How Ill. Ruling Could Influence Future Data Breach Cases

By **Brian Myers and David Ross** (February 18, 2025)

Brian Myers

David Ross

In Petta v. Christie Business Holding Co. PC, the first ruling from the Illinois Supreme Court addressing the merits of data breach litigation, the court affirmed the dismissal of a plaintiff's putative class action for lack of standing under Illinois law.

This Jan. 24 decision solidifies the requirement in Illinois that plaintiffs must establish an injury that can confer standing before they can assert claims arising out of a data security incident.

Background

The suit was brought in 2023 by a patient against her healthcare clinic, Christie Clinic, after it notified its patients that it had identified unauthorized access to one of its email accounts, where the unauthorized actor attempted to intercept a financial transaction between the clinic and a third-party vendor.

The clinic's notice letters acknowledged that it was not able to determine to what extent the unauthorized actor actually viewed any particular emails within the account. As a protective measure, the clinic notified anyone whose personal information may have been contained within messages in the account, and disclosed to the plaintiff that the incident may have involved her Social Security number. The letter included an offer of free credit monitoring, but the plaintiff did not enroll in the service.

Following the incident, the plaintiff alleged that her phone number, city and state were used to make a fraudulent loan application in someone else's name, and she received multiple phone calls about loan applications she did not initiate. The plaintiff did not allege that her name or Social Security number were used to make the fraudulent application, and did not allege that any other putative class members had a similar experience.

The plaintiff asserted negligence claims and a claim pursuant to the Illinois Personal Information Protection Act, or PIPA. The clinic moved to dismiss for lack of standing and failure to state a claim. The trial court found that the plaintiff's allegations of potential identity theft were sufficient to establish standing.

Nevertheless, the trial court dismissed the complaint finding that Illinois does not recognize a common law or statutory duty to protect personal information, and that the economic loss doctrine barred any negligence claims. The Appellate Court of Illinois, Fifth District, affirmed but on the different ground that the plaintiff lacked standing.

The appellate court did not address whether Illinois law imposes a duty to safeguard personal information.

Analysis of the Decision

The Illinois Supreme Court affirmed the appellate court's reasoning, beginning its analysis by explaining that standing under Illinois law requires an injury in fact that is concrete and

fairly traceable to the defendant.

If a plaintiff alleges only a "purely speculative future injury" and is not in "immediate danger" of sustaining an injury, then the plaintiff fails to allege any concrete injury. Turning to the alleged facts, the court found that, at best, the plaintiff alleged only an increased risk of harm following the incident, but failed to allege facts showing she was in sufficiently immediate danger to solidify her alleged injury.

The court noted that the clinic's notice letters stated only that information may have been accessed, and that the motivation for the unauthorized access appeared to be intercepting a financial transaction, not stealing personal information.

Regarding the alleged loan application, the court found that this event failed to confer standing for two reasons.

First, the loan application was made using only publicly available information — city, state and phone number — and failed to support the plaintiff's allegations that her private information was compromised. Second, the loan application was not fairly traceable to the incident because "anyone could have committed the fraud using the same readily available public information."

The Illinois Supreme Court's decision establishes an important benchmark for the viability of Illinois-based lawsuits arising out of data security incidents that defendants can cite to defend these lawsuits.

However, the Petta decision is also notable for some issues it did not address.

Chief among them are two Illinois appellate court decisions that assess whether Illinois imposes a common-law duty to safeguard personal information. In the 2010 case of Cooney v. Chicago Public Schools, the Appellate Court of Illinois, First District, found that Illinois does not impose a common-law duty to safeguard personal information. The court based its analysis in part on the fact that the only requirement at the time under PIPA was that organizations experiencing a data breach provide notice to affected individuals.

While PIPA contains a private right of action, Cooney further found that any action under PIPA requires economic damages, and the mere risk of increased harm or time lost following a data security incident did not constitute economic damages.

The trial court in Petta relied on Cooney to find that the defendant clinic did not owe a common-law duty of care. However, after Cooney, the Illinois Legislature amended PIPA to include a requirement that organizations implement reasonable measures to safeguard personal information.

Relying on that amendment, in 2023, in Flores v. AON Corp., the First District found that Illinois now imposes a common-law duty to safeguard personal information that is actionable in tort, notwithstanding the fact that PIPA creates a statutory cause of action with specific statutory requirements.

The Illinois Supreme Court's Petta decision was based solely on standing. As such, Petta leaves open the possibility that another case with different factual allegations may require the court to resolve the potential conflict between Cooney and Flores.

Conclusion

While data breach litigation has been ongoing in federal court for decades, much of the federal case law is limited to issues of Article III standing. There are only a limited number of state-level appellate court decisions addressing the merits of data breach class action claims.

This is notable because data breach plaintiffs almost exclusively assert state law claims. In the absence of controlling state appellate court authority, both state and federal trial courts have reached inconsistent results on whether data breach plaintiffs have alleged sufficient facts to pursue a claim.

Petta joins decisions from appellate courts in states such as Maine,[1] Michigan[2] and New York[3] that have dismissed data breach lawsuits for various reasons, including lack of standing under state law or failure to allege cognizable damages. However, appellate courts in states such as Georgia,[4] Pennsylvania,[5] Washington[6] and Wisconsin[7] have denied motions to dismiss and allowed data breach class action litigation to proceed.

While defendants will undoubtedly cite the Petta decision in dispositive motions, the decision is unlikely to prompt a significant decrease in data breach class action filings in Illinois. Litigation in Illinois and elsewhere over the merits of such claims will likely continue, as new claims arise with different factual allegations.

Brian H. Myers is of counsel at Wilson Elser Moskowitz Edelman & Dicker LLP.

David M. Ross is a partner and co-chair of the commercial litigation and class action defense practice teams at the firm.

[1] In re Hannaford Bros. Co. Customer Data Sec. Breach Litig., 2010 ME 93, ¶ 8, 4 A.3d 492, 496 (Maine Sup. Ct. 2010).

[2] Doe v. Henry Ford Health Sys., 308 Mich. App. 592, 600, 865 N.W.2d 915 (Mich. Sup. Ct. 2014).

[3] Greco v. Syracuse ASC LLC, 218 A.D.3d 1156, 193 N.Y.S.3d 511 (N.Y. App. Div. 2023).

[4] Collins v. Athens Orthopedic Clinic, P.A., 307 Ga. 555, 837 S.E.2d 310 (Ga. Sup. Ct. 2019).

[5] Dittman v. UPMC, 649 Pa. 496, 196 A.3d 1036 (Pa. Sup. Ct. 2018).

[6] Nunley v. Chelan-Douglas Health Dist., 32 Wash. App. 2d 700, 558 P.3d 513 (Wash. App. Ct. 2024).

[7] Reetz v. Advocate Aurora Health Inc., 2022 WI App 59, 405 Wis. 2d 298, 983 N.W.2d 669 (Wisc. App. Ct. 2022).