# A Comprehensive Look at the State of Biometrics Exposures

Updated: March 2023

ProEx

Professional & Executive Risk Practice
www.hubinternational.com/proex

By Whitney Ross & Robin Ann Nowicki

## OVERVIEW

Nearly all businesses that have operations in Illinois are aware of the Illinois Biometric Information Privacy Act ("BIPA") and how they may be vulnerable to litigation if they collect biometric data from employees or third parties. BIPA was enacted in 2008 to regulate how private companies collect, use, and share biometric data. Unfortunately, numerous businesses have already experienced a lawsuit for alleged BIPA violations. With how fast this litigation has evolved, it remains critical to stay current on the recent cases filed, settlements approved by the courts, *a **first ever jury verdict***, new targets for BIPA claims, and other states' efforts to pass similar legislation. Each of the foregoing continues to greatly impact the way businesses, and their insurance carriers, view BIPA exposures.

### *What is (and is not) biometric data?*

Biometric data, in its simplest form, is individual biometric identifiers unique to each person. Biometric identifiers under BIPA include retina or iris scans, fingerprints, voiceprints, or the scan of hand or face geometry.[1] Biometric identifiers do *not* include writing samples, written signatures, photographs, human biological samples used for valid scientific testing or screening, demographic data, tattoo descriptions, or physical descriptions such as height, weight, hair color, or eye color.[2] Biometric identifiers also exclude information captured from a patient in a health care setting or information collected, used, or stored for health care treatment, payment, or operations under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), as well as x-rays, MRI's, PET scans, and other images used to diagnose, prognose or treat medical conditions.[3] Biometrics are biologically unique to the individual and, once compromised, cannot be changed.[4]

### *What are the requirements of BIPA?*

BIPA was enacted to protect individuals' biometric data that is collected, stored, or shared. To comply with BIPA, a business in possession of biometric identifiers or biometric information must:

[1] Biometric Information Privacy Act, 740 ILCS Section 10.
[2] *Id*.
[3] *Id*.
[4] *Id*.

- Develop a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and information.
- Inform individuals in writing that a biometric identifier is being collected or stored, and the purpose and length of time for which biometric information is being collected, stored, and used.
- Receive a written release from the individual.
- Refrain from selling, trading, leasing or otherwise profiting from a person's biometric information.
- Refrain from disclosing, redisclosing, or otherwise disseminating a person's biometric information unless consent is provided (or if required in limited circumstances).
- Use reasonable standards of care in storing, transmitting, and protecting from disclosure biometric identifiers consistent with the standard of care within the company's industry, and in a manner that is more protective than the manner in which the company stores, transmits, and protects other confidential and sensitive information (i.e., social security numbers, bank information, etc.).

### *Who can file a BIPA lawsuit?*

One of the unique characteristics of the statute is the ability for an individual to bring a private right of action, which allows recovery for damages. For negligent violations, the statute provides a prevailing plaintiff with liquidated damages of $1,000 or actual damages (whichever is greater). For intentional or reckless violations, the statute provides a prevailing plaintiff with liquidated damages of $5,000 or actual damages (whichever is greater). Plaintiffs' attorneys' fees and costs and other relief (including expert witness fees) is likewise available under the statute.

The landmark Illinois Supreme Court case of *Rosenbach v. Six Flags Entertainment Corp.* makes clear that no actual injury or adverse effect, beyond violation of an individual's rights under BIPA, needs to occur for a plaintiff to qualify as an aggrieved person and have standing to sue. 2019 IL 123186 (Jan 25, 2019). *Rosenbach* has essentially opened the floodgates to BIPA class action filings by both consumers and employees – despite claims of little to no actual damages.

### *What statute of limitations applies to BIPA?*

Interestingly, BIPA does not specify a statute of limitations. As a result, this has long been the subject of debate between plaintiffs and defendants. For defendants, the answer is critical to both the defense strategy and the size of a class in connection with a settlement or verdict. It has been suggested that a one-, two-, or five-year statute of limitations applies to BIPA claims. Plaintiffs argue that the five-year statute of limitations applies, which is typically applied to

laws that do not expressly include a statute of limitations. For plaintiffs, a longer statute of limitations potentially weakens the defense and opens the class period for a bigger payout.

On the other hand, defendants argue that either a one- or two-year statute of limitations applies to BIPA claims, since other invasion of privacy laws carry a one-year statute of limitations and statutes that include statutory penalties carry a two-year statute of limitations. For defendants, a shorter statute of limitations narrows the class period and creates leverage when negotiating a settlement.

