *with* In re SuperValu, Inc., 870 F.3d 763, 770 (8th Cir. 2017).

[8] TransUnion LLC v. Ramirez, 141 S. Ct. 2190 (2021).

[9] *Id.* at 2213.

[10] *Id.* at 2204.

[11] *Id.* at 2204–05.

[12] *Id.* at 2200.

the data breach context and addresses how plaintiffs and defendants, respectively, can embrace it as either a sword or shield. Lastly, Part V concludes.

II. STANDING IN DATA BREACH CASES: THE PRE-*TRANSUNION* CIRCUIT SPLIT

Prior to *TransUnion*, federal courts consistently relied upon two Supreme Court cases to guide their inquiry into the thorny question of data breach standing.[13] The first case they relied upon is *Clapper v. Amnesty International*.[14] In that 2013 case, plaintiffs challenged the constitutionality of a section of the Foreign Intelligence Surveillance Act.[15] Attempting to demonstrate standing, the plaintiffs alleged that their communications with clients would likely be surveilled.[16] The Court reiterated that "threatened injury must be *certainly impending* to constitute injury in fact" and "'[a]llegations of *possible* future injury' are not sufficient."[17] The Court ultimately rejected plaintiffs' standing argument because it was built upon a "highly attenuated chain of possibilities."[18] Furthermore, the Court held that the plaintiffs' mitigation costs—like traveling to meet with their clients overseas—failed to provide a basis for standing because the underlying harm was not certainly impending.[19] Naturally, because the risk of future harm plays a central role in data breach standing, this standard of "certainly impending" harm has informed circuit courts' analysis.

The second Supreme Court case often cited is *Spokeo Inc. v. Robins*.[20] Like *TransUnion*, *Spokeo* dealt with the Fair Credit Reporting Act.[21] The plaintiff sued Spokeo—a company which essentially provided a "people search engine" service—for disseminating incorrect information about him.[22] The Supreme Court remanded the case because the Ninth Circuit had wholly ignored the "independent requirement" that an injury in fact must be "concrete."[23] Consequently, circuit courts gathered two key takeaways from *Spokeo*: the

---

[13] *See* R. Andrew Grindstaff, *Article III Standing, The Sword and the Shield: Resolving a Circuit Split in Favor of Data Breach Plaintiffs*, 29 WM. & MARY BILL RTS. J. 851, 860 (2021).

[14] Clapper v. Amnesty Int'l USA, 568 U.S. 398, 401 (2013); *see also* Grayson Wells, Comment, *What's the Harm? Federalism, the Separation of Powers, and Standing in Data Breach Litigation*, 96 IND. L.J. 937, 953 (2021).

[15] *Clapper*, 568 U.S. at 401.

[16] *Id.* at 406.

[17] *Id.* at 409 (citing Whitmore v. Arkansas, 495 U.S. 149, 158 (1990)).

[18] *Id.* at 410.

[19] *Id.* at 415–17.

[20] Spokeo, Inc. v. Robins, 578 U.S. 330 (2016); *see* Ewing v. MED-1 Solutions, LLC, 24 F.4th 1146, 1151 (7th Cir. 2022).

[21] *Spokeo*, 578 U.S. at 333; TransUnion LLC v. Ramirez, 141 S. Ct. 2190, 2200 (2021).

[22] *Spokeo*, 578 U.S. at 333–34.

[23] *Id.* at 339, 342–43.

concreteness of the harm must be independently analyzed,[24] and risk of future harm can *sometimes* fulfill the concreteness requirement.[25]

Taking these cases together, future harm may demonstrate standing if it is "certainly impending" *or* if there is "substantial risk that the harm will occur."[26] Despite this instruction, *Spokeo* and *Clapper* have left data breach plaintiffs in an uncertain litigating position and the federal judiciary with a conspicuous circuit split.[27] The high-level analysis in *Spokeo* provided little guidance.[28] Justice Samuel Alito described this uncertainty best when he commented, during *TransUnion*'s oral argument, "*Spokeo*'s discussion of harm is quite clipped, and it's potentially subject to different interpretations."[29]

A. *Six Circuits Recognize Data Breach Standing Due to the Risk of Future Harm*

The Second, Sixth, Seventh, Ninth, Eleventh, and D.C. Circuits have held that data breach plaintiffs have standing under the risk of future harm theory.[30] Consider, first, the Seventh Circuit. In *Lewert v. P.F. Chang's China Bistro*, it held that stolen data—even if not yet used by the hacker—constitute future harm risks that are "concrete enough to support a lawsuit."[31] The Seventh Circuit relied upon its reasoning from a case just one year prior in which it found "the increased risk of fraudulent credit- or debit-card charges[] and the increased risk of identity theft" to be "certainly impending" and, therefore, sufficient for standing.[32]

Similarly, the D.C. Circuit, in *Attias v. Carefirst, Inc.*, used a two-pronged test to determine whether an "increased-risk-of-harm" claim had standing: (1) is the "ultimate alleged harm . . . concrete and particularized" and (2) whether

---

[24] *Id.*

[25] *Id.* at 341.

[26] Susan B. Anthony List v. Driehaus, 573 U.S. 149, 158 (2014) (quoting Clapper v. Amnesty Int'l USA, 568 U.S. 398, 409, 414 n.5 (2013)).

