February 27, 2023

Illinois Supreme Court Clarifies BIPA Violation Accruals, Opening the Door for "Annihilative" Damages

by Vita E. Zeltser

The Illinois Supreme Court ruled that a company violates the Illinois Biometric Information Privacy Act (BIPA) each time the company scans a person's biometric information (e.g., fingerprints) without consent—not just upon the initial collection. Calculating the number of violations that occurred determines the size of a plaintiff's potential recovery because BIPA authorizes per-violation damages of $1,000 for negligent violations and $5,000 for intentional or reckless violations. The case, *Cothron, V. White Castle System, Inc.*, 2023 IL 128004 (Feb. 17, 2023), is available here.

Background - Biometrics and BIPA

Companies regularly use biometrics for identity verification as a reliable authentication method. To do so, companies generally scan and store a portion of an individual's biometric data (e.g., fingerprints). Each time an individual must authenticate their identity, the company rescans the individual's biometric data. Only a matching biometric will authenticate the individual. For example, employers that have hourly employees often verify when an employee clocks in and out of work with timeclocks that require an individual to verify identity through hand or finger scans.

BIPA requires any company that collects or otherwise obtains biometrics to obtain a prior written consent (referred to in the statute as a "release") from the individual whose data is being collected. The question for the Illinois Supreme Court in the *White Castle* case was whether a BIPA violation occurs only upon a company's initial collection of the individual's biometric data or upon each scan.

The White Castle Case

Employees of White Castle restaurants used finger scans to access paystubs as well as White Castles' computer systems. White Castle used a third-party vendor to verify each scan and authorize the employees' access. White Castle never collected a consent for the biometric scanning, giving rise to the plaintiff employees' putative class action litigation.

White Castle argued that it violated BIPA only once for each employee, upon initially collecting biometric information. The Illinois Supreme Court disagreed, ruling that violations accrue each time a company scans a person's biometric data rather than only upon the first scan.

This decision affects not only damages, for the reasons explained above, but also how courts will apply BIPA's five-year statute of limitations. The *White Castle* decision means that BIPA claims are available five years after the last, rather than the initial, non-compliant scan.

Opening the Door for Change?

The Illinois Supreme Court's dramatic ruling may have invited legislative and judicial challenges to BIPA. The decision permits exceedingly high damages arising from only a technical violation of BIPA's consent requirements. *Amici* supporting White Castle's position described this decision as opening the door to "annihilative liability" not contemplated by the legislature. Future defendants might bring constitutional challenges against enforcement of damages calculated pursuant to the *White Castle* decision, arguing that such damages are unconstitutionally excessive. *See, e.g., Wakefield v. ViSalus, Inc.*, 2022 WL 11530386 (9th Cir. Oct. 20, 2022). Moreover, as of the time of this writing, a bill is advancing through the Illinois legislature that would make recovery under BIPA more difficult. House Bill 3199, would require a plaintiff to provide a potential defendant with 15 days' written notice of an alleged violation before bringing suit. If the defendant then cures the noticed violation (among other steps), then the plaintiff would be barred from bringing an action under BIPA.