Articles + Publications | March 5, 2021

Locke Lord QuickStudy: Standing on Thin Ice? New Guidance on Standing for Data Breach Claims

Locke Lord LLP

WRITTEN BY

Thomas J. Cunningham | Molly McGinnis Stine | Taylor Levesque

RELATED OFFICES

Dallas | West Palm Beach

Who has standing to bring claims for alleged statutory violations of privacy and cybersecurity statutes? There is no easy answer to this question. In *Spokeo, Inc. v. Robins*, the Supreme Court explained that just because a statute grants a plaintiff the right to sue under that statute, that *does not* necessarily mean the plaintiff has *standing* to bring that claim.[1] Instead, since *Spokeo*, the federal district courts and courts of appeals have grappled with what sets of alleged facts are sufficient to confer standing. In the data breach context, the question is even more difficult to answer due to the wide-ranging risks and injuries associated with a data breach.

This QuickStudy will address two related developments in the analysis of Article III standing in data breach cases. First, we discuss the newly adopted standard for analysis in the Eleventh Circuit at the inception of a data breach case. Second, we examine a pending Supreme Court case that will determine whether Article III or Rule 23 permit certification of a damages class when most of the prospective class members have suffered no injury.

Who is "Injured" by a Data Breach?

Shortly after a data breach, the extent of harm done is often unknown. Whether and to what degree individuals may be harmed in the future as a result of the breach is difficult to predict. The eventual impact of the data breach depends upon (1) the amount, categories, and sensitivity of information collected, (2) the breached entity's ability to limit or rehabilitate the disclosed information, as well as (3) the sophistication and intentions of the hacking entity. Rather than identifying traditionally "tangible" injuries, plaintiffs in data breach lawsuit often point to an increased risk of future harm (such as the fear of identity theft and addressing fraudulent transactions). So, in the data breach context, the question posed for the courts of appeals is what "risk" of possible future injury is enough to establish Article III standing? In February 2021, the Eleventh Circuit offered its opinion on this question.[2]

***Tsao v. Captiva MVP Rest. Partners, LLC* (11th Cir. 2021).**

In *Tsao v. Captiva MVP Rest. Partners, LLC*, a restaurant customer brought a class action complaint asserting a number of claims[3] against the restaurant "PDQ" following a data breach of PDQ's point of sale system. Plaintiff's class action complaint alleged that the hacker's breach of the point of sale system resulted in numerous alleged injuries to the putative class. These alleged injuries were divided into two separate categories. Injuries the plaintiff had already suffered can be thought of as "Category 1" injuries. Injuries the plaintiff might suffer in the

©2026 Troutman Pepper Locke

future, and the existing risk that those injuries might be realized, can be thought of as "Category 2" injuries.

The bulk of the Eleventh Circuit's opinion deals with plaintiff's theory of standing based on Category 2—the "elevated risk" of injury. However, the court's framing of the alleged injuries in two separate categories provides insight as to how courts of appeals are analyzing plaintiffs' factual allegations in support of standing in the data breach context.[4] The Eleventh Circuit ultimately denied both standing theories, but for different reasons.

Category 1 — Injury he *already* suffered: "[M]itigation injuries—for example, lost time, lost rewards points, and loss of access to accounts . . . ."[5]

As to alleged injuries *already* suffered, the Eleventh Circuit quickly dismissed arguments regarding injury based on plaintiff's mitigation efforts. The court concluded "[t]he mitigation costs [plaintiff] alleges are inextricably tied to his perception of the actual risk of identity theft . . . ." Plaintiff voluntarily cancelled his own credit cards, and "[plaintiff] cannot conjure standing here by inflicting injuries on himself to avoid an insubstantial, non-imminent risk of identity theft."[6]

Category 2 — Injuries he *might* suffer: "[H]e could suffer future injury from misuse of the personal information disclosed during ?the cyber-attack (though he has not yet) . . . ."?[7]

The Eleventh Circuit began its substantive analysis of standing under the theory of "substantial risk of identity theft" and "increased risk of identity theft" by outlining the current state of the circuit split for standing in the data breach context. "Although this Circuit has not addressed the issue head-on, a number of our sister circuits have, and they are divided[:]"