This issue was decided by the Illinois Supreme Court on February 2, 2023 in the case entitled *Tims v. Black Horse Carriers, Inc.*, No. 127801 (Ill.). In *Tims*, the trial court denied the defendant's motion to dismiss on limitation grounds and certified this question to the Illinois Appellate Court: whether the limitation period in section 13-201 (one year) or section 13-205 (five years) of the Code of Civil Procedure applies to claims under BIPA. 735 ILCS 5/13-201, 13-205 (West 2018). The Illinois First District Appellate Court previously split their decision based on which section of BIPA is implicated holding that a one-year period from 735 ILCS 5/13-201 applies to BIPA sections 15 (c) and 15 (d) because they involve "publication" of biometric data and a five-year limitations period from 735 ILCS 5/13-205 applies to sections 15(a), (b), and (e) because these do not involve publication. *See Tims v. Black Horse Carriers, Inc.*, 2021 IL App (1st) 200563. The Illinois Supreme Court overturned the Appellate Court's approach and held that a five-year limitations period controls any claim brought under BIPA.

## LITIGATION UPDATES

The below update discusses a first ever BIPA jury verdict in *Richard Rogers v. BNSF Railway Company,* No. 1:2019cv03083 (N.D. Ill.) ("BNSF Litigation") and a defensive trend in litigation against higher education in *Cody Powell v. DePaul University, No.:* 21 C 3001 (N.D. Ill. Nov. 4, 2022) ("DePaul Litigation"). It also touches upon new technologies landing one company in the BIPA litigation foray in *Flora, et al. v. Prisma Labs, Inc.*, No. 5:23-cv-00680 (N.D. Cal.) ("Prisma"). Further, a divided Illinois Supreme Court decided the accrual question of whether there is a separate claim each time an entity scans or transmits an individual's biometric information or only upon a first scan and transmission in *Cothron v. White Castle Sys., Inc.,* 2023 IL 128004 (Feb. 17, 2023) ("White Castle").

### *BNSF Litigation*

While BIPA was enacted in 2008, it is not until now, on October 12, 2022, that the first class action trial based on the legislation has gone to verdict. The BNSF Litigation resulted in a $228 million verdict for the class members. The plaintiff, Richard Rogers, a truck driver and former employee of BNSF Railway Company ("BNSF"), filed the class action lawsuit alleging that BNSF collected biometric information in violation of BIPA by requiring a fingerprint scan to enter its facilities without a written release or providing required notice and disclosures. Throughout the litigation, BNSF denied that it operated the scanner and tried to shift

responsibility onto a third-party vendor who, BNSF alleged, was responsible for the data collection and storage. Prior to trial, the court held that the "otherwise obtain" language of the statute is broad enough to include entities that hire third-party vendors to collect or store the information. *See* 740 ILCS 14/15(b) and *Rogers*, No. 1:2019cv03083 (N.D. Ill. Sept. 26, 2022). After a one-week trial the jury reportedly took only an hour to deliberate and found that BNSF violated BIPA 45,600 times, which is one violation per individual who made up the class. The $228 million amount was derived by applying the $5,000 statutory damage per reckless or intentional violation to each of the 45,600 plaintiffs.

### *DePaul Litigation*

On November 4, 2022, the Northern District of Illinois granted DePaul University's ("DePaul") Motion to Dismiss the class action lawsuit alleging its use of an online remote proctoring tool, Respondus Monitor, violates BIPA by not disclosing or obtaining written consent to capture, use, and store a student's biometric identifiers. BIPA does not apply to Title V of the Gramm-Leach Bliley Act, that regulates how financial institutions treat nonpublic personal information about consumers. *See* 740 ILCS 25(c). DePaul argued in its motion that "like all other colleges and universities with federally authorized financial aid programs, it is a financial institution that is subject to Title V of the GLBA and must comply with its implementing rules" and, because of this, it is exempt from adhering to BIPA. *See Powell v. DePaul Univ.*, 21 C 3001, 2 (N.D. Ill. Nov. 4, 2022). The court stated, "[a]t least five courts have reached this exact issue, and all have concluded that the exemption in BIPA section 25(c) applies to institutions of higher education that are significantly engaged in financial activities such as making or administering student loans." *See Id. at* 4 (N.D. Ill. Nov. 4, 2022) citing *Doe v. Elmhurst Univ.*, 2020 L 1400 (Ill. Cir. Ct. Nov. 18, 2021); *Doe v. Northwestern University*, No. 21-cv- 1579 Dkn. No. 31 at 3 (N.D. Ill. Feb. 22, 2022); *Deurr v. Bradley University*, 2022 WL 1487747 at *6-7, (C.D. Ill. March 10, 2022); *Fee v. IIT*, 2022 WL 2791818 at *5 (N.D. Ill. July 15, 2022); *Patterson v. Respondus, Inc.*, 2022 WL 7100547 (N.D. Ill. October 11, 2022).

