ANOTHER FEDERAL COURT ALLOWS DATA BREACH ACTION TO PROCEED UNDER COMMON LAW "BAILMENT" THEORY OF LIABILITY

Joshua Hummel

For as long as there have been data breaches that expose consumer data to hackers, there have been lawsuits by consumers seeking to hold companies liable for failing to protect their data. However, traditional theories of legal liability often do not match up directly with the unique realities of data breaches. As a result, courts have frequently dismissed data breach claims by consumers for reasons relating to lack of standing, unclear causation, nebulous harm, and speculative damages. This problem has been especially acute for plaintiffs hoping to bring claims on behalf of a class of all consumers whose personal data was compromised in a security breach.

The Southern District of Indiana, however, recently allowed a data breach class action to proceed on a theory of liability that has been frequently proposed by commentators but which, until recently, was almost uniformly rejected by courts: the common law theory of bailment.[1] *See Krupa v. TIC International Corp.*, 2023 WL 143140 (S.D. Ind. Jan. 10, 2023).

In *Krupa*, the plaintiff brought a putative class action on behalf of himself and other individuals whose social security numbers were exposed in a hacking of the computer systems of the defendant, a benefits administration company. The defendant moved to dismiss the bailment claim on the grounds that the plaintiff lacked standing to sue and that the complaint did not sufficiently allege damages to assert a cause of action. The court held that both arguments hinged on the same issue, i.e., whether the plaintiff was actually injured by the theft of his personal data, and whether his risk of future injury provided an adequate basis for recovery.

In denying the defendant's motion to dismiss, the court in *Krupa* noted that bailment is not reserved solely for physical goods, as Indiana courts have recognized electronic data as a form of property in other contexts. The *Krupa* court also found that the complaint sufficiently alleged that the defendant held the plaintiff's personal data under a "shared understanding that it would remain confidential," and that the defendant was negligent in exposing his data to hackers.

The *Krupa* court also distinguished an Indiana case decided less than two years earlier, in which the court dismissed a bailment claim due to the defendant's lack of "exclusive

[1] As explained by the court in *Krupa*, bailment is the "delivery of personal property by one person (the bailor) to another (the bailee) who holds the property for a certain purpose." *Krupa*, at *3, *quoting Black's Law Dictionary* 169 (10th ed. 2014); J. Story, *Commentaries on the Law of Bailments* § 2, p. 2 (1832). "'A bailee normally owes a legal duty to keep the item safe, according to the terms of the parties' contract if they have one, and according to the 'implication[s] from their conduct.'" *Id.*

possession" over the plaintiff's data. *See Albanese Confectionery Grp., Inc. v. Cwik*, 165 N.E.3d 139 (Ind. Ct. App. 2021), *transfer denied*, 169 N.E.3d 1117 (Ind. 2021) (where plaintiff's former employer terminated her and remotely wiped her personal smartphone, resulting in the loss of her personal data, court dismissed plaintiff's bailment claim because both parties had some degree of control over phone and its contents). In contrast to the facts in *Albanese*, the *Krupa* court held that the plaintiff "was unable to manipulate his personal data on TIC's servers" and that the defendant "was in full control" of the plaintiff's data, thereby satisfying the "exclusive possession" requirement for a claim of bailment.

Finally, with respect to the plaintiff's alleged injury or damages, the *Krupa* court held that the "invasion of a common law right (i.e., the existence of a common law cause of action) satisfies the 'injury' prong" to establish standing, and that nominal damages are available for breach of bailment. As a result, the court rejected without much additional analysis the defendant's argument that the bailment claim must be dismissed because the plaintiff failed to allege a specific injury arising from the data breach.

Before *Krupa*, numerous courts had dismissed data breach claims based on a bailment theory of liability, for various reasons. However, *Krupa,* and a 2020 decision from a federal court in New York, may signal a trend that more courts are willing to allow data breach claims to proceed under a theory of bailment. *See Wallace v. Health Quest Systems, Inc.*, 2021 WL 1109727, at *13-14 (S.D.N.Y. Mar. 23, 2021) (denying motion to dismiss a constructive bailment claim for data breach, holding that "the Court is persuaded New York's courts would extend a claim for breach of bailment to ... intangible information."). If other courts around the country follow *Krupa*'s lead, it could represent a major shift in how data breach claims are litigated. Companies that maintain Personally Identifiable Information ("PII") belonging to consumers or employees should keep a close eye on this issue as it continues to develop.

For additional information on this topic, please contact Martin Tully at mtully@redgravellp.com or Eliza Davis at edavis@redgravellp.com.

The views expressed in this article are those of the authors and not necessarily those of Redgrave LLP or its clients.

---

[2] *See, e.g., Savidge v. Pharm-Save, Inc.*, 2020 WL 265206, at *7 (W.D. Ky. Jan. 17, 2020) (rejecting claim that plaintiffs' PII constituted "personal property," and noting that *both* parties continued to maintain separate but complete possession of it); *Galaria v. Nationwide Mut. Ins. Co.*, 2017 WL 4918634, at *2 (S.D. Ohio Oct. 31, 2017), report and recommendation adopted, 2017 WL 6375803 (S.D. Ohio Dec. 13, 2017) (rejecting bailment claim based on insufficient allegations regarding transfer of control or custody of plaintiffs' PII to the defendant); *In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, 903 F. Supp. 2d 942, 974 (S.D. Cal. 2012) (rejecting argument that plaintiff's PII was "delivered" to Sony and expected to be returned); *In re Target Corp. Data Sec. Breach Litig.*, 66 F. Supp. 3d 1154, 1177 (D. Minn. 2014) (questioning whether personal financial information constitutes "property" subject to bailment principles, and whether an agreement existed to return it to plaintiffs); and *Ruiz v. Gap, Inc.*, 540 F. Supp. 2d 1121, 1127 (N.D. Cal. 2008) (same).