NOW + NEXT

PRIVACY LAW ALERT | NIXON PEABODY LLP

JANUARY 25, 2019

Illinois Supreme Court decision allows for biometric privacy claims to proceed without a showing of actual harm

By Richard Tilghman, John Ruskusky and Brian Alcala

In 2008, Illinois enacted what is widely considered the strictest legislation in the country for protecting biometric data, such as fingerprints, eye scans and facial scans. The Illinois Biometric Information Privacy Act ("BIPA" or "the Act") requires disclosure and written consent for any entity that collects or stores biometric information as defined in the Act. Any person "aggrieved by" a violation of BIPA can sue for statutory damages of at least $1000 per negligent violation or $5000 per intentional violation, as well as injunctive relief, attorneys' fees, expert witness fees and other litigation expenses.

BIPA has been used by the plaintiffs' class action bar to target over 150 companies involved in the collection or storage of biometric data.[1] In December 2017, the Second District of the Illinois Appellate Court provided a major setback for the plaintiffs' bar when it ruled that BIPA's requirement that a plaintiff be "aggrieved by" a violation of the Act necessitated more than a mere statutory violation. *Rosenbach v. Six Flags Entertainment Corp.*, 2017 IL App (2d) 170317 (Ill. App. Ct. 2017). The *Rosenbach* case was brought by the mother of a 14-year-old who had provided an electronic scan of his thumb as a way to gain repeat entry to the Six Flags Great America amusement park in Gurnee, Illinois. *Rosenbach* alleged that neither she nor her son had received the disclosures required by the Act, and had not given written consent to the collection of his biometric information. The Illinois Appellate Court held that the violation of the Act's disclosure and consent requirement was insufficient to create a cause of action under the Act, and that some "injury or adverse effect" to the plaintiff was required.

In September 2018, the First District of the Illinois Appellate Court reached a contrary conclusion in *Sekura v. Krishna Schaumburg Tan, Inc.*, 2018 IL App (1st) 180175 (Ill. App. Ct. 2018). In *Sekura*, the court ruled that: (1) a statutory violation alone was sufficient to give rise to a claim under the

[1] See our prior coverage of these cases: "Using fingerprints for timekeeping purposes in Illinois — what you need to know about the Illinois Biometric Information Privacy Act," available here, and "Second Circuit issues a leading decision on Article III standing requirements for claims filed under the Illinois Biometric Information Privacy Act," available here.

Act; (2) a disclosure of biometric information to an out-of-state third-party created sufficient injury to give rise to a claim under the Act; and (3) the plaintiff's alleged "mental anguish" at having her biometric information collected was an additional injury that supported her status as an "aggrieved" party.

Before *Sekura* was decided, the Illinois Supreme Court had granted review of the Second District's decision in *Rosenbach*, setting the stage for Illinois's highest court to decide the viability of one of the key defenses against the flood of Illinois class actions being filed under the Act.

On January 25, 2019, the Illinois Supreme Court issued its decision in *Rosenbach*. In a blow to businesses that use biometric information in Illinois, the court ruled that no actual damage beyond a statutory violation was required to bring suit under the Act, characterizing Six Flags' arguments to the contrary as "meritless." The court cited to dictionary definitions and long-standing Illinois cases holding that the violation of any legal right is sufficient to confer "aggrieved" status. It also took issue with the Second District's characterization of a statutory violation as merely "technical" in nature, emphasizing that a statutory violation creates a "real and significant" harm. Requiring additional harm, according to the court, would be "completely antithetical to the Act's preventative and deterrent purposes."

To date, the overwhelming majority of cases filed under the Act have been brought by plaintiffs alleging that their employer had collected an electronic fingerprint for timekeeping purposes without consent. In the wake of the Illinois Supreme Court's decision, we expect a flood of new cases to be filed alleging similar theories. While employers who use fingerprint scans for timekeeping purposes have been the most frequent target of the plaintiffs' bar, any company that collects biometric information should consult with counsel to determine whether the Act applies and, if it does, ensure that steps are taken to comply. As the court noted, compliance "should not be difficult," and avoids the risk of being subject to the harsh penalties imposed by the Act.

The good news is that BIPA sets forth what a company can do to limit its exposure. These steps include having a written policy that complies with the Act and signed written consent from the person whose biometric information is collected. Nixon Peabody has assisted clients to update their disclosures and policies to ensure compliance with BIPA.

For more information on the content of this alert, please contact your Nixon Peabody attorney or:

- Richard Tilghman at **rhtilghman@nixonpeabody.com** or (312) 977-4881
- John Ruskusky at **jtruskusky@nixonpeabody.com** or (312) 977-4460
- Brian Alcala at **bvalcala@nixonpeabody.com** or (312) 977-4366
- Jason Gonzalez at **jgonzalez@nixonpeabody.com** or (213) 629-6019
- Steven Richard at **srichard@nixonpeabody.com** or (401) 454-1020