

Class Action Year in Review: BIPA Class Actions

Article By:

Robert D. Boley

D. Reed Freeman Jr.

Paula M. Ketcham

Adam L. Littman

Eva J. Pulliam

Illinois Biometric Information Privacy Act (BIPA) class action lawsuits were heavily litigated again in 2022, as plaintiffs continued to target companies using biometric technology and their vendors. At the same time, avoiding liability continued to be a challenge for businesses defending BIPA cases.

We [recently reported](#) on the first BIPA class action to go to trial: a \$228 million plaintiffs' verdict. In this latest update, we review noteworthy 2022 court decisions involving a wide range of biometric technologies spanning several industries, including transportation, food service, and higher education.

Regulatory Background

Enacted in 2008, BIPA regulates the collection, use, storage, retention, and destruction of biometric identifiers and biometric information. A "biometric identifier" is a biologically unique personal identifier, including a fingerprint, voiceprint, face geometry, or a retina or hand scan. "Biometric information" is any information based on an individual's biometric identifier used to identify an individual.

Subject to limited exceptions, BIPA generally prohibits the collection or use of a person's biometric identifiers and biometric information without providing notice, obtaining written consent, and developing a publicly available retention and destruction schedule. Companies in possession of biometrics may not profit from the data.

Although other states, such as Texas and Washington, have similar statutes, the Illinois statute provides a private right of action, permitting any person "aggrieved" by a violation to bring suit in state or federal court. The Illinois Supreme Court has held that a person may be "aggrieved" by a

BIPA violation even if their biometric data was never misused, and they were never actually injured. It is sufficient for a plaintiff to point to solely technical violations of the statute. A prevailing plaintiff may recover actual damages or statutory damages of \$1,000 for each negligent violation and \$5,000 for each reckless or intentional violation.

Motor Carrier Industry: Preemption and the Dormant Commerce Clause

In July 2022, an Illinois federal judge denied a motion to dismiss a putative BIPA class action brought by a truck driver against a facial recognition technology provider for interstate motor carriers. *Karling v. Samsara Inc.*, No. 22 C 295, 2022 WL 2663513 (N.D. Ill. July 11, 2022). The defendant, Samsara Inc., developed a dashboard camera that extracted biometric images of drivers' faces to identify and monitor them for fatigue and distraction. The complaint alleged the plaintiff did not give Samsara permission to collect or store his biometric information, nor did he sign a written release.

Samsara moved to dismiss the complaint on preemption grounds, arguing BIPA's requirements disrupt a "uniform scheme of federal regulation of truck safety technology." Samsara did not rely on any particular federal statute. Rather, Samsara cited a variety of Congressional directives, a Department of Transportation website publication, and a Federal Motor Carrier Safety Administration Privacy Impact Assessment relating to equipping commercial vehicles with electronic logging devices, vehicle safety technology, and driver monitoring systems. The court determined the federal sources did not qualify as a uniform regulatory scheme. Although the sources touched on biometrics, the court said their "overwhelming aim" is traffic safety and, theoretically, companies can create truck safety technology while complying with BIPA. At the motion to dismiss stage, based on the allegations of the complaint and without the benefit of outside evidence, the court could not conclude that BIPA conflicts with Congressional intent regarding truck safety technology.

The court also declined to reach Samsara's argument that BIPA is unconstitutional as applied to interstate motor carriers. Relying on the dormant Commerce Clause, Samsara argued BIPA burdens motor carriers and their technology providers and substantially interferes with interstate commerce. However, without discovery into Samsara's process for scanning, storing, and using biometrics and the alleged burden of compliance with BIPA, the court could not determine whether there was a dormant Commerce Clause violation.

Identity Verification Software: Biometric Identifiers v. Biometric Information

In another key BIPA decision, an Illinois federal judge rejected legal defenses raised by biometric software developer Onfido, Inc. *Illinois, Sosa v. Onfido, Inc.*, No. 20-cv-4247, 2022 WL 1211506 (N.D. Ill. Apr. 25, 2022). The plaintiff filed a putative class action alleging Onfido violated BIPA through its facial recognition software. The software scans uploaded images of consumer identification cards and facial photographs to extract a unique numerical representation of each image (often called a "faceprint"). Online businesses use Onfido's software to verify consumer identities.

Onfido moved to dismiss, arguing that information derived from photographs does not qualify as "biometric information" or "biometric identifiers." Onfido relied on the statutory definition of "biometric identifiers," which expressly excludes photographs. The court agreed that information derived from photographs does not constitute biometric *information* under BIPA, but concluded the "faceprints" Onfido created plausibly constitute biometric *identifiers*. The court also rejected Onfido's argument that BIPA does not apply to a scan of a photograph rather than an actual face. The court concluded that nothing in BIPA's text limits it to an "in person" scan.

In addition, the court rejected Onfido's argument that BIPA violates the First Amendment as a content-based restriction on commercial speech. The court concluded BIPA does not restrict Onfido's speech by requiring it to obtain informed consent before collecting an individual's biometric data because BIPA does not restrict what an entity may do with biometric data once it is collected. The court also concluded BIPA is a content-neutral regulation, explaining that the definitions of biometric identifiers and biometric information do not "relate to the communicative content of that information." Because BIPA is a content-neutral regulation, the court applied intermediate scrutiny, concluding BIPA survived because it advanced the government's substantial interest in protecting consumers' rights to privacy and control over their biometric information.

