LAW360

Portfolio Media. Inc. | 230 Park Avenue, 7th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Why Standing Analysis Is Key In Data Breach Mediation

By **Abe Melamed** (October 13, 2023, 3:44 PM EDT)


Abe Melamed

There has been a proliferation of data breach class action litigation in the past several years, including several recent data breach cases against some of the largest law firms in the country and many more against small companies that previously had never been targets.

Some large data breach settlements in 2022 included a T-Mobile US Inc. data breach settlement for $350 million and a Morgan Stanley data breach settlement for $60 million.

This proliferation in data breach cases has brought to the forefront a gateway question in federal court data breach class actions: whether plaintiffs have standing under Article III of the U.S. Constitution based solely on an increased risk of future identity theft.

Plaintiffs may have anxiety that their personal identifying information is out there in the world, and they may take steps to prevent future harm by monitoring or freezing their credit. But is that a sufficiently concrete and particularized injury to satisfy Article III standing?

Many circuit courts have found it may be, depending on the type of data taken, whether it was taken by criminals and whether any members of the class have had their identities stolen.

Based on these factors, the court can assess how likely and imminent an injury might be, and in turn how reasonable the injury of anxiety or protective measures may be, constituting a concrete injury. Yet during settlement negotiations the parties seldom address these factors, despite the case potentially turning on this legal issue.

But this evaluation, if done in advance of mediation, can offer a justification for demands and offers, and ultimately for settlement outcomes in class actions and mass arbitrations.

Standing in data breach cases has always been a central issue in federal court litigation.

McMorris v. Carlos Lopez & Associates

Prior to the U.S. Court of Appeals for the Second Circuit's 2021 decision in McMorris v. Carlos Lopez & Associates LLC, it seemed there was a circuit split on the issue.

In McMorris, the Second Circuit clarified that there was not a circuit split on the issue, and held that the

plaintiffs may have standing in certain circumstances. It was also alleged that a member of the defendant's human resources department was negligent in sending a companywide email with a spreadsheet containing the personally identifiable information of all employees, including dates of birth, Social Security numbers and more.

The plaintiffs filed a class action, and the U.S. District Court for the Southern District of New York dismissed the case for lack of Article III standing.

On appeal, the Second Circuit created a comprehensive three-part test, viewed under a totality of the circumstances, to determine if the plaintiffs in any given data breach have standing to sue:

1. Whether the plaintiffs' data had been exposed as the result of a targeted attempt to obtain the data, such as a criminal hack;

2. Whether any portion of the data has already been misused, even if the plaintiffs themselves have not been the subjects of identity theft or fraud; and

3. Whether the type of data exposed is sensitive enough that it creates a high risk of identity theft or fraud.

The court held that if, in evaluating those three factors, the court finds the plaintiffs have a substantial risk of identity theft, then any expenditures made by the class in protecting themselves against future identity theft are recoverable.

TransUnion v. Ramirez

Following McMorris, in 2021, the U.S. Supreme Court issued a decision in TransUnion LLC v. Ramirez, which was not a data breach case. The plaintiffs were a class of TransUnion customers whose credit reports had alerts placed in them that incorrectly suggested they might be terrorists or criminals.

The Supreme Court held that the members of the class whose incorrectly flagged credit reports had been disseminated to third parties had standing to sue because the injury bore a sufficiently close relationship to "the reputational harm associated with the tort of defamation."

However, the court also held that most of the class members whose credit reports had not been disseminated to third parties lacked standing, because, "in a suit for damages, the mere risk of future harm, standing alone, cannot qualify as a concrete harm-at least unless the exposure to the risk of future harm itself causes a separate concrete harm."

Clemens v. ExecuPharm

Following TransUnion, there was some uncertainty as to whether the decision foreclosed standing in data breach cases premised upon the theory of an increased risk of future identity theft.

In Clemens v. ExecuPharm Inc. in 2022, the U.S. Court of Appeals for the Third Circuit held that plaintiffs could still have standing in data breach cases.

The court stated, "Following TransUnion's guidance, we hold that ... a 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."

The court gave an example: "If the plaintiff's knowledge ... causes him to presently experience emotional distress or spend money on mitigation measures like credit monitoring services, the plaintiff has alleged a concrete injury."

This decision seemed to reconcile TransUnion with McMorris, and standing in data breach cases lived on.

Webb v. Injured Workers Pharmacy

Following Clemens, in Webb v. Injured Workers Pharmacy LLC in June, the U.S. Court of Appeals for the First Circuit found standing based on an imminent and substantial risk of future harm in a data breach case.

In Webb, the plaintiffs both alleged that they spent time and effort monitoring their credit to prevent identity theft, that they experienced stress, anxiety and other physical symptoms, and one of the plaintiffs alleged her personally identifiable information was used to file a fraudulent tax return, and she spent time dealing with the Internal Revenue Service to resolve the issue.

The First Circuit cited McMorris and Clemens as guidance in assessing the standing issue and noted that even though they were decided prior to TransUnion, they remain relevant to assessing the risk of future personally identifiable information misuse. The Webb court held that the complaint "plausibly alleges a concrete injury in fact based on the material risk of future misuse of [plaintiffs'] PII and a concrete harm caused by exposure to this risk."

The court focused on the fact that the data breach was the result of a deliberate attack by cybercriminals, it remained undetected for almost four months, that there had been actual misuse of some of the data, and that the stolen personally identifiable information included patient names and Social Security numbers.

Viewed under a totality of the circumstances rubric, the court held that the plaintiffs had demonstrated they were at an increased risk that their information would be misused, and therefore had standing to sue.

