The Supreme Court TransUnion Case Part 1 —What It Means for Standing in Cyber Cases

July 8, 2021

This is Part 1 of a two-part article on the recent U.S. Supreme Court *TransUnion* decision. In Part 2, we will discuss the implications of the decision for efforts to defeat class certification.

Individuals whose personal information was compromised in a data breach have had mixed success in bringing lawsuits in federal court against the companies that held their data. The federal courts of appeal have taken divergent views on when an increased risk of future identity theft or fraud arising out of a data breach is sufficient to establish standing. Recent decisions had been moving towards a more unified theory of standing, but the Supreme Court's holding in *TransUnion LLC v. Ramirez*, No. 20-297, slip op. (U.S. June 25, 2021) will likely create new uncertainties. Although *TransUnion* did not involve a data breach, the Court's opinion emphasizes that qualifying Article III injuries are those that go beyond procedural statutory violations and that a risk of future harm alone is insufficient under Article III in a suit for damages. As the lower courts interpret and apply *TransUnion*, it will probably become more difficult for data breach victims who allege imminent harm—as opposed to a harm that has already been realized—to establish standing to sue.

Recent Circuit Court Decisions: *Tsao*, *McMorris* and *In re Equifax*. The U.S. federal circuit courts have followed varying approaches as to whether (1) increased risk of future identity theft is a sufficient basis to demonstrate injury-in-fact, and if so, (2) what allegations suffice to establish standing on that ground.

In February, the Eleventh Circuit held that conclusory allegations of an "elevated risk of identity theft" were insufficient to establish standing where hackers accessed a restaurant's point-of-sale system, compromising victims' credit and debit card information. *Tsao v. Captiva MVP Rest. Partners LLC*, 986 F.3d 1332 (11th Cir. 2021). The plaintiffs alleged that the breach, which lasted nearly a year, caused them to suffer a substantial risk of future identity theft. However, no plaintiff could point to any actual identity theft as a result of the breach. The plaintiffs also argued that they had already suffered concrete injuries, including lost credit card reward points, lost time and restricted card access, while their compromised cards were cancelled.

The Eleventh Circuit acknowledged that its sister circuits were divided on the question of whether increased risk of identity theft establishes injury-in-fact at the pleading stage. The court found that the loss of credit card and account numbers rarely leads to identity theft. The plaintiffs therefore did not face a "substantial risk" of identity theft and did not have standing on this basis. Plaintiffs had argued that they suffered concrete injuries because they were forced to respond to the breach. The court found that those injuries constituted "manufactur[ed] standing" because the plaintiffs "inflict[ed] harm on themselves based on their fears of hypothetical future harm that is not certainly impending." The court left the door open to finding standing on the basis of increased risk of identity theft on a different set of facts.

In April, the Second Circuit attempted to harmonize the circuits' treatment of increased risk of future identity theft in data breach cases by articulating a three-factor test. In *McMorris v. Carlos Lopez & Assocs., LLC*, 995 F.3d 295 (2d Cir. 2021), the Second Circuit held that "plaintiffs may establish [Article III] standing based on an increased risk of identity theft or fraud following the unauthorized disclosure of their data." One of defendant's employees accidentally sent a company-wide email that included the personal identifying information (PII) of 130 current and former employees. The PII exposed included "Social Security numbers, home addresses, dates of birth, telephone numbers, educational degrees, and dates of hire." The plaintiffs had alleged injuries in the form of risk of future harm as well as time and costs spent implementing proactive protective measures.

The Second Circuit suggested courts look at three non-exhaustive factors when analyzing whether an alleged increased risk of future harm resulting from a data breach establishes plaintiffs' standing: "(1) whether the plaintiffs' data has been exposed as the result of a targeted attempt to obtain that data; (2) whether any portion of the dataset has already been misused, even if the plaintiffs themselves have not yet experienced identity theft or fraud; and (3) whether the type of data that has been exposed is sensitive such that there is a high risk of identity theft or fraud."

Applying the factors, the court said, was "straightforward"—the disclosure was not targeted because the data was exposed accidentally and only to internal employees, and there were no allegations of misuse, so it did not matter that the disclosure included Social Security numbers. The Second Circuit noted that "plaintiffs do not necessarily suffer an injury in fact any and every time there has been a disclosure involving more sensitive data." The court also held that plaintiffs do not establish standing by spending time and money to protect themselves following data breaches without a predicate finding of substantial risk of future identity theft or fraud.

In June, the Eleventh Circuit endorsed part of the *McMorris* analysis in *In re Equifax Inc. Customer Data Security Breach Litigation*, No. 20-10249, 2021 WL 2250845 (11th Cir.

