

June 20, 2023

Data breach class actions: Eleventh Circuit rules that an employer has a common law duty under Georgia law to safeguard employees' personal data

by [James F. Bogan III](#)

Takeaway: We have written several articles about the development of Georgia common law in data breach litigation. In one article, we discussed the Georgia Supreme Court's decision in *Department of Labor v. McConnell*, 305 Ga. 812, 828 S.E.2d 352 (2019), where it held that the Georgia Department of Labor did not owe a common law duty to an individual to protect his personally identifiable information (PII)—including his social security number—from accidental disclosure. See [Data Breach Class Actions—Georgia Supreme Court Rejects Duty to Safeguard Personal Information](#) (June 28, 2019). In another article, we discussed the Georgia Supreme Court's decision in *Collins v. Athens Orthopedic Clinic, P.A.*, 307 Ga. 555, 837 S.E.2d 310 (2019), where it ruled that the data breach plaintiffs had suffered a cognizable injury—and thus had standing—where they alleged that the criminal theft of their personal data created an imminent and substantial risk of identity theft. See [Data breach class actions—Georgia Supreme Court finds allegations of imminent risk of identity theft sufficient to create standing](#) (Jan. 13, 2020). In a recent case, *Ramirez v. Paradies Shops, LLC*, --- F.4th ---, No. 22-12853, 2023 WL 3813881 (11th Cir. June 5, 2023), the Eleventh Circuit charted its own path, distinguishing the *McConnell* and *Collins* decisions and ruling that the employer in that case had a common law duty to protect the PII of present and former employees.

As with most modern-day employees, when Carlos Ramirez went to work for Hojejj Branded Foods (HBF) in 2007, he provided his PII—including his social security number—to HBF as a condition of his employment. *Ramirez*, 2023 WL 3813881, at *1. After he left HBF, Paradies Shops, LLC (Paradies), acquired HBF.

In 2020, Paradies suffered a ransomware attack in which hackers stole the social security numbers of its current and former employees. In 2021, Ramirez learned that pandemic unemployment assistance claims—which required the disclosure of social security numbers—had been filed in his name in Kentucky and Rhode Island. *Id.* Several months later, Ramirez received notice from Paradies that his PII had been exfiltrated in the 2020 ransomware attack (which pre-dated the filing of the false unemployment assistance claims in his name). *Id.*

Ramirez then filed a putative class action against Paradies, alleging claims including negligence and breach of implied contract. Paradies moved to dismiss, arguing that it did not owe a duty to Ramirez to safeguard his PII under Georgia law for purposes of the negligence claim, and further arguing that Ramirez had failed to allege that there was an implied contract between Paradies and Ramirez to safeguard his PII. *Id.* at *2.

The Northern District of Georgia granted Paradies' motion to dismiss. On appeal, an Eleventh Circuit panel reversed the dismissal of Ramirez's negligence claim but affirmed the dismissal of the implied contract claim. *Id.* at *1, 5.

In analyzing whether a duty to safeguard information exists under Georgia law, the panel distinguished the “no duty” ruling in *McConnell*. According to the panel, *McConnell* focused on a prior ruling by the Georgia Supreme Court, *Bradley Center v. Wessner*, 250 Ga. 199, 296 S.E.2d 693 (1982), concluding that *Bradley* was based on a “special relationship” between the parties in that case and that *Bradley* provided no support for the existence of a duty on the part of the Department of Labor to safeguard an individual's PII. As the panel saw it, *McConnell* “declined to consider whether a duty might arise from any other . . . common law source [apart from *Bradley*], as no such argument had been made in that case.” *Ramirez*, 2023 WL 3813881, at *3.

The panel also distinguished the Georgia Supreme Court's ruling in *Collins*, where the court “recognized a cognizable injury where a criminal theft of the plaintiffs' personal data allegedly put them at an imminent and substantial risk of identity theft” but did not address the breach of duty issue. *Id.* Accordingly, the panel examined other Georgia common law sources to determine whether Paradies owed a duty to Ramirez to protect his PII.

Quoting an earlier decision by the Georgia Supreme Court, the panel ruled that “[t]raditional negligence principles provide that the creator of a potentially dangerous situation has a duty to do something about it so as to prevent injury to others . . . that is, the creator has a duty to eliminate the danger or give warning to others of its presence.” *Id.* (quoting *City of Winder v. Girone*, 265 Ga. 723, 723–24, 462 S.E.2d 704, 705 (1995)). The scope of that duty, however, is “generally limited to reasonably foreseeable risks of harm.” *Id.* at *4 (quoting *Maynard v. Snapchat, Inc.*, 313 Ga. 533, 537 n.3, 870 S.E.2d 739, 745 n.3 (2022)). The panel further observed that “while the intervening criminal act of a third person will often insulate a defendant from liability for an original act of negligence, that rule does not apply when the defendant had reason to anticipate the criminal act.” *Id.*

Based on those principles, the panel found that Ramirez had adequately alleged a cognizable duty as well as reasonable foreseeability, further agreeing with Ramirez that “the district court asked for too much specificity at the pleading stage.” *Id.*

As for duty, and examining the allegations in Ramirez's complaint, the panel concluded that Paradies owed a duty to safeguard the PII of present and former employees, based on their “special relationship.” *Id.* As Ramirez alleged, employers are required to obtain their employees' PII for business and tax purposes; employees are required to disclose their PII as a condition of employment; and Paradies created a potentially dangerous situation to that group by storing PII in an unsecured database. The panel further observed that “employers are typically expected to protect their employees from foreseeable dangers related to their employment.” *Id.*

The panel further determined that Ramirez had adequately alleged foreseeability: “Drawing on our judicial experience and common sense, we can reasonably infer that a company of Paradies's size and sophistication—especially one maintaining such an extensive database of prior employees' PII—could have foreseen being the target of a cyberattack.” *Id.* The panel further criticized the district court's ruling that Ramirez had failed to

adequately allege foreseeability: “We cannot expect a plaintiff in Ramirez’s position to plead with exacting detail every aspect of Paradies’s security history and procedures that might make a data breach foreseeable, particularly where ‘the question of reasonable foreseeability of a criminal attack is generally for a jury’s determination rather than summary adjudication by the courts.’” *Id.* at *5.

The panel concluded that “Ramirez has sufficiently pled the existence of a special relationship and a foreseeable risk of harm” and that “Georgia’s traditional negligence principles are flexible enough to cover Ramirez’s allegations.” *Id.* But the panel affirmed the dismissal of the implied contract claim, “agree[ing] with the district court that Ramirez failed to allege any facts from which we could infer HBF agreed to be bound by any data retention or protection policy.” *Id.*