PUBLISHED

UNITED STATES COURT OF APPEALS
FOR THE FOURTH CIRCUIT

No. 21-2144

BRADY O'LEARY, on behalf of himself and all others similarly situated,

Plaintiff − Appellant,

v.

TRUSTEDID, INC.,

Defendant – Appellee.

Appeal from the United States District Court for the District of South Carolina, at Columbia. Sherri A. Lydon, District Judge. (3:20−cv−02702−SAL)

Argued: December 7, 2022 Decided: February 21, 2023

Before AGEE, DIAZ, and QUATTLEBAUM, Circuit Judges.

Vacated and remanded with instructions by published opinion. Judge Diaz wrote the opinion, in which Judge Agee and Judge Quattlebaum joined.

ARGUED: David Andrew Maxfield, DAVE MAXFIELD, ATTORNEY, LLC, Columbia, South Carolina, for Appellant. Ashley Charles Parrish, KING & SPALDING LLP, Washington, D.C., for Appellee. **ON BRIEF:** Justin T. Holcombe, SKAAR & FEAGLE, LLP, Woodstock, Georgia, for Appellant. Gabriel Krimm, Washington, D.C., Zachary A. McEntyre, Robert D. Griest, KING & SPALDING LLP, Atlanta, Georgia, for Appellee.

DIAZ, Circuit Judge:

Brady O'Leary appeals the dismissal of his claim against TrustedID, Inc. under South Carolina's Financial Identity Fraud and Identity Theft Protection Act (the "Act"), S.C. Code Ann. § 37-20-180. The district court held that O'Leary alleged an Article III injury in fact but failed to state a claim under the Act. O'Leary agrees with the district court's decision on standing but appeals its Rule 12(b)(6) dismissal. But we hold that O'Leary hasn't alleged an Article III injury, so we vacate and remand with instructions.

I.

A.

O'Leary's First Amended Class Action Complaint alleges the following.

Nonparty Equifax was subject to a data breach. Equifax then engaged its subsidiary, TrustedID, to use TrustedID's website to inform customers whether they were impacted by the data breach.

O'Leary had no other way to learn whether his data had been compromised, so he went to TrustedID's website. The website prompted O'Leary to enter six digits of his social security number ("SSN"). In exchange for this information, the website informed O'Leary that he was "not impacted" by Equifax's data breach. J.A. 28 ¶ 11. TrustedID didn't use any other security precautions, such as a password, unique personal identification number, or another authentication device. O'Leary alleges that TrustedID shared the six digits of his SSN with Equifax.

B.

O'Leary sued TrustedID in state court, alleging that TrustedID's practice of requiring six digits of consumers' SSNs violated the Act and South Carolina's common-law right to privacy.

The Act prohibits "requir[ing] a consumer to use his social security number or a portion of it containing six digits or more to access an Internet web site, unless a password or unique personal identification number or other authentication device is also required to access the Internet web site." S.C. Code Ann. § 37-20-180(A)(4). O'Leary alleges that TrustedID "could have avoided violating the statute simply by requesting five or fewer digits" of consumers' SSNs. J.A. 29 ¶ 20.

TrustedID removed the case to federal court under the Class Action Fairness Act ("CAFA"). O'Leary then filed an Amended Complaint in the federal district court, re-asserting the same claims and adding one for negligence. TrustedID moved to dismiss under Federal Rule of Civil Procedure 12(b)(6).

While TrustedID's motion was pending, O'Leary filed a Motion to Determine Subject Matter Jurisdiction Or, in the Alternative, to Remand. O'Leary agreed that the case satisfied CAFA. But he asked the district court to "inquire before reaching the merits into whether it has subject matter jurisdiction" under Article III given *TransUnion LLC v. Ramirez*, 141 S. Ct. 2190 (2021), which had been recently decided. D. Ct. ECF No. 44 at 2. O'Leary took "no position" on whether he'd suffered an Article III injury. *Id.*

TrustedID opposed O'Leary's "puzzling" motion and argued that he had sufficiently alleged standing. D. Ct. ECF No. 46 at 1. The district court held a hearing.

The district court denied O'Leary's motion, holding that he had alleged Article III standing. The court noted the unique posture of a plaintiff questioning his own standing, rather than a defendant raising the issue under Rule 12(b)(1). But the court decided that O'Leary's "harm allegations, while perhaps scarce, certainly suggest that Plaintiff is claiming to have suffered some damage as a result of Defendant's actions." J.A. 43.

