



Illinois Supreme Court Opens the Door for Huge Damages Claims in BIPA Actions

May 11, 2023

Reading Time : **3 min**

By: Natasha G. Kohne, Joseph Hold

The Illinois Supreme Court issued a pair of decisions related to the Illinois Biometric Information Privacy Act (BIPA) that continue to ratchet up compliance pressure on businesses. On February 17, 2023, the Illinois Supreme Court ruled in a narrow 4-3 majority that a separate claim for damages accrues each time a business violates the state's BIPA (e.g., accruing additional damages each time a fingerprint is scanned rather than a single violation for each unique fingerprint collected). Under BIPA, companies collecting biometric data such as facial scans, fingerprints and voiceprints can face millions of dollars in fines if they fail to seek permission to collect this data, or if they fail to disclose their data retention plan.

In a class action filed against White Castle, the United States Court of Appeals for the 7th Circuit certified to the Court the following question: "Do section 15(b) and 15(d) claims accrue each time a private entity scans a person's biometric identifier and each time a private entity transmits such a scan to a third party, respectively, or only upon the first scan and first transmission?"¹ In the underlying case filed in 2018, the putative class action representative Latrina Cothron, a White Castle employee since 2004, alleges that White Castle collected her fingerprints without her consent every time she accessed her computer and weekly pay stubs, violating her biometric privacy rights with every scan since BIPA was enacted in 2008. White Castle argued that Ms. Cothron's BIPA violation claim was time barred because it accrued, if at all, only the first time her fingerprint was scanned after the Act took effect. The Court disagreed, holding that "the plain language of section 15(b) and 15(d) shows that a claim accrues under the Act with every scan or transmission of biometric identifiers or biometric information without prior informed consent."²

The decision came on the heels of another BIPA-related ruling from the Court, which ruled just two weeks earlier that Illinois' five-year "catchall" statute of limitations applies to BIPA claims because the statute does not specify a limitations period.³ Taken together with the *White Castle* decision, these rulings could have catastrophic consequences for corporations defending BIPA class actions because potential liability may be increased exponentially. Under BIPA, companies can face \$1,000 in liquidated damages per violation and \$5,000 for intentional or reckless violations.⁴ *White Castle* estimated that if Cothron succeeds on her claims on behalf of a class of nearly 9,500 employees, it may be on the hook for upwards of \$17 billion in damages.⁵

More recently on March 23, 2023, the Illinois Supreme Court handed down a ruling addressing BIPA claims brought by employees under union contracts with broad management rights clauses. In the case of *William Walton v. Roosevelt University*, the Court determined that the Labor Management Relations Act preempts BIPA, meaning biometric privacy disputes between union employees are resolved under federal law and their collective bargaining agreement.

Unlike in *White Castle*, the plaintiff William Walton must go before an adjustment board instead of a court to pursue claims that Roosevelt University collected his scanned fingerprint data unlawfully. This decision arrives after two other union-related cases—*Miller v. Southwest Airlines* and *Fernandez v. Kerry*—similarly found preemption. In *Miller*, the 7th Circuit found BIPA claims are preempted by the Railway Labor Act, ruling that a dispute over fingerprint scanning must be settled before an adjustment board since the union may have agreed to the scans on behalf of the employees. In *Fernandez*, the 7th Circuit found that the BIPA claims from union-represented workers are preempted under the Labor Management Relations Act, upholding a dismissal because another fingerprint scanning dispute implicated collective bargaining agreements.

The *White Castle* decision has a silver lining for employers utilizing biometric technology to collect data from Illinois residents. In considering *White Castle*'s concerns over potential "annihilative liability," the Court acknowledged that BIPA damages are discretionary rather than mandatory. The Court ultimately left concerns over excessive damages awards unanswered, encouraging the legislature to clarify its intent regarding potential liability under the Act.

In light of these recent rulings, companies are likely to face increased pressure and higher settlement demands from plaintiffs, especially where claims may involve the use of biometric scanners on a daily basis or even multiple times per day. Companies should use caution when implementing biometric scanning technology, and those that already use such technology should conduct regular audits to ensure compliance with BIPA.

¹*Cothron v. White Castle Sys., Inc.*, 20 F.4th 1156, 1167 (7th Cir. 2021).

²*Cothron v. White Castle Sys., Inc.*, --- N.E. 3d ---, 2023 WL 2052410, at *8 (Ill. Feb. 17, 2023).

³*Tims v. Black Horse Carriers, Inc.*, --- N.E. 3d ---, 2023 WL 1458046, at *8 (Ill. Feb. 2, 2023).

⁴ CITE to statute

⁵*Cothron v. White Castle Sys., Inc.*, 2023 WL 2052410, at *7.

Categories

Cybersecurity & Information Security

Privacy Class Action

State Privacy Policy

Biometrics

© 2025 Akin Gump Strauss Hauer & Feld LLP. All rights reserved. Attorney advertising. This document is distributed for informational use only; it does not constitute legal advice and should not be used as such. Prior results do not guarantee a similar outcome. Akin is the practicing name of Akin Gump LLP, a New York limited liability partnership authorized and regulated by the Solicitors Regulation Authority under number 267321. A list of the partners is available for inspection at Eighth Floor, Ten Bishops Square, London E1 6EG. For more information about Akin Gump LLP, Akin Gump Strauss Hauer & Feld LLP and

other associated entities under which the Akin Gump network operates worldwide, please see our Legal Notices page.