Restaurant Point-of-Sale Technology

In April 2022, an Illinois federal judge held that third-party providers of a point-of-sale (POS) system may be liable under BIPA. See *Ronquillo v. Doctor's Assocs., LLC*, No. 21 C 4903, 2022 WL 1016600 (N.D. Ill. Apr. 4, 2022). A Subway restaurant employee who used the POS system to clock in and out and unlock the registers filed a class action complaint alleging the system's hardware and software providers "collected and obtained her biometric information" without notice. Specifically, the POS system scanned, stored, and used the employee's fingerprints to identify her each time she used the system. The complaint alleged the employee did not consent to the "capture, collection, use, or retention of her biometric information."

The technology providers moved to dismiss the complaint on the basis that BIPA's notice and consent requirements do not apply to third-party vendors of technology an employer uses to obtain its employees' biometric data. The court disagreed, saying BIPA contains no text that limits its reach to employers. The court also rejected the argument that the vendors had no opportunity to obtain consent from Subway's employees, because the vendors could have required Subway, as a "contractual precondition" to use the biometric POS system, to obtain its employees' written consent to the vendors obtaining their data.

Additionally, the court disagreed that the "extraterritoriality doctrine" barred the employee's BIPA claims against a non-Illinois resident. Because the alleged scanning of the employee's fingerprints took place "primarily and substantially" in Illinois, the extraterritoriality doctrine did not apply.

Remote Exam Proctoring in Higher Education

In 2022, Illinois federal courts also addressed BIPA claims in a series of putative class actions brought against higher education institutions and a remote exam proctoring software company called Respondus. In each case, plaintiffs alleged that Respondus's exam software uses student webcams to capture biometric data through scans of students' facial geometry in violation of BIPA. In each case, the schools argued BIPA does not apply to them because they fall within an exemption for "financial institutions" subject to Title V of the Gramm-Leach-Bliley Act. Specifically, the schools argued they qualify as financial institutions because they make and administer student loans. While the schools achieved mixed results, the decisions in these cases suggest that the financial institution exemption could be a potentially winning argument for many schools subject to BIPA suits.

In *Fee v. Illinois Institute of Technology*, No. 21-cv-2512, 2022 WL 2791818 (N.D. Ill. July 15, 2022), the court concluded the financial institution exemption applies to institutions of higher education that are "significantly engaged in financial activities, such as making or administering student loans." In doing so, the court rejected the plaintiff's argument that "financial institution" should encompass only traditional financial institutions, such as banks. The plaintiff argued a broader reading could swallow

BIPA given the prevalence of consumer financing and credit in retail. Nevertheless, the court concluded there was insufficient evidence that the Illinois Institute of Technology was regularly extending or administering student loans and, therefore qualified as a financial institution exempt from BIPA.

Similarly, in *Patterson v. Respondus Inc.*, No. 20-cv-7692, 2022 WL 7100547 (Oct. 11, 2022), the court denied Lewis University's bid for dismissal. Although Lewis University presented evidence that it participates in programs through which its students obtain loans from third-party lenders, it did not establish that the university itself was significantly engaged in lending funds to students.

Finally, and most recently, in *Powell v. DePaul University*, No. 21-cv-3001, 2022 WL 16715887 (N.D. Ill. Nov. 4, 2022), the court dismissed BIPA claims asserted against DePaul University. The court discussed prior court decisions addressing the financial institution exemption in the higher education context, including *Fee* and *Patterson*, and held there is a consensus that the exemption "applies to institutions of higher education that are significantly engaged in financial activities such as making or administering student loans." Unlike *Fee* and *Patterson*, however, the *Powell* court took judicial notice of public records establishing that DePaul University participates in federal student aid programs and provides direct loans to students. On the basis of that evidence, the court concluded that DePaul University qualified as a financial institution exempted from BIPA.

When to Develop Written Retention and Destruction Schedule

In November 2022, an Illinois appellate court held that a company subject to BIPA must develop a written retention and destruction schedule before or at the time it first possesses an individual's biometric data. *Mora v. J&M Plating, Inc.*, 2022 IL App (2d) 210692, 2022 WL 17335861 (2022). In *Mora*, the plaintiff began clocking into work via fingerprint scan in 2014. In 2018, the defendant established a retention schedule and the plaintiff signed the policy. After the plaintiff was terminated in 2021, he filed a class action lawsuit alleging the defendant collected, stored, and used employee fingerprints without first publishing a retention and destruction schedule.

The trial court granted summary judgment for the defendant, holding that BIPA contains no time limit by which a retention schedule must be established, and the defendant ultimately established a schedule as required by the statute. The appellate court reversed, concluding that the duty to develop a written schedule is triggered by possession of the biometric data, meaning the schedule must exist on the initial date of possession, not afterward.

What to Watch Going Forward: Statute of Limitations

As businesses have struggled to defeat BIPA claims, the Illinois Supreme Court is poised to clarify the scope of a key defense—the statute of limitations applicable to BIPA claims—in a pair of pending cases. In *Tims v. Black Horse Carriers*, the Court is reviewing an Illinois appellate court decision holding that a one-year statute of limitations applies to BIPA claims involving "publication" of biometric data and a five-year period applies to other BIPA claims. On appeal, the defendant argues a one-year statute of limitations should apply to all BIPA claims. In *Cothron v. White Castle Systems*, the Illinois Supreme Court will determine whether certain BIPA claims accrue only once upon the initial collection or disclosure of biometric information, or each time a company collects or discloses biometric information.

Companies that collect biometric data should closely monitor the outcome of the *Tims* and *Cothron* cases, as each will significantly affect the number and scope of claims they

may face in BIPA class action litigation.

© 2025 ArentFox Schiff LLP

National Law Review, Volume XIII, Number 17

Source URL: <https://natlawreview.com/article/class-action-year-review-bipa-class-actions>