LEGAL UPDATES

PUBLISHED: MARCH 14, 2023

Massive Changes to Illinois BIPA Cases—Claims Now Accrue Per Scan Going Back As Far As Five Years

Services

Data Privacy & Cybersecurity

Labor & Employment

Professionals

ANNE M. MAYETTE
CHICAGO:
312.341.9844
ANNE.MAYETTE@
HUSCHBLACKWELL.COM

JULIE GARABEDIAN
CHICAGO:
312.985.8254
JULIE.GARABEDIAN@
HUSCHBLACKWELL.COM

On February 2, 2023, the Illinois Supreme Court ruled in *Tims et al. v. Black Horse Carriers, Inc.* that all cases filed pursuant to the Illinois Biometric Information Privacy Act (BIPA) are subject to a five-year statute of limitations period. Just over two weeks later, the Court ruled in *Cothron v. White Castle System, Inc.*, that a separate BIPA claim accrues each time a private entity collects and/or transmits an individual's biometric data. In Illinois, this now means that not only can a BIPA claim be brought with merely a statutory violation (see here), but that damages accrue per scan and accrue as far back as five years.

Five-Year Statute of Limitations Implemented for All Illinois BIPA Cases

The Court in Tims found that that 1) the Illinois Code of Civil Procedure's "catch-all" five-year statute of limitations period applied because BIPA otherwise contains no statute of limitations period; and 2) the five-year statute of limitations period embodies the "true intent and meaning of the legislature" when it enacted BIPA. Given this decision and vast expansion of the applicability period, employers need to be cognizant more than ever in ensuring compliance with BIPA's policy, notice, and disclosure requirements.

Previously, the Illinois Appellate Court designated differing statute of limitations periods based on the type of BIPA claim, focusing on whether the claim involved the "publication" of biometric data. Use of the word "publication" was the key indicator in deciphering which statute of limitations period to apply. The Illinois Appellate Court found that the one-year statute of limitations period applied to BIPA claims where "publication or disclosure of biometric data [was] clearly an element" of the claim, and the five-year statute

of limitations applied to BIPA claims where "no element of publication or dissemination" existed in those claims. Following this decision, both parties asked the Illinois Supreme Court to apply either the one-year or five-year statute of limitations period.

In its decision and reasoning, the Illinois Supreme Court focused on the "intent of the legislature, the purposes to be achieved by the statute, and the fact that there is no limitations period in [BIPA]" as key factors in finding that the five-year statute of limitations period was more suitable. Section 5 of BIPA enumerates the statute's goals and intentions, including securing "[t]he public welfare, security, and safety" of the public by "regulating the collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and information." The Illinois Supreme Court found that the legislature gave "extensive consideration" to the fears of and risks to the public regarding to the disclosure of biometric data, and that it would "thwart legislative intent to (1) shorten the amount of time an aggrieved party would have to seek redress…and (2) shorten the amount of time a private entity would be held liable for noncompliance…"

The Illinois Supreme Court looked to other types of privacy claims, like libel or slander, that have a one-year statute of limitations period in justifying its reasoning. It reconciled that an individual bringing a libel or slander claim only gets one year because that individual is expected to quickly learn of their injury and "act just as quickly when their reputation has been publicly compromised," whereas "the full ramifications of the harms association with biometric technology are unknown," and it is "unclear when or if an individual would discover evidence of the disclosure of his or her biometrics in violation of [BIPA]."

Common BIPA claims, as seen in the *Tims* case, stem from an employer's failure to institute, maintain, and adhere to a publicly available biometric information retention and destruction policy required under section 15(a), failure to provide notice and to obtain consent when collecting biometrics, in violation of section 15(b); and disclosure or dissemination of biometric information to third parties without consent in violation of section 15(d). Claims like these can be abated through a thorough review and analysis of company policies and procedures.

BIPA Claims Now Accrue Every Time Data is Collected and Disclosed

After receiving the certified question from the Seventh Circuit Court of Appeals pertaining to whether 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?"—the Illinois Supreme Court has clarified that claims will now accrue per scan and/or transmission.

The Court focused on the plain language of BIPA itself to "ascertain and give effect to the intention of the legislature," in reaching its decision. In doing so, the Court agreed with the plaintiff that the plain

language of BIPA's use of the words "collect" and "capture" support an interpretation that these things can happen more than once. For example, for a White Castle employee to access a White Castle computer (e.g., to view their paystubs), the employee must use their fingerprint per access. Upon subsequent scans, the new fingerprint is then compared to the stored fingerprint—meaning that the collection or capturing process happens per scan. Using a similar analysis in terms of transmission, the Court found this same reasoning applicable to a private entity's disclosure of the individuals' scans to a third party in holding that a claim also accrues per transmission.

White Castle warned the Court that accrual per scan could result in "astronomical" damage awards that would "constitute 'annihilative liability' not contemplated by the legislature and be possibly unconstitutional." White Castle gave the following scenario—if the plaintiff is allowed to bring her claims on behalf as many as 9,500 current or former White Castle employees, White Castle's damages could exceed $17 billion. There is no dispute that damages to this extent could be detrimental to any company. Additionally, the dissenting justices cautioned that under the Court's ruling, this now incentivizes future plaintiffs to delay bringing their claims as long as possible knowing that they can rack up damages per claim over a five-year period.

However, the Court found that the statutory language "clearly supports [the] plaintiff's position," and further reasoned that this was the legislature's intention. Interestingly, the Court agreed with the Illinois Appellate Court prior recognition in another case that "[a] trial court presiding over a class action—a creature of equity—would certainly possess the discretion to fashion a damage award that (1) fairly compensated claiming class members and (2) included an amount designed to deter future violations, without destroying defendant's business." It is unclear, though, how a trial judge, upon a finding from a jury that a violation occurred, can use an equitable power to limit or decrease a statutory damage award. Nonetheless, the Court punted any "policy-based concerns" about potentially excessive damage awards to the Illinois legislature.

What This Means to You

These two new rulings will surely have a significant impact on employers moving forward in terms of potential damage awards. Now more than ever, employers need to ensure that their policies and practices relating to biometric data are compliant with the law.

Contact Us

If you have questions regarding the significance of the recent decisions or other related questions about your current policies and practices relating to biometric information, contact Michael Hayes, Anne Mayette, Julie Garabedian, or your Husch Blackwell attorney today.