WINSTON & STRAWN LLP

CLIENT ALERT

Landmark Ruling on the Illinois Biometric Information Privacy Act

JANUARY 30, 2019

Key Takeaways

- The Illinois Biometric Information Privacy Act ("BIPA") imposes requirements on companies that collect "biometric information," including fingerprints.
- Unlike other, similar state laws regulating the collection of biometric data in Texas and Washington, BIPA includes a private right of action, and, per the Illinois Supreme Court's recent holding, individuals can file suit for a mere violation of the law's requirements, even if the individuals do not suffer any actual harm.
- Numerous class-action lawsuits are being filed, and the targeted defendants largely include employers that collect biometric information for wage-and-hour purposes and companies that collect biometric information for the purpose of providing identity-verification services. While many actions are pending, a number have already settled, for amounts from around $150,000 to $1.5 million, with individual payouts ranging from around $40 to $125 per class member

BACKGROUND

BIPA, in effect since October 3, 2008, regulates the privacy and protection of biometric information (which is defined by the statute as a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry). Under BIPA, companies that collect this information are generally required to inform the individual that his or her biometric information is going to be collected; indicate the purpose of the collection; describe the length of time the biometric information is to be collected, stored, and used; develop a written, publicly available policy that establishes a retention schedule; and obtain a written release from the individual before collecting any biometric data or sharing collected biometric data with a third party.

BIPA provides a private right of action by natural persons who are "aggrieved by a violation of this Act" against a private entity that negligently, intentionally, or recklessly violates the Act's provisions. The Act does not define what it means to be "aggrieved" by a violation of the Act, leaving it to the courts to determine what level of harm, if any, a plaintiff must experience in order to be considered an aggrieved person. This has led BIPA defendants to argue that

plaintiffs must suffer some type of actual harm (e.g., identity theft) in order to assert a BIPA claim and that mere violations of BIPA (e.g., improper notice or lack of consent) were insufficient for statutory standing. This was the key issue to be decided by the Illinois Supreme Court in *Rosenbach v. Six Flags Entertainment Corp*. Through a unanimous decision that will affect more than 200 pending cases, the court held that a plaintiff need not suffer any actual harm to be considered an "aggrieved" person who has standing to sue under BIPA.

ROSENBACH DECISION

Stacy Rosenbach purchased a season pass to Six Flags for her minor son Alexander in 2014. Six Flags uses a fingerprint process when issuing repeat-entry passes that scans an individual's fingerprints, and then stores that information to verify the individual's identity. Thus, Alexander was required to scan his thumbprint into Six Flags' biometric data capture system during his first visit to the park, after which he was able to collect his season pass card. Ms. Rosenbach brought an action against Six Flags on behalf of Alexander and other similarly situated persons under BIPA in the circuit court of Lake County, Illinois. The complaint generally asserted a failure by Six Flags to comply with BIPA's procedural requirements in collecting and handling biometric information. For example, the complaint alleges that Six Flags failed to inform class members, in writing, that the biometric information was being collected, or how the information would be used and for how long. The complaint further alleges that Six Flags failed to obtain a written release from the class members before collecting biometric information.

Six Flags sought dismissal of Ms. Rosenbach's complaint under Sections 2-615 and 2-619 of the Illinois Code of Civil Procedure. Six Flags' main argument under the motion was that Alexander did not have standing to sue under BIPA because he suffered no actual or threatened injury and was therefore not "aggrieved" under the statute. The circuit court denied Six Flags' motion. On appeal, the Illinois Appellate Court for the Second District disagreed, finding that a plaintiff is not "aggrieved" within the meaning of BIPA—and thus cannot sue for damages or injunctive relief—based solely on a defendant's violation of the statute. For the appellate court, actual injury or an adverse effect must be alleged, and the defendant's actions must be more than a "technical violation of the Act." Upon receiving this decision, Ms. Rosenbach petitioned the Illinois Supreme Court for review.