[27] *See* Richard Pierce, Notice and Comment, *Standing Law Is Inconsistent and Incoherent*, YALE J. ON REG. (Sept. 7, 2021), https://www.yalejreg.com/nc/standing-law-is-inconsistent-and-incoherent/ [https://perma.cc/VV9P-5V3T].

[28] *See* Ido Kilovaty*, Psychological Data Breach Harms*, 23 N.C. J.L. & TECH. 1, 10 (2021).

[29] Oral Argument at 44:30, TransUnion v. Ramirez, LLC, 141 S. Ct. 2190 (2021) (No. 20-297), https://www.oyez.org/cases/2020/20-297 [https://perma.cc/H54R-PAKU].

[30] *See* McMorris v. Carlos Lopez & Assocs., LLC, 995 F.3d 295, 300–01 (2d Cir. 2021); Attias v. Carefirst, Inc., 865 F.3d 620, 629 (D.C. Cir. 2017); Galaria v. Nationwide Mut. Ins. Co., 663 F. App'x 384, 387–89 (6th Cir. 2016); Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 692, 694–96 (7th Cir. 2015); Krottner v. Starbucks Corp., 628 F.3d 1139, 1142–43 (9th Cir. 2010); In re Equifax Inc. Customer Data Sec. Breach Litig., 999 F.3d 1247, 1262 (11th Cir. 2021).

[31] Lewert v. P.F. Chang's China Bistro, Inc., 819 F.3d 963, 967 (7th Cir. 2016).

[32] *Id.* at 966 (citing Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 691–94 (7th Cir. 2015)).

the "increased risk of such harm makes injury to an individual citizen sufficiently 'imminent.'"[33] The court ultimately held that the data breach plaintiffs had demonstrated standing in *Attias* because, unlike in *Clapper*, there was no "highly attenuated chain of possibilities."[34] Rather, the hackers had obtained the sensitive information and had "both the intent and the ability to use that data for ill," so the risk of future harm was sufficiently concrete and imminent.[35]

B. *Four Circuits Consider Data Breaches, Alone, Insufficient for Standing*

The First, Third, Fourth, and Eighth Circuits, on the other hand, have denied data breach plaintiffs' theory of future harm.[36] *In re SuperValu, Inc.* is illustrative.[37] In that case, the Eighth Circuit held that the risk of identity theft was too "speculative" to demonstrate standing.[38] Interestingly, the statistical likelihood of future identity theft from data breaches did not convince the court that the future harm was "certainly impending" or a substantial risk.[39] The Fourth Circuit employed similar reasoning when it held that plaintiffs' claim that one in three of those affected by a data breach would experience identity theft fell "far short of" a showing of "substantial risk" of future harm.[40]

* * *

As the Second Circuit recently observed, "no court of appeals has *explicitly* foreclosed plaintiffs from establishing standing based on a risk of future identity theft—even those courts that have declined to find standing on the facts of a particular case."[41] Instead, the specific facts of a case often determine whether plaintiffs have standing.[42] Certain types of stolen information are more likely to trigger future harms than others, so, naturally, some cases will have a greater

---

[33] *Attias*, 865 F.3d at 627 (quoting Food & Water Watch, Inc. v. Vilsack, 808 F.3d 905, 915 (D.C. Cir. 2015)).

[34] *Id.* at 626, 629 (quoting Clapper v. Amnesty Int'l USA, 568 U.S. 398, 410 (2013)).

[35] *See id.* at 628–29.

[36] *See* Katz v. Pershing, LLC, 672 F.3d 64, 79–80 (1st Cir. 2012); Reilly v. Ceridian Corp., 664 F.3d 38, 42–44 (3d Cir. 2011); Beck v. McDonald, 848 F.3d 262, 273–76 (4th Cir. 2017); In re SuperValu, Inc., 870 F.3d 763, 770–72 (8th Cir. 2017).

[37] In re SuperValu, Inc., 870 F.3d 763 (8th Cir. 2017).

[38] *Id.* at 770.

[39] *Id.* at 771 (explaining that because "the report finds that data breaches are unlikely to result in account fraud" and that "most breaches have not resulted in detected incidents of identity theft," the plaintiffs do not have standing (quoting U.S. GOV'T ACCOUNTABILITY OFF., GAO-07-737, PERSONAL INFORMATION: DATA BREACHES ARE FREQUENT, BUT EVIDENCE OF RESULTING IDENTITY THEFT IS LIMITED; HOWEVER, THE FULL EXTENT IS UNKNOWN 21 (2007)).

[40] Beck v. McDonald, 848 F.3d 262, 276 (4th Cir. 2017).

[41] McMorris v. Carlos Lopez & Assocs., LLC, 995 F.3d 295, 300 (2d Cir. 2021) (emphasis added).

