



#### RELATED PRACTICE AREAS

Class and Collective Actions  
Data Security and Privacy  
Labor and Employment

#### RELATED INDUSTRIES

State and Local Government - Illinois

#### RELATED TOPICS

Employee Rights  
Data Collection  
Liability  
Confidentiality

## Illinois Employers On Notice: BIPA Claims Accrue With Each Scan Or Transmission, Court Says

February 20, 2023 | [High Stakes Employment Issues, State Labor Laws, Labor And Employment](#)



**Mark Wallin**  
Partner

Just as the wave of Illinois Biometric Information Privacy Act (BIPA) class action lawsuits seemed to have crested, the Illinois Supreme Court handed down a 4-3 decision that will undoubtedly spur further BIPA litigation. Last week, in [Cothron v. White Castle System, Inc.](#), the state's high court ruled that a separate claim accrues under BIPA each time an entity scans or transmits an individual's biometric information. These hits just keep on coming from the Supreme Court, which [ruled a few weeks ago that all BIPA claims](#) were subject to a five-year look-back.

The court's ruling is the worst-case scenario for businesses in Illinois and could lead to exponentially greater liability for those who are not compliant. Now that the Supreme Court has weighed in, Illinois law dictates that businesses could incur liability for each unconsented scan and transmission of biometric information – \$1,000 per negligent violation and \$5,000 per intentional violation. In light of this ruling, employers could accrue hundreds (if not thousands) of violations per person over the five-year limitations period.

The holding is the result of a certified question from the U.S. Court of Appeals for the Seventh Circuit stating: "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?" In answering that claims do

accrue each time biometric information is collected and each time it is transmitted, the majority looked to the plain language of the statute. The court agreed with the lower court's interpretation of BIPA, reasoning that each time biometric information is collected or captured without consent, a violation occurs. And similarly, the moment an individual's biometric information is disclosed or disseminated, without consent, to a third party (i.e. a vendor), a violation occurs.

The Supreme Court acknowledged, but quickly dispatched, the concern raised by White Castle that such a reading would lead to "annihilative liability," which White Castle stated would be in excess of \$17 billion. The majority waved this away, stating the language of the statute is clear and must be given effect, while suggesting that the Illinois legislature could address this policy concern.

The three dissenting justices took issue with the majority's construction of the statutory language, looking instead to the interests protected by BIPA. In particular, the dissent reasoned that, logically, one's biometric information could only be collected and transmitted once. Indeed, once an entity is in possession of an individual's biometric information, it could not possess it again because it already had it, according to the dissent. As a result, the dissent concluded that an individual could only possess one claim for the collection and transmission of his or her biometric information.

The dissent further stated the court was not powerless to address absurd and unjust consequences of the statute. Pointing to potential liability in the billions, the dissent chided the majority's suggestion that the legislature intervene, explaining that the court has the ability to decide the legislature did not intend to impose crippling liability on businesses that "wildly" exceeded the harm.

Given this ruling, expect the next line of defense to be challenges to BIPA's constitutionality, likely on due process and/or Eighth Amendment grounds. Regardless, businesses operating in Illinois that utilize biometric information would be well-served to review their policies and practices to ensure BIPA compliance.