The court explained that because plaintiffs alleged they had lost time implementing protective measures, they plausibly alleged a "separate, concrete, present harm" because "time spent responding to a data breach can constitute a concrete injury sufficient to confer standing, at least when that time would otherwise have been put to profitable use."[1]

Additionally, because the alleged injury was in response to a substantial and imminent risk of harm, the court found that the plaintiffs were not manufacturing standing by incurring costs in anticipation of a nonimminent harm, and therefore they had standing.

In re: Brinker Data

It should be noted that U.S. Court of Appeals for the Eleventh Circuit's recent decision in In re: Brinker Data Incident Litigation does not seem to address the question of whether exposure of personally identifiable information to unauthorized third parties, without an additional harm such as time and

money spent monitoring credit and preventing future harm or actual misuse of the personally identifiable information, will satisfy the concrete prong of Article III.

Brinker involved a class of individuals who either had been subjected to fraudulent charges or who were aware their credit card information was obtained by cybercriminals because it had been posted on the dark web. These claims were therefore based upon a concrete and separate harm of actual misuse or of exposure of their information on the dark web, an injury that would be concrete on its own.

But the Brinker case does not seem to answer the question of whether class members who have not had their information posted on the dark web or have not been the victims of fraudulent charges would have Article III standing based only on an increased risk of future identity theft or on the time and money spent on preventing future identify theft.

Bohnak v. Marsh & McLennan

Most recently, in Bohnak v. Marsh & McLennan Companies Inc. on Aug. 24, the Second Circuit found standing in a data breach class action and reversed and remanded the district court's dismissal of the complaint.

The court concluded that TransUnion is the touchstone for determining whether a risk of future injury is sufficiently concrete to constitute an injury in fact, and that the McMorris three-factor test remains the touchstone for determining whether the injury is sufficiently imminent to constitute an injury in fact.

The court held that "similar to the publication of misleading information about some of the plaintiffs in TransUnion, the core injury here — exposure of Bohnak's private, personally identifiable information to unauthorized third parties — bears some relationship to a well-established common-law analog: public disclosure of private facts" and therefore, it was sufficiently concrete to establish Article III standing.

The court also held that Bohnak's allegations that she has suffered a separate harm of the out-of-pocket expenses associated with the prevention, detection and recovery from identity theft, and the lost time associated with attempting to mitigate the consequences establish a concrete injury.

With the question of concreteness answered in the affirmative, the court held that TransUnion did not address the question of imminence and did not override the McMorris analysis of imminence, and therefore the three-factor test from McMorris remains the touchstone for that analysis.

Applying the three-factor test, under a totality of the circumstances analysis, the court held that the plaintiff's allegations that her personally identifiable information was taken through a criminal hack, and that it included her name and Social Security number — highly sensitive information — was sufficient to establish an imminent injury, even though there was no allegation of actual misuse to date.

Therefore, the plaintiff had satisfied both the concrete and imminent prongs of Article III and she had standing. So, in the Second Circuit, the allegation of actual exposure of personally identifiable information to unauthorized third parties or the allegation of additional harm such as time and money spent preventing future harm after exposure, will satisfy the concrete prong of Article III.

With that satisfied, district courts must look to the three-factor McMorris test in determining whether the injury is sufficiently imminent to satisfy Article III, and if it is, plaintiffs will have standing.

Conclusion

Many litigators do not address any of these factors in outlining a damages analysis for settlement purposes that would justify their demands or offers. But, when done correctly, this analysis offers a valuable perspective in settlement negotiations.

Litigants can brief whether the nature of the breach is sufficient to create a separate harm of its own, be it emotional distress from fear of future identity theft or time and money spent in monitoring accounts and credit. In evaluating this, they can look to the three-factor test established in McMorris to determine whether the nature of the breach is sufficient to show the increased risk of future identity theft is sufficiently imminent.

For example, if a data breach involves a hack by criminals, and the nature of the personally identifiable information stolen includes dates of birth and Social Security numbers, and some members of the class have already suffered from identity theft, then it makes it more plausible that the entire class suffers from an imminent increased risk of identity theft, and it justifies their anxiety and fears, and in turn their costs spent in protection and monitoring services.

The damages in that case would justifiably be greater than, for example, a case where the breach was just the negligence of human resources, and none of the members of the class have suffered any identity theft or fraud, even if the personally identifiable information included dates of birth and Social Security numbers.

This analysis can be critically helpful in assessing settlement value of data breach cases. It could also be particularly helpful in claims-made settlements, where the defendant may look to limit their exposure across the class, and creating several tranches of settlement values based on which of the McMorris factors a given class member satisfies. And, it may serve as the rubric for evaluating whether a particular member of the class is entitled to relief altogether in common fund settlements.

This evaluation, if done by the parties in advance of mediation, can offer a concrete justification for demands and offers, and ultimately for settlement outcomes in class actions and mass arbitrations.

This will in turn assist the mediator in helping the parties assess risk throughout the settlement process, in addition to the cost assessment and insurance limits issues that usually play a central role in data breach settlements.

Abe Melamed is a mediator at Signature Resolution.

[1] Citing Clemens, 48 F.4th at 158; Hutton v. Nat'l Bd. of Exam'rs in Optometry, Inc., 892 F.3d 613, 622 (4t Cir. 2018); Galaria, 663 F. App'x at 388-89; Lewert v. P.F. Chang's China Bistro, Inc., 819 F.3d 963, 967 (7th Cir. 2016); Equifax, 999 F.3d at 1262.