[42] *See id.* at 302; *In re SuperValu, Inc.*, 870 F.3d at 769.

risk of future harm.[43] Furthermore, because the "extent to which data breaches result in identity theft is not well known," uncertainty muddles the risk analysis of future harms.[44]

III. *TRANSUNION*: A NEW LOOK AT FUTURE-HARM STANDING

The Supreme Court, in *TransUnion v. Ramirez*, set out a comprehensive standing analysis. But before discussing the Court's analysis, a brief recounting of the facts is in order. Sergio Ramirez, along with a class of over 8,000 others, sued TransUnion for incorrectly listing them as potential matches on a terrorist list.[45] While 1,853 class members were directly affected by this false positive match because this information was sent to a third party, 6,332 class members' inaccurate credit information was never sent to a third party.[46] The Court focused upon this latter group: Did the plaintiffs whose credit reports inaccurately flagged them as potential terrorists demonstrate standing if such reports were never disclosed to a third party?[47] A majority of the Justices said no.[48]

TransUnion—like the majority of data breach cases—hinges upon the "concrete" injury requirement of standing.[49] The Court begins and ends with the succinct phrase: "No concrete harm, no standing."[50] Between these two bookends, the Court elucidates how courts should determine concreteness. The concreteness analysis for the 6,332 class members whose inaccurate information was *not* sent to third parties proved demanding.[51] Justice Kavanaugh, citing Judge David Tatel of the D.C. Circuit, analogized the situation to a common philosophical quip: "'[I]f inaccurate information falls into' a consumer's credit file, 'does it make a sound?'"[52] Without employing metaphysical reasoning, the Court answered in the negative.[53] As Justice Kavanaugh explained, the mere presence of inaccurate information in an unshared file is not *close enough* to the

---

[43] *See* Kamal v. J. Crew Grp., Inc., 918 F.3d 102, 116 (3d Cir. 2019) (considering whether the stolen data include enough information to likely enable identity theft).

[44] *In re SuperValu, Inc.*, 870 F.3d at 771 (quoting U.S. GOV'T ACCOUNTABILITY OFF., *supra* note 39, at 5).

[45] TransUnion, LLC v. Ramirez, 141 S. Ct. 2190, 2200–01 (2021). The class sued under the Fair Credit Reporting Act, which requires credit reporting agencies to, inter alia, "follow reasonable procedures to assure maximum possible accuracy" in customers' credit reports. *Id.* (quoting 15 U.S.C. § 1681e(b)).

[46] *Id.* at 2200.

[47] *See id.*

[48] *Id.*

[49] *Id.* at 2200, 2203.

[50] *Id.* at 2200, 2214.

[51] *See TransUnion*, 141 S. Ct. at 2209–12. The Court was split 5–4. *Id.* at 2199.

[52] *Id.* at 2209 (citing Owner-Operator Indep. Drivers Ass'n, Inc. v. U.S. Dep't of Transp., 879 F.3d 339, 344 (D.C. Cir. 2018)).

[53] *Id.* at 2209–12.

traditionally-recognized harm of defamation.[54] Publication is necessary for a defamation-related harm to become concrete.[55] Without publication, Justice Kavanaugh compared the harm alleged by this subset of plaintiffs to the "harm" from "[an insulting] letter that is not sent."[56] Justice Kavanaugh restricted this test's flexibility: "*Spokeo* is not an open-ended invitation for federal courts to loosen Article III based on contemporary, evolving beliefs about what kinds of suits should be heard in federal courts."[57] Therefore, a majority of the Court does not appear to have the appetite to reshape standing doctrine in light of a changing society.[58]

After dismissing the closely-related argument, the Court proceeded to the plaintiffs' second argument—the risk of future harms.[59] The 6,332 plaintiffs asserted that the inaccurate information in TransUnion's database significantly increased the risk that inaccurate information would be disseminated when requested by a third party.[60] After all, TransUnion was not collecting this information and matching it to the Office of Foreign Assets Control (OFAC) list for its own exclusive use.[61] Plaintiffs found support for this argument in *Spokeo*, which stated that "the risk of real harm" may sometimes "satisfy the requirement of concreteness."[62] The Court rejected the plaintiffs' appeal to *Spokeo*.[63] In Justice Kavanaugh's words, the "6,332 plaintiffs did not demonstrate that the risk of future harm *materialized*," so the harm was not concrete.[64]

This rejection of future harm signals a noteworthy shift in standing doctrine. While *Spokeo* preserved the opportunity of a risk of future harm being concrete,[65] *TransUnion* appears to have all but shut that door.[66] Justice Clarence Thomas, dissenting in *TransUnion*, emphasized the majority's pivot: "The majority . . . all but eliminat[es] the risk-of-harm analysis."[67] To be sure, the majority explained that the risk of future harm may still be used for injunctive

---

[54] *Id.* at 2210.
[55] *Id.* at 2211.
[56] *TransUnion*, 141 S. Ct. at 2210.
[57] *Id.* at 2204.
[58] *See id.*
[59] *Id.* at 2210.
[60] *Id.*
[61] *See id.* at 2201.
[62] *TransUnion*, 141 S. Ct. at 2210 (quoting Spokeo Inc. v. Robins, 578 U.S. 330, 341–42 (2016)).
[63] *Id.* at 2210–12.
[64] *Id.* at 2211 (emphasis added). The majority essentially adopted a "wait and see" approach in which damages can only be awarded if the risk actually causes harm.
[65] *See Spokeo*, 578 U.S. at 341 (citing Clapper v. Amnesty Int'l USA, 568 U.S. 398 (2013)) ("This does not mean, however, that the risk of real harm cannot satisfy the requirement of concreteness.").
[66] *See TransUnion*, 141 S. Ct. at 2222 (Thomas, J., dissenting).
[67] *Id.*

relief, but it explicitly discontinued using risk of harm to justify a damages award.[68]

The Court rejected the 6,332 plaintiffs' future harm argument for another reason—the risk of future harm was "too speculative."[69] Adopting the reasoning of Judge Margaret McKeown of the Ninth Circuit, the Supreme Court held that this subset of plaintiffs failed to show "sufficient likelihood" that their information would be passed along to a third party.[70] However, this is a questionable assumption. As Justice Elena Kagan pointed out in her dissent, TransUnion is a company "in the business of selling credit reports."[71] Thus, it seems reasonable to expect TransUnion to provide such reports to third parties in line with their business plan.[72]

