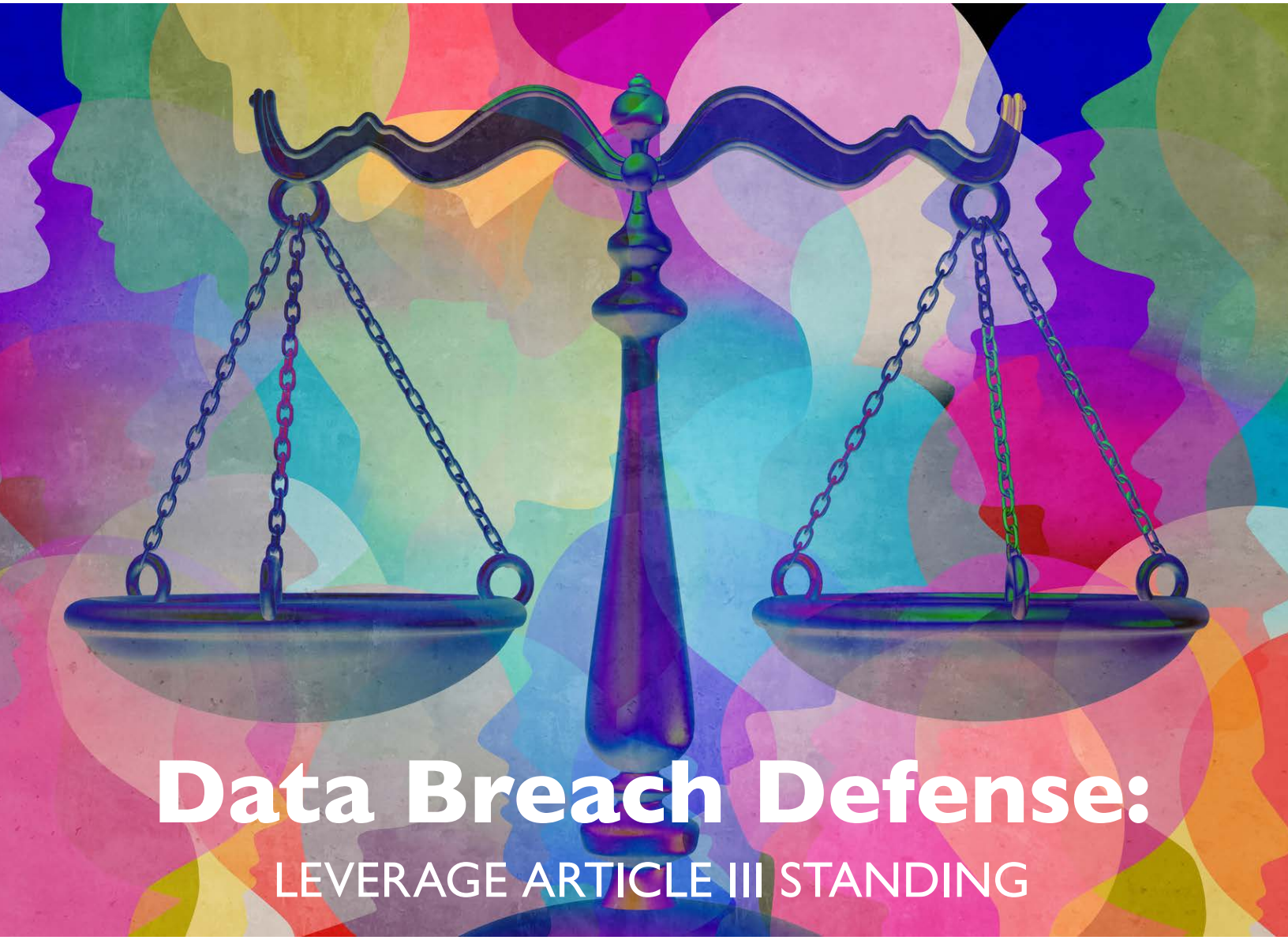
CBA Report
Cincinnati Bar Association
January/February 2021



Data Breach Defense:

LEVERAGE ARTICLE III STANDING

Data Breach Defense

Leveraging Article III standing defense to dispose of Sixth Circuit Data Breach Class Action suits

By David J. Oberly

Today, data breaches continue to proliferate at a rapid pace, often spurring consumer class action litigation in their wake. Oftentimes, a successful data breach suit can empty a corporate defendant's coffers. For example, Equifax was recently forced to shell out $575 *million* to settle a major data breach class action suit stemming from its 2017 mega-breach that impacted over 100 million individuals. Consequently, companies that handle consumer personal data must be prepared to forcefully defend such high-stakes, bet-the-company litigation.

