

Biometric Bombshells: Twin Shots Across the BIPA Bow

MARCH 28, 2023

Authors: [Marc S. Blubaugh](#), [Mark S. Eisen](#)

Effective development and deployment of innovative technology is often a key differentiator among providers of transportation and logistics-related services. Of course, innovation can also create certain risks that must be managed carefully. Providers and commercial users of transportation and logistics services should take heed from two recent developments in court that dramatically illustrate the high stakes involved when adopting biometric technology without commensurate compliance measures.

Biometrics are distinct, measurable, human physiological characteristics—such as fingerprints, palms, faces, retinas, voices, and gaits. Increasingly, providers of transportation and logistics services are using biometrics in their daily operations. For example, biometric technology has been used to authenticate truck drivers who are picking up high-value or other critical cargo, to control access to (and within) secure warehouse facilities, to record employee work hours, to lock and unlock containers carrying cargo, and the like. Some particularly common biometric systems include (i) time clocks using fingerprints, (ii) driver monitoring through video recordings, (iii) security access via various scans, and (iv) temperature screenings that use facial recognition. Biometrics can naturally enhance operational security, safety, accuracy, and efficiency, but the use of biometrics can also create meaningful risks if not carefully deployed.

For instance, the Illinois Biometric Information Privacy Act (BIPA), a statute enacted in 2008, creates significant liability exposure for companies in Illinois that collect and use biometric data without complying with specific requirements imposed by BIPA. Considering that many deem Chicago to be the informal logistics capital of North America, BIPA creates an outsized exposure for the transportation and logistics industry. BIPA is also critical because it covers not just biometrics, like fingerprints or retina scans, but also information *based on* biometrics used to identify someone, covering technology and information that may not at first glance appear to be covered.

Massive Verdict in Rail-Motor Carrier Dispute

In October 2022, an Illinois jury entered a \$228 million class action verdict against the BNSF Railway under BIPA. In the case, the class representative, a truck driver for a motor carrier, claimed that the railroad required drivers to provide fingerprints and “related biometric information” in order to gain access to the railroad’s intermodal facilities. However, the railroad allegedly did not obtain written consents from the drivers before collecting and storing this biometric data, all of which was in violation of BIPA requirements. The jury agreed with the drivers and, as the class involved around 45,000 drivers, each of whom could potentially recover \$5,000, the size of the verdict was eye-popping.

Accordingly, even a biometric statute like BIPA that has been in effect for over 15 years continues to create liability exposure for those in the transportation and logistics industry.

New Guidance from Illinois Supreme Court

Just last month, on February 17, 2023, the Illinois Supreme Court issued a decision in *Cothron v. White Castle System, Inc.*, a case which unfavorably resolved the issue of when claims accrue under BIPA. In this putative class action, a manager of a White Castle restaurant argued that employees were required to scan their fingerprints in order to access their paystubs and computers, and that White Castle shared that information with a third party in violation of BIPA.

The Illinois Supreme Court issued a highly fractured, 4-3 decision. However, the majority determined that a new claim under key provisions of BIPA accrues with *each scan* of biometric information. This means that, as a practical matter, plaintiffs pursuing BIPA claims will now argue that a distinct statutory damages claim of up to \$1,000 (or \$5,000 for an intentional violation) accrues upon each and every use of a biometric system. Therefore, one can easily see how damages can add up remarkably fast in the case of an hourly employee clocking in and out for breaks, lunch, and the beginning and end of shifts.

The only silver lining in the *Cothron* decision is the Court's recognition that damages under BIPA are discretionary. That said, a majority of the Court did not appear to bat an eye that White Castle could be facing damages in the amount of *\$17 billion* or more.

Conclusion

The impact of these recent decisions will not be fully known for years, as parties in BIPA cases litigate the facts of their particular cases, including how and when biometric equipment actually collects or captures information, and what actually constitutes a biometric identifier and biometric information under BIPA. Likewise, a variety of other states have also enacted or introduced legislation aimed at regulating the collection and use of biometrics, some of which create private causes of action (such as in California).

In short, the transportation and logistics industry should expect to see an influx of BIPA cases against Illinois transportation businesses and businesses operating in Illinois as well as comparable actions in other states that have similar legislation. As a result, companies that are implementing any biometric system should first implement a compliance program. Among other things, those in the industry are reminded that compliance with any notice and consent requirements under biometric legislation is critical.

For more information on these topics, contact a member of the firm's Transportation & Logistics or Class Action practice groups.

Marc S. Blubaugh is a partner and Co-Chair of Benesch's Transportation & Logistics Practice Group. He may be reached at (614) 223-9382 and mblubaugh@beneschlaw.com.

Mark S. Eisen is a partner and Co-Chair of Benesch's Class Action and Telephone Consumer Protection Act (TCPA) Groups. He may be reached at (312) 212-4956 and meisen@beneschlaw.com.