

January 29, 2020

Georgia Identity Theft on the Court's Mind

BY:

As the ever-expanding Digital Age inserts itself into more and more facets of our lives, the possibility of our personal data being obtained through illegal methods exponentially increases. Data hackers targeting sensitive and confidential medical records have become a serious dilemma for patients. It seems logical that medical entities should be held responsible for failing to adequately protect a patient's electronic medical records. Yet, what legal recourse does a patient have against a medical entity when their sensitive personal data has been hacked if they are unable to prove that their personal data has fallen into criminal hands or were used against the patient in some tangible way? The Supreme Court of Georgia addresses this issue in their recent decision styled *Collins et al. v. Athens Orthopedic Clinic, P.A.*

Back in June of 2016, an anonymous hacker successfully infiltrated the Athens Orthopedic Clinic's (hereinafter the "Clinic") computer database and stole personal identifiable information from over 200,000 current and former patients. This stolen information included Social Security numbers, personal addresses, dates of birth, and health insurance details. The hacker demanded a ransom, but the Clinic refused to pay. In turn, the hacker offered some of the personal data on the "dark web" and made some of the personal data temporarily available on the data-storage website Pastebin. The Clinic informed the patients of this breach in August of 2016.

The plaintiffs, all of which are current or former patients of the Clinic that had their personal data breached, filed a class action lawsuit against the Clinic for negligence, breach of implied contract, and unjust enrichment. The class sought damages based on costs related to credit monitoring and identity theft protection, as well as attorneys' fees. They also sought injunctive relief under the Georgia Uniform Deceptive Trade Practices Act, OCGA § 10-1-370 et seq. ("UDTPA"), and a declaratory judgment to the effect that the Clinic must take certain actions to ensure the security of class members' personal data in the future.

A divided panel in the Court of Appeals of Georgia granted the Clinic's motion to dismiss finding that the class sought "only to recover for an increased risk of harm," and therefore, lacked standing. *Collins v. Athens Orthopedic Clinic*, 347 Ga. App. 13 (2018). While the majority opinion recognized that credit monitoring and other precautionary measures requested by plaintiffs were "undoubtedly prudent," they were still insufficient claims since "prophylactic measures such as credit monitoring and identity theft protection and their associated costs, which are designed to ward off exposure to future, speculative harm, are insufficient to state a cognizable claim under Georgia law." *Id.* at 18. Judge McFadden, who concurred in part, dissented from the holding that the plaintiffs' did not have standing to bring their claims for future injury based on a substantial showing that harm would occur. *Id.* 22–25.

The majority decision in the Court of Appeals was largely based on two of its former opinions styled *Finnerty v. State Bank and Trust Co.*, 301 Ga. App. 569 (2009) and *Rite Aid of Ga. v. Peacock*, 315 Ga. App. 573 (2012). In *Finnerty*, the defendant filed a counterclaim alleging that the plaintiff bank wrongfully included his social security number in an exhibit to the complaint. The *Finnerty* court held that any alleged injury was "wholly speculative" because the defendant "failed to demonstrate that the Bank's purported unlawful disclosure made it 'probable' that he would suffer any identity theft or that any specific persons actually have accessed his confidential personal information as a result of the purported unlawful disclosure." *Id.* at 572. In *Rite Aid*, the court rejected class certification partially because the named plaintiff could only speculate that a criminal *might* associate with an employee of the new pharmacy who had access to his prescription information.

The Supreme Court of Georgia reversed the holding of the Court of Appeals ruling that plaintiffs' had standing for their claims of future injury. First, the Supreme Court that the *Finnerty* and *Rite Aid* decisions relied on by the Court of Appeals were not issued in the context of a motion to dismiss—they were based on a summary judgment case and question of class certification, respectfully. In Georgia, a motion to dismiss is properly granted when a plaintiff would not be entitled to relief under any state of provable facts asserted in support of the allegations in the complaint and could not possibly introduce evidence within the framework of the complaint sufficient to warrant a grant of the relief sought. As the plaintiffs in this matter alleged that criminals assumed their identities fraudulently and that the risk of such identity theft is "imminent and substantial," these allegations were taken as true for defeating the motion to dismiss.

And second, unlike in *Finnerty* and *Rite Aid*, the plaintiffs in this matter alleged that their personal data was stolen by criminals whose purpose was to sell and/or ransom the personal data. The Supreme Court recognized that this matter was factually distinguished from *Finnerty* and *Rite Aid* because it would have taken a "long series of speculative inferences" to find that those respective plaintiffs would have had their personal data illegally used. The Supreme Court recognized that the plaintiffs in this matter would have their personal data sold for the purpose of identity theft—which is much farther along in the chain of inferences for the plaintiffs to likely suffer injury.

Overall, the Georgia Supreme Court reversed the court of appeals decision to dismiss plaintiff's negligence claim for failure to allege a cognizable injury. When viewing the facts in favor of the plaintiffs, the Supreme Court could not determine that plaintiffs would not be able to introduce sufficient evidence of injury in the complaint. Notably, the Court's decision in *Collins* is also consistent with recent federal court decisions applying Georgia law. See *In re Equifax, Inc., Customer Security Breach Litigation*, 362 F.Supp.3d 1295, 1315 (N.D. Ga. 2019) ("Plaintiffs here have alleged that they have been harmed by having to take measures to combat the risk of identity theft, by identity theft that has already occurred to some members of the class, by expending time and effort to monitor their credit and identity, and that they all face a serious and imminent risk of fraud and identity theft due to the Data Breach. These allegations of actual injury are sufficient to support a claim for relief."); *In re Arby's Restaurant Group Inc. Litigation*, 2018 WL 2128441, at *11 (N.D. Ga. 2018) ("While Arby's is correct that a plaintiff may not recover for injuries that are purely speculative, such as the potential risk of future identity theft, Plaintiffs' Complaint alleges costs associated with actual data theft.").