Lastly, while the Fair Credit Reporting Act includes a statutory carveout for consumers to sue reporting agencies for violating the Act,[73] the Court was unpersuaded.[74] Justice Kavanaugh—building upon precedent[75]—reasoned that Congress' view on standing can be "instructive," but Congress "may not simply enact an injury into existence."[76] At the end of the day, the courts have the "responsibility to independently decide whether a plaintiff has suffered a concrete harm under Article III . . . ."[77] Put another way, *TransUnion* clarified that standing requires a concrete injury and that "an injury in law is not an injury in fact."[78]

IV. WAYS TO SHORE UP DATA BREACH STANDING NOTWITHSTANDING *TRANSUNION*

As a monumental case for federal standing doctrine, *TransUnion* will likely affect data breach standing in three significant ways. First, *TransUnion* essentially held that the risk of future harm alone is not "concrete" for purposes of seeking damages.[79] Second, it seemingly restricted the expanse of *Spokeo*'s "close relationship" test.[80] Third, it affirmed that the Court will not enforce statutorily-derived standing for plaintiffs whose stolen data have not yet been concretely used for a harmful purpose.[81] Each of these principles, if interpreted

---

[68] *Id.* at 2210–13 (majority opinion).
[69] *Id.* at 2212.
[70] *Id.* (citing Ramirez v. TransUnion LLC, 951 F.3d 1008, 1040 (9th Cir. 2020)).
[71] *Id.* at 2225 (Kagan, J., dissenting).
[72] *TransUnion*, 141 S. Ct. at 2225.
[73] *Id.* at 2201 (majority opinion) (citing 15 U.S.C. § 1681n(a)).
[74] *Id.* at 2214.
[75] *See* Lujan v. Defenders of Wildlife, 504 U.S. 555, 560, 576 (1992).
[76] *TransUnion*, 141 S. Ct. at 2204–05 (citing Spokeo Inc. v. Robins, 578 U.S. 330, 341 (2016)); Hagy v. Demers & Adams, 882 F.3d 616, 622 (6th Cir. 2018)).
[77] *Id.* at 2205.
[78] *Id.*
[79] *Id.* at 2213–14.
[80] *See id.* at 2204.
[81] *See id.* at 2204–06.

by courts as such, will make it more difficult for data breach plaintiffs to bring suit if they only allege a risk of future harm.

Nevertheless, data breach plaintiffs may creatively employ a multitude of arguments that were not foreclosed by *TransUnion*. The following Parts apply *TransUnion* to the data breach context and suggest how plaintiffs can find their footing to demonstrate standing. First, in the risk of future harm realm, plaintiffs can distinguish the risk of harm stemming from data breaches as less speculative and less attenuated than the risk in *TransUnion*. Second, plaintiffs can often demonstrate independent harm irrespective of whether the hacker uses the data; emotional distress and mitigation costs top this list. Third, while *TransUnion* narrows the possibility of plaintiffs successfully using the "closely related" analogue test,[82] it does not foreclose it. Data breaches resemble the torts of intrusion upon seclusion and disclosure of private information.[83]

The Supreme Court, in *TransUnion*, further emphasized that standing must encompass a concrete harm in the real world—not merely any harm dreamt up by Congress.[84] Accordingly, any future favorable developments for plaintiffs will likely arise from the courts themselves. The three strategies enumerated above may persuade courts to hold open the courtroom doors for data breach plaintiffs despite *TransUnion*.

A. *The Further Narrowing of Risk of Future Harm Standing*

To recap, six circuits have held the risk of future harm alleged by data breach plaintiffs as sufficient to demonstrate standing.[85] Their reasoning relies on *Spokeo*, which opened the courtroom doors for such plaintiffs by emphasizing that risk of harm may be concrete in certain situations.[86] But *TransUnion* has effectively shut that door.[87] Justice Kavanaugh—writing for the majority—unequivocally stated that "the risk of future harm on its own does not support Article III standing for the plaintiffs' damages claim."[88]

Now, under a broad reading of *TransUnion*, data breach plaintiffs must show that their data were harmfully used to demonstrate standing.[89] In other words, data breach victims must wait and see if their stolen information is used

---

[82] *TransUnion*, 141 S. Ct. at 2204.

[83] *See infra* notes 129–31 and accompanying text.

[84] *TransUnion*, 141 S. Ct. at 2205 ("Congress . . . may not simply enact an injury into existence . . . .").

[85] *See supra* Part II.

[86] Spokeo Inc. v. Robins, 578 U.S. 330, 341 (2016).

[87] *See TransUnion*, 141 S. Ct. at 2222 (Thomas, J., dissenting).

[88] *TransUnion*, 141 S. Ct. at 2213 (majority opinion).

