KILPATRICK
TOWNSEND

November 25, 2020

Data Breach Class Actions – Eleventh Circuit En Banc Decision Could be Bad News for Plaintiffs

by Jeffrey H. Fisher

Takeaway: The Eleventh Circuit has yet to address whether a future risk of identity theft is sufficient to establish standing in a data breach case. In *Muransky v. Godiva Chocolatier, Inc*., 16-16486, 2020 WL 6305084, at *12 (11th Cir. Oct. 28, 2020), the en banc Eleventh Circuit held that the plaintiff failed plausibly to allege that a risk of future identity theft flowing from a violation of the Fair and Accurate Credit Transactions Act (FACTA) constituted a material risk of harm sufficient to establish Article III standing. Although *Muransky* is not a data breach case, it could be bad news for data breach plaintiffs. *Muransky* suggests that the Eleventh Circuit will carefully scrutinize future injury allegations and require data breach plaintiffs to satisfy a relatively high bar to establish standing.

Muransky Facts and Holding

The allegations, holding, and unique procedural posture of *Muransky* have been discussed in numerous articles. This article focuses on the allegations and rulings relevant to the standing issue of future injury.

Muransky received a receipt from a Godiva store that revealed the first six and last four digits of his credit card number. FACTA prohibits merchants from printing more than the last five digits on a receipt. Muransky filed a FACTA class action and – with the Supreme Court about to issue its standing decision in *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540 (2016) – the parties agreed to a class settlement. But after the Supreme Court issued its ruling in *Spokeo*, class members objected to the settlement, including for lack of standing. Without considering *Spokeo*, the district court concluded it had jurisdiction and approved the settlement. On appeal, an Eleventh Circuit panel affirmed, finding that Muransky had satisfied Article III standing under *Spokeo*. The Eleventh Circuit, however, vacated that panel decision, ordering rehearing en banc on the standing issue.

In a 7-3 decision, the en banc Eleventh Circuit held – over three strident dissenting opinions – that Muransky lacked standing. The majority opinion, penned by Judge Britt Grant, concluded that "[a]lthough the receipt violated the law because it contained too many digits, Muransky has alleged no concrete harm or material risk of harm stemming from the violation." 2020 WL 6305084, at *15. The opinion rejected the panel's conclusion that it was required to accept Congress' assessment of injury. *Id*. at *4. Judge Grant further explained that, although Godiva violated FACTA, it was up to the district court to determine whether the harm caused by that violation was concrete or "real." *Id*. at *5. "So although a congressional judgment may be 'instructive and important' to this Court's analysis, we need to come to our own conclusion that the alleged harm is concrete before we can find that a plaintiff has standing." *Id*.

Whether Muransky suffered harm largely turned on the court's assessment of his future risk of injury. Like many data breach plaintiffs, Muransky could not allege that his identity had actually been stolen. Instead, he alleged only that Godiva's violation "exposed him to an increased risk of identity theft." *Id*. The court explained that "[e]ven without any direct harm, a plaintiff can establish an injury in fact by showing that a statutory violation created a 'risk of real harm.'" *Id*. at *7 (quoting *Spokeo*, 136 S. Ct. at 1549 (citing *Clapper v. Amnesty Int'l USA* , 568 U.S. 398, 416 (2013))). "But while very nearly any level of direct injury is sufficient to show a concrete harm, the risk-of-harm analysis entails a more demanding standard—courts are charged with considering the magnitude of the risk." *Id*. "[C]ases use slightly different formulations to describe a significant or substantial risk, but they are consistent in recognizing a high standard for the risk-of-harm analysis, and a robust judicial role in assessing that risk." *Id*.

The court then evaluated whether Muransky could show that the printing of extra digits on his credit card number "posed a material risk of harm." *Id*. at *8. It found he had not. *Id*. at *12. The court ruled that Muransky's allegations of harm did not "establish a risk that is substantial, significant, or poses a realistic danger." *Id*. Notably, the complaint included scant injury allegations. Muransky alleged only that he "and members of the class continue to be exposed to an elevated risk of identity theft." He provided no indication of "how much risk this might be," and no "insight into what degree of 'elevated risk' Muransky faced, or why." *Id*. The court concluded that Muransky's "conclusory" and "threadbare" allegations failed to meet the high burden of demonstrating a risk of future harm. *Id*.