In its decision, the court recounted both parties' articulation of O'Leary's alleged injury: At the hearing, O'Leary said he was injured when TrustedID "intentionally [took] personal identifying information and monetiz[ed] it in some way." *Id.* And TrustedID called the alleged injury "an invasion of privacy or 'intrusion upon seclusion,' as used in *Ramirez*." J.A. 44. The district court held that O'Leary had alleged "an intangible concrete *harm* in the manner of an invasion of privacy," which the court said was "enough to give [it] subject-matter jurisdiction at this early stage of the case." *Id.*

Nonetheless, the district court granted TrustedID's motion to dismiss on the merits, holding that O'Leary had not plausibly stated a claim under the Act or under common-law principles of privacy or negligence.

On appeal, O'Leary again notes his "concerns as to whether the [statutory] violation in this case constitutes a concrete injury in fact for Article III standing," Appellant's Br. at 2, but he asks us to affirm the district court's holding on standing anyway. He challenges only the district court's dismissal of his claim under the Act, not the dismissal of his common-law privacy and negligence claims.

II.

We hold that O'Leary has alleged only a bare statutory violation and no Article III injury. So we do not—and cannot—reach the question whether he's pleaded facts that state a claim under the Act, though he may presumably pursue that claim in state court.

We begin with some key principles of federal jurisdiction. Article III constrains federal courts to hear only cases or controversies in which (1) a plaintiff "suffered an injury in fact that is concrete, particularized, and actual or imminent," (2) "the injury was likely caused by the defendant," and (3) "the injury would likely be redressed by judicial relief." *TransUnion*, 141 S. Ct. at 2203.

This case implicates the first requirement: whether O'Leary suffered a concrete injury in fact. Without one, he can't pursue his claim in federal court. *Id.* at 2200 ("No concrete harm, no standing.").

The most obvious concrete injuries are "tangible harms, such as physical harms and monetary harms." *Id.* at 2204. Intangible harms are trickier, but they too can be concrete. *Id.* "Chief among them are injuries with a close relationship to harms traditionally recognized as providing a basis for lawsuits in American courts," such as "reputational harms, disclosure of private information, and intrusion upon seclusion." *Id.*

The intangible harm of enduring a statutory violation, standing alone, typically won't suffice under Article III—unless there's separate harm (or a materially increased risk of another harm) associated with the violation. *See Spokeo, Inc. v. Robins*, 578 U.S. 330, 342 (2016) (no standing based on "bare procedural violation" of the Fair Credit Reporting Act); *see also Baehr v. Creig Northrop Team, PC*, 953 F.3d 244, 254 (4th Cir. 2020) (being

"deprived of impartial and fair competition between settlement services providers," in violation of the Real Estate Settlement Procedures Act, isn't a concrete injury when it didn't increase plaintiffs' costs); *Dreher v. Experian Info. Sols., Inc.*, 856 F.3d 337, 347 (4th Cir. 2017) (alleged informational injury from the violation of a Fair Credit Reporting Act provision wasn't a concrete injury when the plaintiff didn't allege how the violation adversely affected him). In other words, "under Article III, an injury in law is not an injury in fact." *TransUnion*, 141 S. Ct. at 2205.[1]

There don't appear to be cases interpreting the South Carolina Act under an Article III framework. But several analogous contexts provide guidance, and we discuss them below.

A.

Cases involving the Fair and Accurate Credit Transactions Act ("FACTA"), 15 U.S.C. § 1681 *et seq.*, show that a FACTA digit-truncation violation isn't a concrete injury unless it creates a nonspeculative risk of identity theft.

"FACTA forbids merchants from printing more than the last five digits of the [credit] card number (or the card's expiration date) on receipts offered to customers." *Muransky v. Godiva Chocolatier, Inc.*, 979 F.3d 917, 921 (11th Cir. 2020) (en banc). In

[1] *TransUnion*, *Spokeo*, and the other key standing cases dealt with federal statutes, so their separation-of-powers concerns aren't implicated in this case. But the district court assumed that the same principles (i.e., that a mere statutory violation typically won't suffice as an Article III injury) apply whether the alleged statutory violation is under federal or state law. J.A. 42 n.6. We think the district court must be right. It would be an anomaly if a state legislature could grant plaintiff the keys to federal court based on a mere statutory violation when Congress can't.