Plaintiff *Can* Establish Standing Based on Increased Risk: Sixth Circuit; Seventh Circuit; Ninth Circuit; D.C. Circuit

Plaintiff *Cannot* Establish Standing Based on Increased Risk: Second Circuit; Third Circuit; Fourth Circuit; Eighth Circuit[8]

At a high-level, the Eleventh Circuit attempted to reconcile the split by noting "the cases conferring standing after a data breach based on an increased risk of theft or misuse included at least some allegations of actual misuse or actual access to personal data."[9] This commentary suggests the Eleventh Circuit favors the application of an "increased risk *plus*" type of test in determining standing in the data breach context. Although the court offered no name for the type of analysis it conducted, the opinion reveals the implied application of an "increased risk *plus*" test. The opinion discusses "[t]hree considerations" that "color [the court's] conclusion" plaintiff has not "met his burden to show that the [sic] there is a 'substantial risk' of harm, or that such harm is 'certainly impending.'"[10]

Specifically, the Eleventh Circuit determined plaintiff's allegations were not sufficient to confer standing because (1) plaintiff's reports outlining the risks and statistics associated with identify theft were "conclusory allegations" that "do nothing to clarify the risks to the plaintiffs *in this case*";[11] (2) plaintiff does not provide "specific evidence of *some* misuse of class members' data";[12] and (3) plaintiff's immediate cancellation of his credit cards following

PDQ's disclosure of the data breach "eliminate[ed] the risk of credit card fraud" and the "risk of future harm involving identity theft . . . is not substantial and is, at best speculative."[13]

The court summed up its analysis by stating "[i]n short, [plaintiff] Tsao has not alleged either that the PDQ data breach placed him at a 'substantial risk' of future identity theft or that identity theft was 'certainly impending.' Evidence of a mere data breach does not, standing alone, satisfy the requirements of Article III standing."[14] The Eleventh Circuit's analysis in *Tsao* provides another helpful marker for when standing exists in the data breach context and establishes how the issue will be analyzed by district courts in that circuit.

While the *Tsao* decision establishes the standard by which standing in data breach cases will be reviewed in the Eleventh Circuit at the threshold of a case, a related issue in the context of class certification will be addressed by the Supreme Court this term. Even if an individual plaintiff has standing to bring a claim, how should courts analyze the standing of prospective class members when determining whether a damages class should be certified pursuant to Federal Rule of Civil Procedure 23(b)(3) for damages?

Who Should be Included in a Class in the Data Breach Context?

In the class action context (common for statutory privacy and cybersecurity claims), the stakes are high for both plaintiffs and defendants as class action lawsuits based on statutory violations can include significant claims for statutory damages. In late February 2021 alone, there have been several marquee examples. On February 25, 2021, plaintiffs in a multidistrict litigation based on alleged violations of the Illinois Biometric Information Privacy Act sought preliminary approval of a settlement agreement involving TikTok for $92 million.[15] On February 26, 2021, the Northern District of California issued an order granting final approval for a $650 million settlement with Facebook—up $100 million from Facebook's 2020 proposal of $550 million that the judge deemed inadequate.[16] In the order finally approving the Facebook settlement, the judge stated the $650 million figure was a "landmark result" and "one [of] the largest settlements ever for a privacy violation."[17]

With the high exposure to liability due to the aggregation of multiple statutory penalties in a class action, defendants need clarity as to how a court will analyze the standing of absent class members in the data breach context. Fortunately, the Supreme Court recently granted certiorari in a Ninth Circuit case that should provide that clarity. The forthcoming decision should help guide federal courts in addressing whether a class can be certified and who may be included in a data breach class.

Supreme Court Guidance? *TransUnion v. Ramirez*, Supreme Court Case No. 20-297.

In December 2020, the Supreme Court granted certiorari in *Ramirez v. TransUnion LLC*.[18] Oral argument is scheduled for March 30, 2021, and a decision is likely to issue by the end of the Supreme Court's term in June 2021. In *Ramirez*, the Court will consider whether either Article III or Rule 23 permit certification of a damages class where the vast majority of the class suffered no actual injury, let alone an injury anything like what the class representative suffered.