[89] Other legal commentators agree with this analysis. *See, e.g.*, Joshua Briones, Arameh Zargham O'Boyle & Matthew Novian, *Supreme Court Decision May Have Significant Implications for Data Breach and Privacy Class Actions*, SECURITY (July 2, 2021), https://www.securitymagazine.com/articles/95556-supreme-court-decision-may-have-significant-implications-for-data-breach-and-privacy-class-actions [https://perma.cc/W4TU-NTBB].

before suing in federal court.[90] Because—to borrow a phrase from Justice Thomas—*TransUnion* "all but eliminat[ed] the risk-of-harm analysis,"[91] data breach plaintiffs will now have a more challenging time demonstrating standing. Therefore, the six circuits, which have held that a data breach itself can sufficiently demonstrate standing, could reevaluate their approach.[92]

Still, *TransUnion* leaves a couple narrow pathways for data breach victims to demonstrate standing. Primarily, plaintiffs can argue that the type of risk is unique in the data breach context. While the risk of future harm associated with TransUnion disseminating the inaccurate credit reports to third parties was too speculative in the eyes of the Supreme Court,[93] the future harm of identity theft after a data breach is not. Risk is not binary but should be viewed as a matter of degree.[94] Data breach plaintiffs can accept that the *TransUnion* plaintiffs insufficiently demonstrated the likelihood that their incorrect credit reports would be provided to third parties without conceding their entire argument. After all, only one in four (25%) of the *TransUnion* class members had false flags sent to a third party.[95]

On the other hand, it is more likely that nefarious hackers will use the illegal fruits of their crime (i.e., plaintiffs' data) in a manner that harms the plaintiffs down the road.[96] As the Seventh Circuit succinctly put it, "Why else would hackers break into a store's database and steal consumers' private information?"[97] Statistics support the intuitive answer to this rhetorical question. According to national statistics, only 2.8% of individuals are victims of identity theft, but this number jumps to 31.7% among individuals whose personal information was stolen in a data breach.[98]

While this number is not much greater than the 25% risk in *TransUnion*,[99] data breach plaintiffs may still distinguish their risk as "substantial." First, there is evidence that identity theft, a frequent consequence of data breaches,[100] is

---

[90] *TransUnion*, 141 S. Ct. at 2211.

[91] *Id.* at 2222 (Thomas, J., dissenting).

[92] *See* Legg v. Leaders Life Ins. Co., 574 F.Supp.3d 985, 993 (W.D. Okla. 2021).

[93] *TransUnion*, 141 S. Ct. at 2212.

[94] Risk is defined as the "*possibility* of loss or injury" and "the *degree* of probability of such loss." *Risk*, MERRIAM-WEBSTER ONLINE DICTIONARY, https://www.merriam-webster.com/dictionary/risk [https://perma.cc/D9SX-J9HH] (emphasis added).

[95] *TransUnion*, 141 S. Ct. at 2222 (Thomas, J., dissenting).

[96] *See* Galaria v. Nationwide Mut. Ins. Co., 663 Fed. Appx. 384, 388 (6th Cir. 2016) ("[A] reasonable inference can be drawn that the hackers will use the victim's data for the fraudulent purposes . . . .").

[97] Remijas v. Neiman Marcus Grp., 794 F.3d 688, 693 (7th Cir. 2015).

[98] Matt Tatham, *Identity Theft Statistics*, EXPERIAN (Mar. 15, 2018), https://www.experian.com/blogs/ask-experian/identity-theft-statistics/ [https://tinyurl.com/bdp3keh3].

[99] *TransUnion*, 141 S. Ct. at 2225 (Kagan, J., dissenting).

[100] *See supra* note 98 and accompanying text.

chronically undercounted.[101] Therefore, plaintiffs can point out that statistics do not tell the full story of their risk. Second, there are fewer links in the causal chain in data breach cases than in *TransUnion*. Recall that TransUnion had inaccurately flagged all the plaintiffs as potential matches on its OFAC terrorist list.[102] For one of these false flags to end up in the hands of a third party, however, the third party *itself* must have requested the report.[103] This added another layer of attenuation in the causal chain—namely, the autonomy of a third party. In contrast, as the D.C. Circuit has pointed out, this extra layer of attenuation is absent in the data breach context because the hacker holds "both the intent and ability to use that data for ill."[104] Therefore, data breach plaintiffs are more likely to meet the *Clapper* standard of "certainly impending" injury because the chain of possibilities is less attenuated than in *TransUnion*.[105]

Admittedly, these arguments may not persuade courts in circuits traditionally unreceptive to future harm standing. The Fourth Circuit, in *Beck v. McDonald*, was unpersuaded by plaintiffs' evidence that 33% of data breaches of health information led to identity theft.[106] Nevertheless, the uniqueness of data breach risks may dissuade courts from applying *TransUnion* too broadly. While *TransUnion* will likely act as a one-way ratchet in favor of data breach defendants, plaintiffs can limit its unfavorable impact.

Defendants will likely counter that *TransUnion*'s holding regarding the speculative nature of future harm is quite instructive for data breach cases. Specifically, they will underscore that while TransUnion—the credit reporting agency—is "in the business of selling credit reports,"[107] this was insufficient to demonstrate that TransUnion would likely distribute the faulty reports. Defendants will draw a parallel to the data breach context: while hackers might be "in the business of" stealing data for their own use, this does not necessarily demonstrate a sufficient risk of future harm.

In response, data breach plaintiffs may also allege harms independent of the identity theft ever materializing. Just because the harm may become greater down the road due to identity theft, this does not erase the initial harm of the data breach. Because the Court in *TransUnion* held that "the risk of future harm *on its own* does not support . . . standing," other avenues remain open for data breach plaintiffs to demonstrate standing.[108] Specifically, Justice Kavanaugh elucidated that standing may be shown if the plaintiffs were "independently

---

[101] *See* CTR. FOR VICTIM RESEARCH, WHAT WE KNOW ABOUT IDENTITY THEFT AND FRAUD VICTIMS FROM RESEARCH- AND PRACTICE-BASED EVIDENCE 8 (Aug. 2019), https://justiceresearch.dspacedirect.org/server/api/core/bitstreams/fdc6b634-7d40-4ac2-adf7-101d75748a95/content [https://perma.cc/WG5Y-EJ9M].