Muransky, the plaintiff received "a receipt containing the first six and last four digits of his sixteen-digit credit card number—too many digits under FACTA." *Id.* at 922. The en banc Eleventh Circuit held that receiving the receipt wasn't itself a concrete injury under Article III, and the plaintiff didn't "plausibly allege a material risk . . . or anything approaching a realistic danger" of identity theft. *Id.* at 933. Even though Congress drew the line at five unredacted digits, the court reasoned, federal courts must still independently determine whether the plaintiff alleging a FACTA violation suffered a concrete injury. *Id.* at 933–34.

The D.C. Circuit appears to be the only Court of Appeals to find Article III standing based on a FACTA violation, in a case in which the plaintiff received a receipt that exposed the entire credit-card number and expiration date—that is, "sufficient information for a criminal to defraud her." *Jeffries v. Volume Servs. Am., Inc.*, 928 F.3d 1059, 1066 (D.C. Cir. 2019). Given this "egregious" FACTA violation, the plaintiff's increased risk of identity theft wasn't speculative or conjectural, the court reasoned. *Id.* So her injury sufficed under Article III.

B.

Also illustrative are our data-breach precedents. As in the FACTA cases, we've held that being subjected to a data breach isn't in and of itself sufficient to establish Article III standing without a nonspeculative, increased risk of identity theft.

In *Beck v. McDonald*, we held that plaintiffs whose personal information was compromised in a data breach hadn't shown an Article III injury based on an alleged "increased risk of future identity theft and the cost of measures to protect against it." 848

F.3d 262, 267 (4th Cir. 2017). The plaintiffs' alleged increased risk was only speculative, and even though a laptop and reports with their personal information had been stolen, "the mere theft of these items, without more, cannot confer Article III standing." *Id.* at 275.

In contrast, the plaintiffs in *Hutton v. National Board of Examiners in Optometry, Inc.*, were, in fact, victims of identity theft traceable to the defendant's data breach. 892 F.3d 613, 621–22 (4th Cir. 2018). Unlike the *Beck* plaintiffs, who relied on "a mere compromise of personal information," the *Hutton* plaintiffs suffered identity theft and credit-card fraud such that there was "no need to speculate on whether substantial harm will befall" them—it already had. *Id.* at 621–22. So those plaintiffs had standing.

C.

The parties also point us to one more relevant authority: *Ruiz v. Gap, Inc.*, 380 F. App'x 689 (9th Cir. 2010). *Ruiz* involved a California statute that prohibited requiring "an individual to use his or her social security number to access an Internet Web site, unless a password or unique personal identification number or other authentication device is also required to access the Internet Web site." *Id.* at 693 (quoting Cal. Civ. Code § 1798.85(a)(4) (2006)).

The plaintiff there alleged that he had to use his (full) SSN to fill out a job application for the defendants, in violation of the statute. *Id.* He also submitted an expert affidavit explaining how the disclosure of his SSN increased his risk of identity theft. *Id.* at 691. On that record, the district court found that the plaintiff's increased risk of identity theft was "real, and not merely speculative," constituting an Article III injury. *Id.* at 691. The Ninth Circuit affirmed in an unpublished opinion.

III.

Applying the principles just discussed, we hold that O'Leary hasn't alleged an Article III injury in fact. It's true that "general factual allegations of injury resulting from the defendant's conduct" can suffice at the pleading stage. *Beck*, 848 F.3d at 270 (quoting *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 561 (1992)). But even given that low bar and taking all plausible factual inferences in O'Leary's favor, his complaint doesn't allege an injury that suffices under Article III.

A.

As the cases above show, Article III excludes plaintiffs who rely on an abstract statutory privacy injury unless it came with a nonspeculative increased risk of identity theft. And unlike in *Ruiz*, *Beck*, and the FACTA cases, O'Leary hasn't alleged—even in a speculative or conclusory fashion—that entering six digits of his SSN on TrustedID's website has somehow raised his risk of identity theft.

Simply put, O'Leary can't connect the alleged statutory violation to an increased risk of identity theft without a Rube Goldberg-type chain reaction. For example, crediting his allegation "on information and belief" that TrustedID shared his six SSN digits with Equifax, J.A. 29 ¶ 17, there would have to be another Equifax data breach, that breach would have to compromise O'Leary's partial SSN, and an identity thief would then have to misappropriate that information to harm O'Leary (presumably by first figuring out the rest of his SSN). That's the kind of daisy chain of speculation that can't pass muster under Article III. *See Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 410–11 (2018); *Beck*, 848 F.3d at 274–75.

