

CLIENT ALERT

Significant Illinois Biometric Information Privacy Act Rulings Create Additional Liability Risk For Companies

February 21, 2023

AUTHORS

Daniel K. Alvarez | Michael G. Babbitt | Laura E. Jehl | LaRue L. Robinson
Kari Prochaska

Two recent bellwether Illinois class action decisions reaffirm the significant risks and challenges that await companies which collect and use biometric data identifiers from people in Illinois. On February 17, 2023, the Illinois Supreme Court (the “Court”) held that separate claims for damages accrue under the Biometric Information Privacy Act (“BIPA”) *each time* an entity scans or transmits an individual’s biometric identifier, rather than upon only the first scan or transmission.¹ Just a few weeks earlier, on February 2, 2023, the Court ruled in a separate case that claims brought under BIPA are subject to a five-year, rather than a one-year, statute of limitations. Taken together, the Court’s rulings recognizing cumulative violations and an extended statute of limitations period create unprecedented BIPA litigation risk for businesses.

BIPA At a Glance

In effect since 2008, BIPA requires that notice be provided to, and written consent obtained from, an individual prior to collecting and using the individual’s biometric information, and also sets limitations on the use and sharing of that biometric information even after a business has provided notice and obtained consent. Under BIPA, “biometric information” is defined as any information, regardless of how it is captured, stored, or shared, based on an individual’s

¹ See *Latrina Cothron v. White Castle System, Inc.* 2023 IL 128004 ¶45.

Significant Illinois Biometric Information Privacy Act Rulings Create Additional Liability Risk For Companies

biometric identifier (e.g., a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry) used to identify an individual.²

Although other states maintain either biometric-specific laws or general privacy laws that expressly address the use of biometric identifiers, none of those laws has BIPA's enforcement teeth. In particular, BIPA includes a private right of action with steep statutory damages: successful plaintiffs can recover either \$1,000 or \$5,000 per claim, leading to substantial awards where large classes of plaintiffs have been certified.³ This private right of action has been effectively exploited by the plaintiffs' bar, in the form of both significant judgments *and* significant settlements. In 2022, in the first BIPA case to go to trial, a federal jury awarded the plaintiffs a \$228 million judgment,⁴ and settlements for even small classes have run into the tens of millions of dollars.

Tims and Cothron Reaffirm and Multiply the Risks Presented by BIPA

The Court's February 2023 BIPA rulings do not merely continue the trend of outcomes favorable to plaintiffs. Instead, these rulings are likely to exponentially increase damage awards—and risks to defendants—in BIPA class action matters. In particular, Illinois employers that have engaged in biometric data collection are now at significant risk of crippling damage awards.

In *Tims et al. v. Black Horse Carriers, Inc.*, plaintiff Tims sued his former employer, Black Horse Carriers (“Black Horse”), alleging that Black Horse violated BIPA by failing to (1) maintain a biometric information retention and destruction program; and (2) provide notice to or obtain consent from employee plaintiffs for the use of their biometric information. On appeal to the Court, the question presented was whether claims under BIPA (which does not include its own statute of limitations period) fall under a one-year or five-year statute of limitations under the state's civil procedure statutes.⁵ Reasoning that a single statute of limitations “reduce[s] uncertainty and create[s] finality and predictability in the administration of justice,” the Court held that the five-year “catchall” statute of limitations governs all claims brought under the Act.⁶ The Court concluded that the longer limitation period was more consistent with the legislative intent, purpose, and plain language of BIPA, particularly in light of the heightened risk of harm associated with the compromise of biometric information.⁷

² See 740 ILCS § 14/10.

³ See *Id.* at § 14/20. Damages are enumerated as follows: (1) for negligent violations of the law, the greater of \$1,000 in liquidated damages or actual damages; (2) for intentional or reckless violations, the greater of \$5,000 in liquidated damages or actual damages; (3) reasonable attorneys' fees and costs, including expert witness fees and other litigation expenses; and (4) injunctive relief, as the state or federal court may deem appropriate.

⁴ See *Rogers v. BNSF Railway Co.*, 19 C3083 (N.D. Ill. 2022).

⁵ See 735 ILCS 5/13-201; 735 ILCS 5/13-205.

⁶ See *Jorome Tims et al. v. Black Horse Carriers, Inc.*, 2023 IL 127801 ¶120.

⁷ See *Id.* at 32.