The Illinois Supreme Court, in a relatively short opinion, sided against Six Flags, finding that limiting relief under BIPA to those who sustained actual injury or damage would go against the commonly understood and accepted meaning of the term "aggrieved," and would depart from the plain, unambiguous language of BIPA. The court cited precedent that a person who suffers actual damages as a result of a violation of his or her rights would be an aggrieved person, but sustaining such damages is not necessary to qualify as aggrieved. Rather, the court held that a person is aggrieved, in the legal sense, when "a legal right is invaded by the act complained of or his pecuniary interest is directly affected by the decree or judgment." Further, the court reasoned that the duties imposed on private entities through Section 15 of BIPA, which duties address the collection, retention, disclosure, and destruction of a person's biometric information, define the boundaries of the statutory right granted to individuals by the Illinois General Assembly. Thus, per the court, when a private entity fails to comply with Section 15's requirements, the violation is an impairment of the person's statutory rights whose biometric information is subject to the breach.

Given this position, the court determined that there is no such thing as a "technical" violation of BIPA. The court also emphasized the deterrence aspect of the law, noting that the procedural protections implemented through the law are crucial in a digital world because "technology permits the wholesale collection and storage of an individual's unique biometric identifiers—identifiers that cannot be changed if compromised or misused. The court further noted that the private right of action in BIPA is the Act's only enforcement mechanism. From this, the court reasoned that the legislature intended for the provision describing the private right of action to have substantial force.

WHAT'S NEXT

Of note, the court commented on the ease, from its perspective, with which a private entity could comply with the law, stating that "[c]ompliance should not be difficult; whatever expenses a business might incur to meet the law's requirements are likely to be insignificant compared to the substantial and irreversible harm that could result if biometric identifiers and information are not properly safeguarded…." Indeed, while many BIPA suits are pending, a number have settled for amounts from around $150,000 to $1.5 million, with individual payouts ranging from around $40 to $125 per class member.

Based on the foregoing, the primary way to mitigate the likelihood of receiving a BIPA complaint is simply to comply with the statute and all of its requirements, including those provisions related to giving notice and obtaining consent before collecting any biometric information. In addition, it is likely that any BIPA litigation going forward is going to be very fact-intensive regarding whether the defendant actually complied with BIPA's provisions. To that end, a rather significant question that remains open after the court's decision in *Rosenbach* is what constitutes "consent" under BIPA, especially in the employment context, where the statute's definition of "written release" appears to provide some flexibility. As such, a potential argument for BIPA defendants going forward may be to assert that proper consent was obtained from an individual before his or her biometric information was collected.

As a practical matter, companies that engage in the collection of biometric information from individuals in Illinois should examine their practices (in particular, how such information is collected, used, and shared) and evaluate whether they have obligations to comply with BIPA. In particular, this may be critical to employers that, for example, collect fingerprints from employees and contractors for timekeeping purposes. Other companies that should take care to evaluate their BIPA obligations are those that collect biometric information for identity verification purposes, especially where a company may not have direct touchpoints with the individual who is submitting the biometric information and may need to rely on contractual promises from its customers related to BIPA compliance.

Note that BIPA lacks an express statute of limitations for claims brought under the Act. As such, even if a company takes action now to meet its BIPA obligations, it may still be liable for past years of non-compliance, and thus may be vulnerable to a class action complaint. If you are unsure what your level of exposure is under BIPA, contact your Winston & Strawn attorney. Winston has extensive experience in both counseling companies on compliance with BIPA and similar laws and, should it become necessary, defending consumer class actions in Illinois state and federal courts.

6 Min Read

Related Locations

Chicago

Related Topics

Biometrics | Consumer Privacy | Global Privacy & Data Security Task Force | Tracking and Monitoring

Related Capabilities

Privacy & Data Security | Privacy: Regulated Personal Information (RPI)

Related Regions

North America

Related Professionals

Steven Grimes

Sean G. Wieber

Eric Shinabarger

Alessandra Swanson

© 2025 Winston & Strawn LLP.