O'Leary's position that it would've been fine for TrustedID to require five digits of his SSN—but not six—is telling. He's failed to explain how entering six digits increased his risk of identity theft (or otherwise concretely injured him) in a way that five digits wouldn't. This omission betrays the fact that O'Leary relies entirely on a mere procedural violation of a statute, which Article III rejects. *See Spokeo*, 578 U.S. at 342.

B.

Nor has O'Leary alleged an injury with a "close relationship" to a traditional or common-law analog. *TransUnion*, 141 S. Ct. at 2204. The parties point generally to O'Leary's "privacy interest in his Social Security number." Appellee's Br. at 8. But the cases they cite suggest that SSN privacy is important to stave off identity theft—of which O'Leary doesn't allege an increased risk. *See, e.g.*, *Ostergren v. Cuccinelli*, 615 F.3d 263, 279–80 (4th Cir. 2010) (suggesting, in First Amendment challenge to statute, that states likely have a compelling interest in prohibiting disclosure of SSNs because of the risk of identity theft); *Sherman v. U.S. Dept. of Army*, 244 F.3d 357, 365–66 (5th Cir. 2001) (noting that disclosure of SSNs can be appropriate, especially to avoid fraud, but individuals also have an interest in keeping them private to avoid identity theft).

Since O'Leary hasn't pleaded a nonspeculative connection between the alleged statutory violation and identity theft, he appears to rely on some abstract privacy interest in his SSN itself. But such an injury bears no close relationship to a traditional or common-law analog.

First, O'Leary hasn't alleged an injury with a close relationship to "intrusion upon seclusion,"[2] as TrustedID suggested in the district court. True, *TransUnion* mentions intrusion upon seclusion as a traditionally recognized harm that provides a basis for lawsuits in federal court. 141 S. Ct. at 2204. The case *TransUnion* cites as an example was then-Judge Barrett's holding in *Gadelhak* that receiving unwanted text messages (which violated the Telephone Consumer Protection Act of 1991) could be a concrete injury in fact, as it closely relates to intrusion upon seclusion. 950 F.3d at 462.

We too have recognized that violations involving unwanted calls under the Telephone Consumer Protection Act are concrete injuries in fact, based on federal courts' traditional protection of "privacy interests in the home." *Krakauer v. Dish Network, L.L.C.*, 925 F.3d 643, 653 (4th Cir. 2019). But the injury O'Leary alleges doesn't bear a close relationship to this traditional harm.

O'Leary pleaded that he chose to hand over his partial SSN "[i]n exchange for" finding out whether he was impacted by Equifax's data breach. J.A. 28 ¶ 11. It's the unwanted intrusion into the home that marks intrusion upon seclusion, and O'Leary hasn't pleaded anything that closely relates to that.

Second, *TransUnion* recognizes that the "disclosure of private information" can be another traditional analog for intangible harms that confer standing. 141 S. Ct. at 2204 (citing *Davis v. FEC*, 554 U.S. 724, 733 (2008)). Neither party has argued that this applies

[2] Intrusion upon seclusion is a common-law cause of action "against defendants who invade[] the private solitude of another." *Gadelhak v. AT&T Servs., Inc.*, 950 F.3d 458, 462 (7th Cir. 2020) (quoting Restatement (Second) of Torts § 652B (Am. Law Ins. 1977)).

to O'Leary, though. And "[t]he party invoking federal jurisdiction bears the burden of establishing" standing. *Lujan*, 504 U.S. at 561.

The parties' silence on this theory is likely for good reason. *Davis* held that a self-financed political candidate had standing to challenge a statute that would require him to disclose to the government when he spent more than $350,000 in personal funds on his campaign, which implicated the candidate's privacy of association guaranteed by the First Amendment. 554 U.S. at 733, 744. Here, nothing implicates O'Leary's associational rights. And he (voluntarily) disclosed his partial SSN to TrustedID, not to the government.

At bottom, O'Leary hasn't adequately pled that he was injured by the alleged statutory violation at all—much less in a way that closely relates to a traditional analog for a federal lawsuit.

IV.

It's certainly odd that TrustedID failed to comply with the five-digit SSN cutoff, which doesn't appear to be unique to South Carolina's Act. But federal courts can't entertain a case without a concrete injury in fact. We therefore vacate the district court's judgment and remand with instructions to remand this case to state court, where it originated. *See Dixon v. Coburg Dairy, Inc.*, 369 F.3d 811, 815–16 (4th Cir. 2004) (en banc). We offer no opinion about whether the alleged facts state a claim under the Act. Absent Article III jurisdiction, that's a question for O'Leary to take up in state court.

VACATED AND REMANDED WITH INSTRUCTIONS