Kilpatrick

January 13, 2020

Data breach class actions – Georgia Supreme Court finds allegations of imminent risk of identity theft sufficient to create standing

by Jeffrey H. Fisher

Takeaway: A key issue in data breach litigation is whether a data breach plaintiff has alleged facts sufficient to establish a cognizable injury. In *Collins v. Athens Orthopedic Clinic, P.A.*, S19G0007, 2019 WL 7046786 (Ga. Dec. 23, 2019), the Georgia Supreme Court, reversing the Court of Appeals, ruled that the plaintiffs had standing where they alleged that the criminal theft of personal data left them at imminent and substantial risk of identity theft, Although Collins makes Georgia plaintiffs less vulnerable to a threshold (motion to dismiss) standing attack, the decision also includes a silver lining for data breach defendants.

In *Collins*, three class plaintiffs filed a putative class action against an orthopedic clinic (Athens Orthopedic Clinic, P.A.), alleging that a criminal hacker – the "Dark Overlord" – stole personally identifiable information, including Social Security Numbers, belonging to the clinic's current and former patients. According to the complaint, at least some of this personal data had already been made available for sale on the "dark web" or otherwise posted on a data storage website. Alleging that the clinic failed to take reasonable steps to prevent the hack, the plaintiffs sought class certification, alleging claims for negligence, breach of implied contract, unjust enrichment, injunctive relief under the Georgia Uniform Deceptive Trade Practices Act, and declaratory relief.

In June 2018, a divided Georgia Court of Appeals affirmed the trial court's grant of the clinic's motion to dismiss, concluding that allegations of increased risk of identity theft were insufficient to establish a cognizable injury. *Collins v. Athens Orthopedic Clinic*, 347 Ga. App. 13, 18, 815 S.E.2d 639, 645 (2018). The Court of Appeals further found that the time and money spent on precautionary measures, like identify theft protection, credit freezes, and credit monitoring, were not recoverable damages. The Court of Appeals agreed with the trial court that, because plaintiffs failed to allege a cognizable injury, each of their claims failed as a matter of law. *Id*.

The Georgia Supreme Court reversed and remanded, ruling that plaintiffs' allegations concerning the criminal theft of their personal data created an imminent and substantial risk of identity theft sufficient to establish cognizable injury. The court distinguished cases—relied on by the Court of Appeals—holding that allegations of increased risk of harm generally do not suffice. Collins, 2019 WL 7046786, at *4 (considering *Rite Aid of Georgia v. Peacock*, 315 Ga. App. 573, 726 S.E.2d 577 (2012), and *Finnerty v. State Bank & Trust Co.,* 301 Ga. App. 569, 572 (4), 687 S.E.2d 842 (2009)).

The Georgia Supreme Court observed that *Finnerty* and *Rite Aid* were decided at the summary judgment and class certification stages, where the submission of evidence was required. 2019 WL 7046786, at *4. *Collins*, on the other hand, was adjudicated on a motion to dismiss. The court therefore had to take as true the plaintiffs' allegation that the risk of identity theft was "imminent and substantial." *Id*. at *5. Also, the court concluded that the plaintiffs' allegations that their data had been stolen by a specific criminal hacker for the express purpose of selling the data made it highly plausible that the risk of identity theft was high. *Id.* at *5. Noting that its conclusion did not turn on whether the plaintiffs had to spend money to mitigate the data breach, the court said that plaintiffs' "allegation that the criminal theft of their personal data has left them at an imminent and substantial risk of identity theft is sufficient at this stage of the litigation." *Id*. at *6.

Although this standing ruling is potentially bad news for data breach defendants, the opinion contains a silver lining. First, the Georgia Supreme Court's ruling is expressly limited to the motion to dismiss stage in a Georgia state court. The outcome may have been different in federal court, which the Supreme Court acknowledged has stricter pleading requirements. *Id*. at *8 (noting "the more stringent pleading standards governing federal cases"). And to survive summary judgment, plaintiffs will need to support their risk of injury claims with evidence. The court also pointed out that proving an imminent and substantial risk of identity theft will be more difficult as more time passes after a breach and a plaintiff still has not suffered identity theft. The Collins breach, for example, took place more than three years ago, in June 2016.

Furthermore, the Collins court did not disturb its recent ruling, in *Georgia Department of Labor v. McConnell*, 305 Ga. 812, 815-816, 828 S.E.2d 352 (2019), that there is no common law duty to safeguard personal information. The *Collins* court explained that the "easier showing of injury" to establish standing "may well be offset by a more difficult showing of breach of duty." 2019 WL 7046786, at *6. It cited *McConnell* with approval and made it clear that because "the Court of Appeals' decision did not turn on" any issue of duty or breach of duty, it was leaving any discussion of duty "for another day." Id. And the court signaled that legislative intervention would be appropriate, because "traditional tort law is a rather blunt instrument" to address data breach cases and suggesting that "the legislative process" may be better suited to resolve "all of the complex tradeoffs" at issue. *Id*. at n.7. But until the court or legislature acts, *McConnell* remains a significant obstacle for any Georgia data breach plaintiff.

Finally, there are important limitations to the court's holding. The plaintiffs in *Collins* specifically alleged that their most sensitive data, including social security numbers, was stolen by the Dark Overlord. They also alleged that some of the data had already been offered for sale on the dark web and otherwise posted on a data storage website. The court found that these allegations put the case "much further along in the chain of inferences" necessary to conclude the plaintiff "likely will suffer identify theft." *Collins*, 2019 WL 7046786 at *5. In other words, allegations of an imminent risk of identity theft may not be enough to establish injury where less sensitive data is taken and where there are no allegations identifying who perpetrated the hack or what the hacker planned to do with the stolen data.