Significant Illinois Biometric Information Privacy Act Rulings Create Additional Liability Risk For Companies

In *Cothron v. White Castle System, Inc.*, the Court doubled down on its expansive interpretation of BIPA. There, the plaintiff brought a class action lawsuit against White Castle, alleging that the company violated BIPA by collecting her fingerprint scan without obtaining her written consent to do so.⁸ The plaintiff worked at a White Castle restaurant where biometric information was collected as part of the company's employee timekeeping system. White Castle repeatedly collected the plaintiff's fingerprint scan over a period of several years, but the plaintiff asserted that consent to obtain her fingerprint scan was not obtained until 2018. The Court held that each scan of biometric information constitutes a separate collection—and, therefore, a separate potential claim—under BIPA. In response to White Castle's argument that this approach would lead to crippling damages—in this case, in excess of \$17 billion—the Court referenced its 2019 holding in *Rosenbach v. Six Flags Entertainment Corp.*, in which it recognized the potential for significant damages under BIPA as a way to give entities “the strongest possible incentive to conform to the law and prevent problems before they occur.”⁹ In contrast, the dissenting justices lamented that the majority's interpretation of BIPA was wrong as to the substance and bad policy insofar as it places on businesses the risk of “annihilative liability.”¹⁰

What's Next for Doing Business in Illinois

It is unclear how the Court's expansive reading of BIPA today will incentivize greater protections for biometric information collected in the past. However, these decisions will force companies to rethink the extent to which they collect this information in Illinois moving forward. As a practical matter, the expanded limitations period established in *Tims* will likely lead to significant increases in plaintiff class-size as plaintiffs' attorneys reach further and further back to find allegations of non-compliance, and to a longer period of uncertainty for businesses worried about liability for past—and even long-since corrected—business practices. And both *Tims* and *Cothron* will increase the cost of getting compliance wrong—even for well-intentioned companies—and generally raise the cost of doing business in Illinois.

Together, *Tims* and *Cothron* exponentially increase the already-significant risk for companies that are subject to BIPA. To understand and better quantify that risk and any ongoing BIPA exposure, companies that collect biometric information in Illinois should evaluate any and all current or contemplated uses of biometric information—including the sufficiency of any notice provided to and consent obtained from the individuals from whom the information is collected, record-keeping as to the provision of notice and obtaining of consent, the time period during which such consent has been sought and obtained, the purposes for which such information is collected, and any alternatives to collecting such information that

⁸ See *Latrina Cothron v. White Castle System, Inc.*, 2023 IL 128004 ¶¶ 4-6. As a procedural matter, the suit was being heard in federal district court in Illinois because of diversity with another defendant. White Castle sought to dismiss the case in its entirety, arguing that the statute of limitations had lapsed, but the district court disagreed and rejected White Castle's motion. White Castle appealed the decision to the Seventh Circuit, which then certified the question to the Illinois Supreme Court, concluding that “collection” is not defined under BIPA and, therefore, there was an open question for the Court as to whether claims accrue only at the time of initial collection, or each time biometric data is collected.

⁹ See *Id.* at 41; quoting *Rosenbach v. Six Flags Entertainment Corp.*, 2019 IL 123186, ¶ 37.

¹⁰ See *Id.* at 40.

Significant Illinois Biometric Information Privacy Act Rulings Create Additional Liability Risk For Companies

would accomplish the relevant business objectives. For many companies, this will likely lead to a determination as to whether the efficiency and utility of using biometric information outweighs the daunting risk of BIPA class action litigation.

Barring corrective action by the Illinois legislature, this kind of eye-popping liability will likely become the norm for companies that utilize fingerprint scanning or other biometric identifier technologies without adequate consent. On February 16, 2023, a bill to amend BIPA's private right of action was introduced to the Illinois House of Representatives that would provide a cure period for an entity upon 15 days' written notice of a violation; if the violation is cured, no statutory or class-wide damages may be initiated against an entity.¹¹ While this bill may be a promising development, companies that fall under the scope of BIPA cannot wait for a legislative solution before taking action.

If you have any questions regarding this client alert, please contact the following attorneys or the Willkie attorney with whom you regularly work.

Daniel K. Alvarez

202-303-1125

dalvarez@willkie.com

Michael G. Babbitt

312-728-9070

mbabbitt@willkie.com

Laura E. Jehl

202-303-1056

ljehl@willkie.com

LaRue L. Robinson

312-728-9022

lrobinson@willkie.com

Kari Prochaska

312-728-9080

kprochaska@willkie.com

Copyright © 2023 Willkie Farr & Gallagher LLP.

This alert is provided by Willkie Farr & Gallagher LLP and its affiliates for educational and informational purposes only and is not intended and should not be construed as legal advice. This alert may be considered advertising under applicable state laws.

Willkie Farr & Gallagher LLP is an international law firm with offices in Brussels, Chicago, Frankfurt, Houston, London, Los Angeles, Milan, New York, Palo Alto, Paris, Rome, San Francisco and Washington. The firm is headquartered at 787 Seventh Avenue, New York, NY 10019-6099. Our telephone number is (212) 728-8000 and our fax number is (212) 728-8111. Our website is located at www.willkie.com.

¹¹ See H.B. 3199, 103rd Gen. Assemb. (Ill. 2023) amending 740 ILCS 14/20.