Application to Data Breach Cases

The Eleventh Circuit's factually-intensive approach is broadly consistent with the approach of federal appellate courts considering risk of future injury in data breach cases. The Sixth, Seventh, Ninth, and D.C. Circuits have found allegations of future injury sufficient to establish standing, while the Third, Fourth, and Eighth Circuits have found future injury allegations insufficient. *See In re SuperValu, Inc*., 870 F.3d 763, 769 (8th Cir. 2017) (collecting cases). But as the Eighth Circuit noted in *Supervalu*, these cases "ultimately turned on the substance of the allegations before the court." *Id*. In *Supervalu*, the court found no standing where the allegedly stolen information did not include personally identifying information like social security numbers, birth dates or driver's license numbers, and there was no evidence that any of the stolen information had been used. In *Attias v. Carefirst, Inc*., 865 F.3d 620, 628 (D.C. Cir. 2017), on the other hand, the complaint alleged theft of personally identifying information, including social security numbers. And in *Remijas v. Neiman Marcus Grp., LLC*, 794 F.3d 688, 690 (7th Cir. 2015), and *Krottner v. Starbucks Corp*., 628 F.3d 1139, 1141 (9th Cir. 2010), at least one of the class members had actually experienced identity theft. District courts in the Eleventh Circuit have similarly split depending on the quality and nature of the injury allegations. *Compare Provost v. Aptos, Inc*., 1:17-CV-02120-ELR, 2018 WL 1465766, at *6 (N.D. Ga. Mar. 12, 2018) (finding future injury allegation speculative where breach did not expose social security numbers and plaintiff alleged only one fraudulent charge that occurred two years ago) *with In re 21st Century Oncology Customer Data Sec. Breach Litig.*, 380 F. Supp. 3d 1243, 1256 (M.D. Fla. 2019) (finding plaintiff had demonstrated standing based on increased risk of identity theft where breach exposed plaintiff's social security number and numerous class members had experienced fraudulent charges).

The allegations of future injury in *Muransky* would certainly fall on the weak end of the spectrum in a data breach case. First, while every data breach case involves at least allegations of theft by criminal actors, there was no of theft – or even exposure – of Muransky's receipt (the receipt was provided to him and no one else). Second, unlike in *Carefirst*, where the plaintiff alleged theft of personally identifiable information like social security numbers, Muransky's entire credit card account number was not even printed, only the first 6 and last 4 digits. And third, Muransky did not allege that he or any other class member had experienced identity theft as a result of Godiva's FACTA violation.

Importantly, and in contrast to most data breach plaintiffs, Muransky made little effort to even plead injury. Instead, the core of Muransky's claim was that he should have standing because Godiva violated FACTA (entitling him to statutory but not actual damages), an issue not relevant in most data breach cases.

But that does not mean *Muransky* is irrelevant to the standing issue in data breach cases. The dissenting opinions attacked the majority opinion from a policy perspective, asking why plaintiffs should have to wait until their data is stolen to successfully assert a claim. *Muransky*, 2020 WL 6305084, at *33 (Jordan, J. dissenting). They also criticized the majority for requiring an unrealistic amount of factual support at the pleading stage and for taking an unpredictable, "I know it when I see it" approach to standing. *Id*. The Eleventh Circuit's insistence on detailed factual allegations at the pleading stage and explicit adoption of a "high standard" and "robust judicial role" in evaluating standing will likely make it more difficult for data breach plaintiffs to successfully plead standing based on an increased risk of future injury.

Conclusion

Muransky is certainly not dispositive of the Eleventh Circuit's view of future injury standing in data breach cases. Whether the Eleventh Circuit ultimately finds standing will likely depend on the quality of the class plaintiff's injury allegations, including the nature of the information stolen and whether there is any indication of misuse. But *Muransky* makes clear that district courts in the Eleventh Circuit will scrutinize allegations of future risk of injury, and that data breach plaintiffs seeking to rely on an increased future risk of injury alone will face an uphill battle.