Fortunately, Article III standing serves as a viable defense to obtain dispositive dismissals from a wide range of data breach class actions in federal court. While a current circuit split exists over the threshold for establishing standing in such cases, the standard articulated by the Sixth Circuit Court of Appeals provides a significant opportunity for defendants to completely dispose of litigation at the pleading stage based on an absence of constitutional standing.

Overview of Article III Standing

To establish Article III standing, a plaintiff must establish three core elements: (1) an injury-in-fact; (2) causation; and (3) a likelihood that the injury will be redressed by a favorable decision. To establish a cognizable injury-in-fact, a plaintiff must show that he or she suffered "an invasion of a legally protected interest" that is "concrete and particularized" and "actual or imminent, not conjectural or hypothetical." Where a plaintiff seeks to establish an injury-in-fact based on an imminent injury, that threatened injury must be "certainly impending."

In the context of data breach class action litigation, the question of whether Article III standing can be satisfied is often dispositive of the outcome of an action. However, a deep circuit split currently exists between the federal appellate courts regarding the level of proof required to establish standing in data breach class actions—particularly as it relates to demonstrating a sufficiently "concrete" injury-in-fact, and whether allegations of an increased risk of future identity theft are sufficient to satisfy this aspect of the standing test.

Article III Standing in the Sixth Circuit

The Sixth Circuit directly addressed the standard for establishing Article III standing in the data breach context in *Galaria v. Nationwide Mut. Ins. Co.*, 663 Fed. Appx. 384 (6th Cir. 2016), which represents the seminal data breach standing decision in the Sixth Circuit.

Galaria involved allegations that hackers infiltrated Nationwide's computer network and stole sensitive personal identifying information ("PII") of over 1.1 million individuals. On appeal, the Sixth Circuit held that the plaintiffs' allegations of a substantial risk of harm, coupled with reasonably incurred mitigation costs, were together sufficient to establish a cognizable concrete and particularized imminent injury to clear the Article III standing hurdle at the pleading stage of the litigation.

Importantly, the *Galaria* court's holding was based predominantly on the existence of proof that the plaintiffs' personal information had, in fact, been *stolen*, finding that "[t]here is no need for speculation *where Plaintiffs allege that their data has already been stolen and is now in the hands of ill-intentioned criminals*." The *Galaria* court held that the possibility of future injury in the form of a continuing, increased risk of fraud and identify theft went beyond mere speculation of "possible future injury" or "objectively reasonable likelihood of injury," both of which were found to be inadequate to confer standing pursuant to the U.S. Supreme Court's ruling in *Clapper v. Amnesty International USA*, 568 U.S. 398 (2013). This was so, according to the court, because "there is no need for speculation where Plaintiffs allege that their data *has already been stolen* and is now in the hands of ill-intentioned criminals."

Thus, pursuant to *Galaria*, the key factor to establishing—and defeating—standing in the Sixth Circuit turns on the existence of facts to show that an *actual theft of data* took place in connection with a data breach event.

For this reason, courts sitting in the Sixth Circuit have held that a plaintiff *cannot* establish Article III standing in the absence of any allegations that the plaintiff's data was *stolen* or otherwise *improperly acquired* in connection with a breach event.

For example, in *Williams-Diggins v. Mercy Health*, 2018 WL 6387409 (N.D. Ohio Dec. 6, 2018), the plaintiff alleged that Mercy Health's online platform caused patient data to be "publicly available" and to "*potentially* allow" unauthorized individuals or other third parties to acquire patients' medical information, which was sufficient to establish standing. The U.S. District Court for the Northern District of Ohio disagreed, finding instead that the plaintiff was precluded from establishing standing through his allegations that Mercy put his personal information at risk because it *could* have been acquired without permission by a third party. In doing so, the court noted that the "mere possibility" that the personal information "may have already been compromised or misused" was "*only a link in the 'speculative chain of possibilities' which might lead from Plaintiff's relationship with Defendant to the alleged harm for which he seeks to recover.*" "That possibility," the court concluded, "is *not* sufficient to confer standing."

A similar result was seen in *Oneal v. First Tennessee Bank*, 2020 WL 1352519 (E.D. Tenn. Mar. 15, 2018), a case involving claims that First Tennessee Bank allegedly accessed the plaintiff's credit report for a purpose not authorized by the Fair Credit Reporting Act ("FCRA"). In *Oneal*, the plaintiff attempted to establish standing by asserting that the bank's conduct increased the risk that he would be injured if the bank experienced a data breach because the bank had obtained his highly sensitive information and saved that data on its computer systems.

