Illinois Supreme Court Opens Door for Massive Damage Awards in Biometric Cases: 5 Things Employers Need to Know

Insights
2.17.23

The Illinois Supreme Court just ensured that employers who don't strictly comply with the state's landmark biometric law could be on the hook for massive damage awards, a ruling that should cause you to immediately review your biometric collection practices. Specifically, the court addressed the way "violations" under the Illinois Biometric Information Privacy Act (BIPA) are determined. Under today's far-reaching ruling, a separate claim accrues ***each time*** a private business scans or discloses an individual's biometric information or identifier without prior written consent— rather than just the first time it happens. This means employers in the state may face steep penalties even for technical "violations" ***each and every time*** an employee provides their biometric information, such as when they use fingerprints to clock in and out of shifts. BIPA has been the source of expensive class action lawsuits, arbitrations, and settlements over the past several years — and today's ruling further tilts the scales in favor of employees. What do you need to know about the ruling and its impact on employers in the state?

What Does BIPA Require?

Before diving into the impact of *Cothron v. White Castle System, Inc.*, it is important to explore what BIPA requires. Among other things, BIPA mandates that private entities — including employers — that collect or maintain employees' fingerprints, retinal or iris scans, voiceprints, hand scans, or face geometry, must first receive written consent from the employee. Covered entities also must develop a publicly available policy that establishes the retention schedule for the applicable biometric data.

Notably, the act's requirements apply to information derived from biometric data, which could include electronic or mathematical representations of biometric data. The statute also contains various data retention requirements concerning individuals' biometric data.

Failure to comply with BIPA's requirements can result in liquidated damages of $1,000 per negligent "violation" and $5,000 per intentional "violation," or actual damages, whichever is greater. Indeed, employees do not need to show that they have suffered any actual harm in order to prevail. The law also provides for attorneys' fees, costs, and any other relief that a court may deem appropriate.

5 Key Takeaways from the Ruling

The Illinois Supreme Court's decision in *Cothron* determined when a claim or "violation" under BIPA accrues. Here are the five key takeaways you should note from the ruling:

1. **Every scan counts:** In its ruling, the sharply divided court held that a separate claim accrues under the act ***each time*** a private entity scans or discloses an individual's biometric information or biometric identifier in the absence of prior written consent.
2. **Steep penalties:** Thus, when an employee provides their biometric information or biometric identifier (whether to clock in or out for a shift, or any other purpose), ***each and every such instance*** is an independent violation that is subject to a new $1,000 (or $5,000) liquidated damages penalty.
3. **Significant consequences for employers:** Even a ***per person*** definition of a "violation" under the act led to astronomical damages awards and settlements, but a ***per scan*** assessment will likely be exponentially higher.
4. **Court punts to legislature:** With respect to the ruinous consequences that many employers may face as a result of the court's interpretation, the court's majority noted that it was up to the legislature to limit the damages that may be assessed. In any event, it said, the likely dire consequences that employers are concerned about may not pan out because:
   - damages under the act are discretionary; and
   - trial courts overseeing class actions can equitably fashion awards and settlements.

   These assurances will do little to calm the nerves of employers, however, given the incredibly large stakes now at play in these cases.
5. **Dissent notes absurd consequences:** According to the dissent, absurd consequences (such as ruinous damages) could not have been the legislature's intent in enacting BIPA. "Imposing punitive, crippling liability on businesses could not have been a goal of the act," the dissent said. Nevertheless, until the court reconsiders this question, the majority's interpretation prevails, and businesses will be subject to a per-scan assessment under BIPA.

What Should Employers Do?

Employers must remain vigilant in complying with BIPA's requirements. BIPA requires strict compliance ***before, during, and after*** collecting individuals' biometric information and biometric identifiers. Employers need to implement lawful policies, procedures, and authorizations before they collect any biometric data. There are also various (but narrowly interpreted) exceptions to BIPA, so employers may be able to avail themselves of those as well. These measures are essential to defending against claims under the act.

We will continue to monitor any further developments and provide updates on these and other labor and employment issues affecting employers, so make sure you are subscribed to Fisher Phillips'

Insight System to gather the most up-to-date information. If you have questions, please contact your Fisher Phillips attorney, the authors of this Insight, or any attorney in our Chicago office.

Related People

Joel W. Rice
Partner
312.580.7810
Email

Franklin Z. Wolf
Partner
312.580.7807
Email

Service Focus

Consumer Privacy Team

Privacy and Cyber

Litigation and Trials

Related Offices

Chicago