June 3, 2021), suggesting that perhaps the *McMorris* analysis would prevail. The Equifax case involves a 2017 data breach where the Social Security numbers, names, dates of birth, addresses and other data of nearly 150 million people were exposed. On appeal of a class-action settlement approval, the court found that the plaintiffs had standing in large part because "the allegations of some Plaintiffs that they have suffered injuries resulting from actual identity theft support the sufficiency of all Plaintiffs' allegations that they face a risk of identity theft." In support of its holding, the court quoted *McMorris*: "[C]ourts have been more likely to conclude that plaintiffs have established a substantial risk of future injury where they can show that at least some part of the compromised dataset has been misused."

TransUnion: A Win for Defendants in Breach Lawsuits? The Supreme Court's June 25 ruling in *TransUnion* adds a wrinkle to the standing analysis in data breach cases by suggesting that standing on the basis of a future risk of harm may only exist in an action for injunctive relief.

A group of individuals who had been erroneously categorized as being on the U.S. Treasury Department's Office of Foreign Assets Control (OFAC)'s list of terrorists, drug traffickers and other serious criminals by a credit reporting agency sued the agency under several statutes and won a multimillion dollar verdict after a jury trial. On appeal, TransUnion challenged the plaintiffs' standing, claiming that they had not suffered a qualifying injury in fact and were therefore ineligible to bring their claims in federal court. Assuming that the plaintiffs could establish a violation of the Fair Credit Reporting Act, the Court held 5–4 that only a subset of the class—less than a quarter of the 8,000 total—had Article III standing. Only the smaller group of plaintiffs' erroneous potential terrorist status had been released externally to third parties. The other class members were merely labeled as potential terrorists in TransUnion's system. As a result, the Court found, these class members did not suffer any of the concrete injuries that "traditionally" form the basis of lawsuits in American courts.

Plaintiffs had also brought disclosure and summary-of-rights claims on the grounds that TransUnion's mailings to them failed to meet statutory requirements. The Court also found that plaintiffs had no standing to bring these "bare procedural violations" because there was no evidence that any plaintiff (other than the named plaintiff) had even opened these mailings or been harmed by them.

TransUnion is relevant to data breach class actions in at least two ways. First, *TransUnion* may spell the end of standing based on risk of future harm in cases seeking damages. The *TransUnion* majority appears to have cabined the language in *Spokeo, Inc. v. Robins*, 578 U.S. 330 (2018) that a "material risk of harm" can sometimes "satisfy the requirement of concreteness" as applying only to matters seeking injunctive relief. The Court found persuasive "that in a suit for damages [as opposed to injunctive relief], the

mere risk of future harm, standing alone, cannot qualify as a concrete harm." The Court presented an analogy: if a reckless driver gets on the road, drivers around them may not sue them for the damages caused by the elevated risk they experienced, only for actual injuries they sustain in a crash. The Court did make clear that "a person exposed to a risk of future harm may pursue *forward-looking, injunctive relief* to prevent the harm from occurring." But, as Justice Thomas noted in his dissent, the majority performed a "reworking of *Spokeo*" by "all but eliminating the risk-of-harm analysis." Therefore, it appears that *TransUnion* poses new hurdles for plaintiffs in data breaches who have not suffered from actual misuse of their PII and will likely be grappled with anew among the lower courts.

Second, *TransUnion* answers a question that *McMorris* did not reach but that is relevant to any class action alleging violations of data breach or privacy statutes, namely: whether "plaintiffs may allege *present* injury in fact stemming from a violation of a statute designed to protect individuals' privacy." Even though all of the *TransUnion* plaintiffs claimed they were harmed by the defendant's violation of federal law, the Supreme Court found only those who suffered a "concrete" injury—separate from the violation alone—had standing. Accordingly, a bare procedural violation of a data privacy statute, such as the CCPA or FCRA, is likely *not* enough to establish standing going forward under the reasoning of *TransUnion*. Under *TransUnion*, plaintiffs must allege a concrete injury, likely with a historical analogue, in order to establish Article III standing.

In sum, Article III standing in data breach class actions is on uneven ground. The Court in *TransUnion* did clarify that bare statutory violations alone are not sufficient to confer Article III standing, emphasizing the need for a concrete harm with a traditional analogue. For plaintiffs whose injury-in-fact theory rests on risk of future harm, the Second and Eleventh Circuits seemed to be moving towards a factor test based on the targeting, misuse and sensitivity of the data breached. Yet *TransUnion* casts serious doubt on whether risk-only plaintiffs suing for damages may proceed at all. It remains to be seen how lower courts will apply the *TransUnion* holding in data breach cases. Standing is not settled yet, and interested parties should continue to watch the courts and take a look at our practical tips for reducing data breach litigation risk based on our analysis of recent CCPA litigation. To subscribe to the Data Blog, please click here.

The authors would like to thank Debevoise law clerk Samuel J. Allaman and summer associates Kat McKay and John Juenemann for their contributions to this client update.

* * *

Please do not hesitate to contact us with any questions.

NEW YORK

Avi Gesser
agesser@debevoise.com

Johanna N. Skrzypczyk
jnskrzypczyk@debevoise.com