The court rejected these contentions, holding instead that the plaintiff's argument that the bank's credit inquiry exposed him to an increased risk of a data breach and a resulting exposure of his personal information to third parties failed to constitute a sufficient injury-in-fact to confer standing. Here, the court found that the plaintiff's allegations amounting to a hypothetical breach failed to plead a concrete risk of harm, noting that in the cases where courts *did* find standing had been established, at a minimum third-party hackers had already obtained access to the plaintiffs' confidential information. Conversely, the *Oneal* plaintiff's theory of standing failed because it was premised on a "probabilistic leap"—in that the plaintiff relied on a *potential* future data breach, which, if it ever occurred, might *potentially* result in identify theft or fraud." Like the *Williams-Diggins* court, the *Oneal* court characterized this theory as a "highly attenuated chain of possibilities" that was insufficient to constitute an injury-in-fact under *Clapper*.

In its analysis, the court highlighted the distinction between *Galaria* and the case at issue, which further supported the conclusion that Article III standing was lacking in *Oneal*. In *Galaria*, the court noted, a data breach had already occurred and—more importantly—the plaintiffs' credit information was "already in the hands of ill-intentioned criminals." The *Oneal* plaintiff, on the other hand, did not allege that the bank had suffered a data breach or that any third party had attempted to access his credit report—only that a breach of this nature was possible. Thus, because the plaintiff had failed to allege a substantial risk of a data breach involving the access or theft of his personal data, *Galaria* failed to support the plaintiff's claim of standing.

Analysis & Takeaways

Taken together, *Galaria* and subsequent decisions operate to create a clear dividing line between circumstances where standing might exist, and where it does not, in the Sixth Circuit.

Under *Galaria,* standing can often be established where plaintiffs are able to set forth facts supporting the conclusion that both a data breach incident took place *and*

the plaintiffs' data was actually accessed or stolen during the breach.

Conversely, where allegations are limited to only the existence of data compromise event, but no further evidence exists that the plaintiff's data was stolen or otherwise improperly acquired in connection with the breach, courts are likely to find that insufficient facts exist to confer Article III standing in connection with the breach incident.

Conclusion

To date, the Second, Third, Fourth, and Eighth Circuits have found allegations of an increased risk of future identity theft fall short of demonstrating a cognizable injury-in-fact in data breach class action litigation. Conversely, the Seventh, Ninth, Eleventh, and D.C. Circuits have all found such allegations sufficient to establish Article III standing in the breach context. The Sixth Circuit falls somewhere in the middle of these two camps, permitting an increased risk of future identity theft to confer standing, *but only* where those allegations are coupled with additional facts to demonstrate that the plaintiffs' personal data has been improperly acquired by the malicious actors who perpetrated the breach. Ultimately, this longstanding uncertainty regarding the level of proof required to establish standing will continue moving forward until a definitive ruling is handed down by the U.S. Supreme Court.

While standing will continue to remain a very fact-specific inquiry, the Sixth Circuit has provided businesses with a blueprint to procure an early exit from a wide range of data breach class action suits through the pursuit of an Article III standing defense. Corporate defendants that find themselves a target of a data breach class action suit in the Sixth Circuit should analyze the potential applicability of this defense at the outset of any litigation.

Pursuant to *Galaria* and subsequent decisions interpreting the seminal Sixth Circuit opinion, where a plaintiff's claims are limited to the mere fact that a breach event occurred, but no allegations are asserted that the plaintiff's data made its way into the "hands of ill-intentioned criminals," an early motion to dismiss under Federal Civil Rule 12(b)(1) should be pursued to dispose of the case at an early juncture. In particular, corporate defendants should highlight any absence of evidence that: (1) malicious actors actually accessed or acquired the data in question; (2) the breach was intentional or malicious; and (3) the data was misused, all of which demonstrate that the alleged injuries in question are not sufficient to meet the *Galaria* injury-in-fact standard established by the Sixth Circuit.

Oberly is an attorney in the Cincinnati office of Blank Rome LLP and is a member of the firm's Biometric Privacy, Privacy Class Action Defense, and Cybersecurity & Data Privacy groups. David's practice encompasses both defending clients in high-stakes, high-exposure biometric privacy, privacy, and data breach class action litigation, as well as counseling and advising clients on a wide range of biometric privacy, privacy, and data protection/cybersecurity matters. He can be reached at doberly@blankrome.com.