[102] *See TransUnion*, 141 S. Ct. at 2200–01.

[103] *See id.*

[104] Attias v. Carefirst Inc., 865 F.3d 620, 628 (D.C. Cir. 2017).

[105] *See* Clapper v. Amnesty Int'l USA, 568 U.S. 398, 401 (2013).

[106] Beck v. McDonald, 848 F.3d 262, 275 (4th Cir. 2017).

[107] *TransUnion*, 141 S. Ct. at 2225 (Kagan, J. dissenting).

[108] *Id.* at 2213 (majority opinion) (emphasis added).

harmed by the exposure to the risk itself."[109] One common harm associated with perceived risks, as highlighted in *TransUnion*, is emotional distress.[110] Data breach victims frequently experience anxiety—an intangible yet concrete harm—due to the theft of their personal and sensitive information.[111] Such an emotional reaction should be expected; individuals often experience distress from identity theft,[112] and data breach victims are placed at a higher risk of identity theft.[113] The Supreme Court and circuit courts have confirmed that emotional distress can provide a basis for standing.[114]

There are other latent harms associated with data breaches that are concrete and independent of the data ever being used in a nefarious manner. If someone is notified that their credit card and other personal financial information is compromised, they will probably take mitigating actions. These prophylactic acts commonly include credit monitoring services, informing credit reporting agencies, and cancelling credit cards and other accounts.[115] In turn, these reasonable preventative acts are stressful and time-consuming. It makes sense that individuals would go to such lengths, however, because mitigation efforts likely dwarf the significant costs to rectify identity theft once fraudulent accounts are opened.[116]

There is backbone behind this cost of mitigation theory. In *Galaria v. Nationwide Mutual Ins. Co.*, for instance, the Sixth Circuit held that the plaintiffs' claims of "substantial risk of harm, coupled with reasonably incurred mitigation costs," demonstrated standing.[117] The court reasoned that once individuals realized their data had been breached, it would be "unreasonable" to

---

[109] *Id.* at 2211.

[110] *See id.*

[111] *See* Daniel J. Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data-Breach Harms*, 96 TEX. L. REV. 737, 772 (2018); Kilovaty, *supra* note 28, at 4–5.

[112] For a comprehensive analysis of the emotional distress experienced by identity theft victims, see ERIKA HARRELL, U.S. DEP'T OF JUSTICE, VICTIMS OF IDENTITY THEFT, 2018, at 11 (2021), https://bjs.ojp.gov/content/pub/pdf/vit18.pdf [https://perma.cc/N86T-NBBT] (showing that 8.4% of identity theft victims reported severe emotional distress, 22.9% reported moderate emotional distress, and 48.1% reported mild emotional distress).

[113] *See supra* note 98 and accompanying text.

[114] *See, e.g.*, Clemens v. ExecuPharm Inc., 48 F.4th 146, 155–56 (3d Cir. 2022) (explaining that, in light of *TransUnion*, "a [data breach] plaintiff suing for damages can satisfy concreteness as long as he alleges that the exposure to that substantial risk caused additional, currently felt concrete harms"); Doe v. Chao, 540 U.S. 614, 617–18 (2004) (holding that plaintiff had standing because he was "greatly concerned and worried" after his Social Security number was disclosed).

[115] *See* Hutton v. Nat'l Bd. of Exam'rs in Optometry, Inc. 892 F.3d 613, 622 (4th Cir. 2018).

[116] *See* HARRELL, U.S. DEP'T OF JUST., *supra* note 112, at 12 (explaining that while around 40% of identity theft victims resolved the opening of fraudulent accounts in one day or less, the other victims took anywhere from a week to more than six months to resolve the issue).

[117] Galaria v. Nationwide Mut. Ins. Co., 663 Fed. Appx. 384, 388 (6th Cir. 2016).

make them wait until confirmation of misuse before taking mitigation steps.[118] To be sure, the Sixth Circuit did not hold that standing was entirely brought about by these mitigation measures; the court had already considered the future harm to be "imminent."[119] It is more challenging for plaintiffs to justify the mitigation costs if the court rejects the underlying risk of future harm as neither "certainly impending" nor "concrete." After all, *Clapper* seems to foreclose the sufficiency of costs incurred from fears detached from a "certainly impending" threat.[120] Nevertheless, this litigation strategy should not be removed from plaintiffs' quiver.

In another carveout of its risk of future harm analysis, *TransUnion* emphasized that injunctive relief may be a more appropriate remedy than damages.[121] Since *TransUnion* held that "the risk of future harm on its own does not support Article III standing for the plaintiffs' *damages* claim," there is still an opportunity to readily use the risk of future harm for injunctive relief.[122] This language suggests that the Court interpreted *Spokeo* to mean that the risk of future harm can be concrete only in the context of injunctive relief and only as long as the risk is "sufficiently imminent and substantial."[123] Thus, it appears that data breach plaintiffs may seek injunctive relief despite not yet being concretely harmed. In the data breach context, injunctive relief may include the negligent company taking steps to prevent the harmful use of the stolen information.[124] But since the information is already out of the defendants' hands, it is unclear how effective this relief would be in practice.[125] Yet, in a post-*TransUnion* landscape, damages may be off the table if plaintiffs can only allege the risk of future harms.

