Lessons Learned From Eleventh Circuit's Dismissal of Data Breach Suit Alleging Only Increased Risk of Future Harm for Lack of Article III Standing

David J. Oberly
Blank Rome LLP

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

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.

Just recently, the Eleventh Circuit Court of Appeals weighed in on the issue and held that an increased risk of future identity theft faced by data breach victims, without more, does *not* satisfy the injury-in-fact prong of the standing analysis.

In addition to widening the current circuit split, the Eleventh Circuit's opinion also provides in-house counsel and privacy attorneys with several key lessons both on how to properly respond to breach incidents and effectively defend against the class action litigation that is often generated in the aftermath of a breach incident.

The case is *Tsao v. Captiva MVP Rest. Partners, LLC*, 986 F.3d 1332 (11th Cir. 2021).

Analysis of the Eleventh Circuit's Opinion

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. Where a plaintiff seeks to establish an injury-in-fact based on an imminent injury, that threatened harm must be "certainly impending." At the very least, this requires a showing that there is a "substantial risk" that the harm will occur.

To date, the Sixth, Seventh, Ninth, and D.C. Circuits have all held that an increased risk of future identity theft is sufficient to establish Article III standing in data breach class action litigation. Conversely, the Second, Third, Fourth, and Eighth Circuits have found such allegations fall short of demonstrating a cognizable injury-in-fact in the breach context.

Read more on page 32

Lessons... Continued from page 12

In *Tsao*, the Eleventh Circuit joined the latter camp in holding that an increased risk of future identity theft, without more, is insufficient to establish standing in data breach litigation.

Thus, arguments that data breach plaintiffs *could* suffer future injury from misuse of their personal information disclosed during a breach—but where no actual misuse has occurred—and the risk of misuse, by itself, are now foreclosed in the Eleventh Circuit pursuant to *Tsao*.

Takeaways & Practical Tips

Utilizing Successful Article III Injury-in-Fact Challenges to Defeat Data Breach Class Action Suits

While Article III standing will continue to remain a very fact-specific inquiry, the Eleventh Circuit has provided in-house counsel and privacy litigators 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.

"The Eleventh Circuit has provided in-house counsel and privacy litigators with a blueprint to procure early exit from a wide range of datta breach class actions..."

The *Tsao* court held that a plaintiff alleging a threat of future identity theft or other harm lacks Article III standing unless the hypothetical harm alleged is either certainly impending or there is a substantial risk of such harm taking place. Importantly, to make this showing a plaintiff must present evidence of at least some misuse of class members' data. According to the Eleventh Circuit, in the absence of such evidence, satisfying this standard for Article III standing will be "difficult to meet." Under *Tsao*, evidence of a mere breach will not, standing alone, satisfy the requirements of Article III standing for data breach plaintiffs in the Eleventh Circuit.

Further, if the future harm alleged is not certainly impending and there is no substantial risk of harm, a plaintiff cannot manufacture standing by inflicting a direct harm on himself/herself to mitigate a perceived risk.

Taken together—pursuant to *Tsao*—where a plaintiff's claims are limited to the mere fact that a breach occurred, but no allegations are asserted that any data involved in the breach was misused, an early motion to dismiss under Fed. R. Civ. P. 12(b)(1) should be pursued to dispose of the case at an early juncture. In particular, corporate defendants and their counsel should highlight: (1) the absence of any evidence that malicious actors actually accessed or acquired the data in question; (2) the absence of any evidence that data was misused; (3) that only compromised credit/debit card information—but no additional personal identifying information—was involved in the breach, thereby eliminating the ability of malicious parties to open unauthorized

new accounts; and (4) any subsequent action taken by the plaintiff to cancel his or her cards following disclosure of the breach, which effectively eliminates the risk of credit card fraud in the future—all of which illustrate that the alleged injuries in question are not sufficient to meet the *Tsao* injury-in-fact standard established by the Eleventh Circuit.

The Importance of Properly Handling Breach Notification

In addition, the *Tsao* opinion also showcases the critical role that breach notification can play in mitigating (or expanding) companies' data breach class action litigation exposure in the wake of a data security incident.

One of the major factors in the Eleventh Circuit's rejection of the plaintiff's "increased risk of future harm" theory was the absence of any factual allegations put forth by the plaintiff of actual misuse or unauthorized access relating to the personal data involved in the breach. Importantly, this inability to allege actual misuse/access was largely attributable to the language used by the defendant in its notice that was issued after learning of the breach—and, more specifically, the care taken to make clear in the notice that its customers' data "*may*" have been accessed.

Oftentimes, however, in the wake of a breach in-house counsel will fail to exercise this same level of care in selecting the precise wording to be used in the company's breach notice. Ordinarily, this will result in the over-notification of individuals impacted by the breach—namely, by affirmatively stating that personal data *was* accessed and/or acquired during the incident—when, in fact, the question of whether unauthorized access or acquisition *actually* took place remained unclear at the time the notice was issued.

Moreover, many state data breach notification laws may not even require notice in the first instance under similar circumstances, depending upon factors such as the state's definition of what constitutes a "breach" and whether the state provides a risk of harm analysis exemption that obviates the duty to provide notice where there is no material risk of harm to those individuals impacted by the breach.

Tsao serves as a key reminder of the important role that words play with respect to data breach notification in mitigating potential class action liability exposure. In most instances, in-house attorneys should contact experienced outside counsel who is well-versed in responding to breach events and the nuances of data breach class action litigation to ensure compliance with the law and adherence to other breach response best practices, including properly balancing the need for transparency and legal compliance with the risks of over-notification.

Conclusion

Data breaches are here to stay, despite even the most robust efforts to prevent security incidents.

Thus, companies and their in-house counsel must be in a position to quickly and *properly* respond to a breach event—including providing notice of the breach in a manner that is both transparent and mitigates potential class action liability exposure.

In addition, companies must also be prepared to aggressively defend data breach class action suits in the event the need arises. Corporate defendants that find themselves a target of data breach class action suit should analyze the potential applicability of an Article III standing defense at the outset of any litigation to determine whether a standing challenge can be pursued to extricate the company from the litigation at an early juncture. For companies who find themselves in litigation in the Eleventh Circuit, *Tsao* provides a helpful blueprint for designing a winning Article III standing defense where a lack of any evidence exists of any type of misuse of or access to the personal data of individuals impacted by a breach event.