Awaiting an answer to this question, one federal court has already stayed its data breach case pending a decision from the Supreme Court.[19]

While the Supreme Court's decision may provide some guidance, it is not likely to resolve every future standing decision. Parties will look to distinguish any given case on the alleged harm identified by a plaintiff, by the specifics of the statute at issue, and more. That said, it will be helpful if the Supreme Court decision provides more clarity around the issues.

Conclusion

Moving forward, plaintiffs and defendants will need to continue to stay aware of the recent developments in federal court cases across the country analyzing Article III standing under the increasing number of privacy and cybersecurity statutes. The facts that may support standing in the data breach context differ from the facts that may support standing for alleged privacy violations under specific statutes such as the Illinois Biometric Privacy Act. Understanding the facts and outcomes of the recent cases from the courts of appeals—and considering the Supreme Court's forthcoming ruling in *Ramirez*—will allow parties to analogize their facts to cases with favorable results and better predict how a district court or court of appeals may evaluate similar sets of facts.

For more information on the matters discussed in this Locke Lord QuickStudy, please contact the authors.

—

1. *Spokeo, Inc. v. Robins*, —– U.S. ——–, 136 S. Ct. 1540, 1547-48 (2016) (quoting *Raines v. Byrd*, 521 U.S. 811, 820 n.3 (1997)).
2. *Tsao v. Captiva MVP Rest. Partners, LLC*, 986 F.3d 1332 (11th Cir. 2021).?
3. The six (6) claims asserted include breach of implied contract, negligence, violation of Section ?5 of the Federal Trade Commission Act, unjust enrichment, declaratory judgment, and violation of ?the Florida Unfair and Deceptive Trade Practices Act.
4. Before beginning its formal analysis, the Eleventh Circuit characterized plaintiff's appellate briefing ??"as mostly retread[ing] the arguments he made below—that he and the class are at an elevated ?risk of future identity theft and that he lost cash back and rewards point, time, and account ?access—in an effort to satisfy Article III's standing requirement." *Tsao*, 986 F.3d at 1337.
5. *Id.* at 1337.
6. *Id.* at 1345.
7. *Id.* at 1337.
8. *Id.* at 1340.
9. *Id.*
10. *Id.* at 1343. *(quoting Clapper v. Amnesty Int'l USA, 568 U.S. 398, 409 (2013)).*
11. *Id.* at 1343 (citing *Muransky v. Godiva Chocolatier, Inc.*, 979 F.3d 917, 933 (11th Cir. 2020) (en banc)).
12. *Id.* at 1343-44 (noting, however, that some "sister Circuits have recognized [that] evidence of actual misuse is not necessary for a plaintiff to establish standing following a data breach.").
13. *Id*. at 1344.
14. *Id.* (internal citation omitted).
15. *In re: TikTok, Inc., Consumer Privacy Litig.,* 1:20-cv-04699 (N.D. Ill.), MDL 2948, Plaintiffs' Motion for

Preliminary Approval of Class Action
Settlement,
https://www.docketalarm.com/cases/Illinois_Northern_District_Court/1–20-cv-04699/In_Re–_TikTok_Inc._Consumer_Privacy_Litigation/122/.
16. *Patel v. Facebook, Inc.*, No. 3:15-cv-03747 (N.D. Cal.), Order re Final Approval, Attorneys' Fees and Costs, and Incentive
Awards,
https://www.docketalarm.com/cases/California_Northern_District_Court/3–15-cv-03747/In_re_Facebook_Biometric_Information_Privacy_Litigation/537/.
17. *Id.*
18. *Ramirez v. TransUnion LLC*, 951 F.3d 1008 (9th Cir. 2020), cert. granted in part sub nom., *TransUnion LLC v. Ramirez*, No. 20-297, 2020 WL 7366280 (U.S. Dec. 16, 2020).
19. *Stoll v. Musculoskeletal Inst., Chartered,* 2021 WL 632622, at *2 (M.D. Fla. Feb. 18, 2021) ??("[T]he parties would benefit significantly from the Supreme ?Court's ruling in litigating the issue ?as to whether a class can be certified and who may be included within that class.").?

RELATED INDUSTRIES + PRACTICES

- Data + Privacy
- Privacy + Cyber