B. *Navigating the Post-*TransUnion *"Closely Related to Traditional Harm" Test*

In *TransUnion*, the Court provided only vague guidance about this test.[126] Although *TransUnion* does not bar data breach plaintiffs' arguments regarding closely related harms, it does not help said plaintiffs. The "close relationship

---

[118] *Id.*

[119] *Id.* at 389.

[120] *See* Clapper v. Amnesty Int'l USA, 568 U.S. 398, 417 (2013).

[121] *See TransUnion*, 141 S. Ct. at 2198, 2213.

[122] *Id.* at 2213 (emphasis added).

[123] *Id.* at 2210.

[124] *See, e.g.*, In re Target Corp. Data Sec. Breach Litig., 66 F. Supp. 3d 1154, 1161 (D. Minn. 2014) (describing extended credit-monitoring services).

[125] *See* Ben Luthi, *Four Ways to Reduce the Risk of Identity Theft*, EXPERIAN (Jan. 10, 2020), https://www.experian.com/blogs/ask-experian/how-to-reduce-the-risk-of-identity-theft/ [https://perma.cc/QPE9-37HQ].

[126] Hunstein v. Preferred Collection & Mgmt. Servs., Inc., 17 F.4th 1016, 1024 (11th Cir. 2021), *vacated en banc*, 48 F.4th 1236 (11th Cir. 2022) (explaining that the "precise fit between an alleged intangible harm and a common-law tort" was left unanswered by *TransUnion*).

with traditional harms" test is a backwards-looking approach. Data breach cases are novel when juxtaposed to the long tradition of the common law, so this test is necessarily biased against such claims.[127] Justice Kavanaugh's language criticizing the "contemporary, evolving beliefs" of standing evinces that it will be an uphill battle for data breach plaintiffs to assert their harm within the traditional concreteness framework.[128]

Beholden to this tradition-based approach, data breach plaintiffs may nevertheless attempt to demonstrate standing by associating their harms with traditionally-recognized privacy harms.[129] Specifically, the data breach of private information may be considered closely related to intrusion upon seclusion[130] or disclosure of private information.[131] Courts would likely entertain arguments grounded in both of these common law harms—especially because they were singled out in the *TransUnion* decision itself as exemplary.[132]

To limit the reach of *TransUnion*, data breach plaintiffs can attempt to paint data breaches as intimately overlapping with common law privacy harms. Through this lens, data breach harms are distinguishable from the harm in *TransUnion*. Justice Kavanaugh portrayed the harm as "inaccurate or misleading information sit[ting] in a company database," and he analogized it to a "defamatory letter . . . stored . . . in [a] desk drawer."[133] As such, the harm was not closely related to a traditional harm recognized by the courts.[134] This specific reasoning would not ring true in the data breach context. A data breach, by definition, involves the theft of information.

In response, data breach defendants will indubitably characterize this harm as an incongruous analogue to any harm recognized by common law. More specifically, they may contend that the company is one step removed from the data breach and, consequently, multiple steps removed from the harm. Since hackers disclose (or are expected to disclose) private information, the hackers are the ones giving publicity to private facts and intruding upon plaintiffs' seclusion. The defendants, the counterargument goes, were merely negligent in the protection of this information.

On balance, *TransUnion*'s interpretation of the "closely related" test makes a difficult test even more difficult for data breach plaintiffs. While the majority explains that "an exact duplicate in American history" is not required,[135] it simultaneously disavows the idea that courts should loosen standing requirements based upon "contemporary, evolving beliefs about what kinds of

---

[127] *See* Kesan & Zhang, *supra* note 2, at 561.
[128] *TransUnion*, 141 S. Ct. at 2200, 2204.
[129] *See* Wells, *supra* note 14, at 956, 958.
[130] *See* RESTATEMENT (SECOND) OF TORTS § 652B (AM. L. INST. 1977).
[131] *See* RESTATEMENT (SECOND) OF TORTS § 652D (AM. L. INST. 1977).
[132] *See TransUnion*, 141 S. Ct. at 2204.
[133] *Id.* at 2210.
[134] *Id.* at 2209–10.
[135] *Id.* at 2204.

suits should be heard."[136] This test has been described as "a horseshoe test" due to the difficulty in predicting which harms will be "close enough" to traditionally cognizable harms in the eyes of courts.[137] Therefore, judicial discretion and the specific facts will determine whether data breach harms are concrete. Nevertheless, if the Supreme Court's narrow application of this test in *TransUnion* is any litmus test, this suggests a shrinking of the test's application since *Spokeo* first introduced it.[138]

C. TransUnion*'s Narrowing of Statutorily-Derived Standing*

Finally, *TransUnion* significantly impacts the future solutions for data breach standing. After *TransUnion*, a statutory violation alone will not necessarily demonstrate standing.[139] Recall that the *TransUnion* plaintiffs alleged violations of the Fair Credit Reporting Act, which provides clients of negligent companies with a private right of action.[140] The Court rejected statutory-derived standing and held that Congress "may not simply enact an injury into existence."[141] This will hamstring data breach plaintiffs' ability to show standing by solely pointing to the Fair Credit Reporting Act or other statutes.[142]

In light of this development, *TransUnion* also throws into question the practicality of a data breach private right of action that Congress may legislate in the future.[143] The Federal Credit Reporting Act unambiguously states that companies failing to provide "reasonable procedures to assure maximum possible accuracy"[144] of credit reports "with respect to *any* consumer is liable to *that* consumer."[145] Congress broadly granted this private right of action, but the Supreme Court contorted the statute to its own vision of standing. *TransUnion* prevented plaintiffs from suing under the FCRA without a concrete, real-world injury.[146] This holding is significant, per Justice Kagan, because the

---

[136] *Id.*

[137] *See* Daniel J. Solove & Danielle Keats Citron, *Standing and Privacy Harms: A Critique of* TransUnion v. Ramirez, 101 B.U. L. REV. ONLINE 62, 66 (2021).

[138] *See supra* notes 57–58 and accompanying text.

[139] *See TransUnion*, 141 S. Ct. at 2204–05.

[140] *Id.* at 2200–01.

[141] *Id.* at 2204–05 (citing Hagy v. Demers & Adams, 882 F.3d 616, 622 (6th Cir. 2018)).

[142] Prior to *TransUnion*, the Third Circuit had held that an FCRA violation (by itself) was sufficient to demonstrate standing in the data breach context. *See* In re Horizon Healthcare Servs., Inc. Data Breach Litig., 846 F.3d 625, 641 (3rd Cir. 2017).

[143] In a slightly different context, the Sixth Circuit has reaffirmed that plaintiffs "[do] not automatically have standing simply because Congress authorizes a plaintiff to sue a debt collector for failing to comply with the FDCPA." Ward v. Nat'l Patient Acct. Servs. Sols., Inc., 9 F.4th 357, 361 (6th Cir. 2021).

[144] 15 U.S.C. § 1681e(b).

[145] *Id.* § 1681n(a) (emphasis added).

[146] As the Third Circuit put it, "the lesson of *Spokeo* is that we must confirm a concrete injury or material risk exists even when Congress confers a right of action." Kamal v. J. Crew

Court held "for the first time, that a specific class of plaintiffs whom Congress allowed to bring a lawsuit cannot do so under Article III."[147]

If Congress were to similarly legislate on data breach standing, the legislation would likely meet an equally dismal fate.[148] This is particularly true if the legislation were to provide a right to those who were not yet directly harmed by the data breach. While *TransUnion* acknowledges that Congress can elevate injuries to the level of legally cognizable injuries sufficient for standing, such injuries must be "*de facto*" and "exist" in the world.[149] This brings us full circle. Plaintiffs would, once again, be stuck arguing that the harms associated with a data breach are concrete and that the risk of future harm is not too speculative.[150] Therefore, *TransUnion* complicates the calls for Congress to legislate broadly on the issue.[151] Since the Supreme Court views itself as the ultimate arbitrator of standing issues,[152] a more favorable doctrine of standing for data breach plaintiffs will likely originate from the courts rather than from Congress.

V. CONCLUSION

In recent years, there has been a controversial circuit split over data breach standing in federal courts. While some circuits have viewed the risk of future harm stemming from a data breach as sufficient to demonstrate standing, others have not.[153] *TransUnion* will likely significantly reshape this essential question. It creates three significant roadblocks for data breach plaintiffs: (1) the risk of future harm is not likely to be "concrete" for purposes of seeking damages; (2) *Spokeo*'s "close relationship" concreteness test is not conducive to evolving, modern ideas about standing; and (3) the Court will not recognize a congressionally-granted right of action in the absence of plaintiffs suffering a concrete injury.[154]

While *TransUnion* does not definitively shut the door on data breach plaintiffs, they will be on even shakier footing when it comes to Article III standing. Not all hope is lost, however. To review, plaintiffs can distinguish themselves from the *TransUnion* holding in three ways. First, the risks from

---

Group, Inc., 918 F.3d 102, 115 (3d Cir. 2019). *TransUnion* confirms this lesson. *See TransUnion*, 141 S. Ct. at 2204–05.

[147] *TransUnion*, 141 S. Ct. at 2225 (Kagan, J., dissenting).

[148] Certainly, not every scholar expects *TransUnion* to doom statutorily-derived standing. *See, e.g.*, Pierce, *supra* note 27.

[149] *TransUnion*, 141 S. Ct. at 2204–05.

[150] *See id.* at 2205 (citing Spokeo Inc. v. Robins, 578 U.S. 330, 341 (2016)).

[151] Much of the literature has recommended that Congress enact statutory standing legislation in the data breach context. *See, e.g.*, Ioannis Koutsodendris, Note, *Adjudicate or Legislate: The Great Data Breach Standing Circuit Split*, 30 S. CAL. INTERDISC. L.J. 771, 792 (2021).

[152] *See TransUnion*, 141 S. Ct. at 2205.

[153] *See supra* Part II.

[154] *See supra* notes 79–81 and accompanying text.

data breaches are more significant than those alleged in *TransUnion*.[155] Second, data breach plaintiffs often suffer independent harms—namely, emotional distress and mitigation costs.[156] Third, data breach victims experience harms closely related to the common law harms of intrusion upon seclusion and disclosure of private information.[157] These strategies provide plaintiffs with potential footholds in a post-*TransUnion* world of standing doctrine.

[155] *See supra* notes 93–105 and accompanying text.
[156] *See supra* notes 108–16 and accompanying text.
[157] *See supra* Section IV.B.