### *Prisma*

Artificial Intelligence ("AI") has been in the headlines for a majority of 2023 thus far. It also made headlines on February 15, 2023, because Prisma Labs, Inc., the developer of the Lensa app that allows users to edit and retouch "selfies," was sued by a group of its customers alleging BIPA violations. The app scans a user's "facial geometry" and creates custom avatars - all in violation of BIPA, according to the plaintiffs. Interestingly, this class action was brought by the same law firm, Loevy & Loevy, that won the *BNSF* verdict. So, while this new technology is starting to take off, it is not immune from BIPA litigation.

### *White Castle*

On February 17, 2023, the Illinois Supreme Court decided the issue of whether BIPA allows for a "per scan" violation or a single violation per plaintiff in *Cothron v. White Castle Sys.,*

*Inc.,* 2023 IL 128004 (Feb. 17, 2023). The Court held that there is a separate claim each time an entity scans or transmits an individual's biometric identifier or information rejecting White Castle's argument to limit claims to the first time an entity scans or transmits a party's biometric information. The Court did, however, note that the statute is not intended to cause the financial destruction of a business because it uses the phrase, "prevailing party *may* recover" finding that the Illinois Legislature clearly intended to make damages discretionary, rather than mandatory. The Court also called upon the Illinois Legislature to address the concerns about potentially excessive damage awards and "make clear its intent regarding the assessment of damages under the ACT." White Castle's counsel has stated that they are reviewing options to seek further judicial review because there was a strong dissenting opinion that raises concerns about the opinion.[5]

### *Takeaways*

The *BNSF* Litigation and the *White Castle* decision should be concerning for companies that collect biometric data. These decisions show that significant damage awards could be issued against companies that do not follow BIPA. Additionally, *BNSF* provides that those companies that outsource the collection and storage of biometric data can be held statutorily liable under BIPA for functions provided by third-party vendors. This verdict and the Supreme Court decision may open a floodgate of litigation. On the other hand, the DePaul Litigation provides yet another case highlighting that higher education could be precluded from BIPA violations based on their financial institution status.

## STATUS OF STATE REGULATION

There is no singular federal law governing biometric data. There are currently three states that have comprehensive biometrics privacy laws, including Texas, Washington, and Illinois. In 2020, several states introduced biometric legislation without success, including Arizona, New Hampshire, South Carolina, and West Virginia.[6] Although Illinois remains the only state which allows a *private* right of action, it appears in 2023 other states are moving in that direction. Arizona, Hawaii, Kentucky, Maryland, Massachusetts, Minnesota, New York, Tennessee, and Vermont have proposed legislation mirroring BIPA with private rights of action.[7] Interestingly, a proposed update to Washington's Privacy Act broadening its current scope to include a private right of action failed to pass the state legislature.[8]

---

[5] Illinois Supreme Court Allows Big Biometric Privacy Fines (3) (https://new.bloomberglaw.com/privacy-and-data-security/illinois-justices-allow-big-biometric-fines-in-white-castle-case-6?source=newsletter&item=body-link&region=text-section)
[6] U.S. Biometrics Laws Part 1: An Overview of 2020 (https://www.jdsupra.com/legalnews/u-s-biometrics-laws-part-i-an-overview-2275684/)
[7] 2023 State Biometric Privacy Law Tracker (https://www.huschblackwell.com/2023-state-biometric-privacy-law-tracker) last accessed 3/6/2023.
[8] Washington State's Privacy Bill Emerges as National Model, Despite Failure Over Private Right of Action (https://www.law.com/legaltechnews/2022/05/06/washington-states-privacy-bill-emerges-as-national-model-despite-failure-over-private-right-of-action/)

Interestingly, in 2021, New York City passed a biometrics law of its own that is similar to BIPA. New York City's Biometric Identifier Information Law (§22-1202 of the New York City Administrative Code) went into effect on July 9, 2021. The law applies to "commercial establishments" that collect, retain, convert, store or share biometric information from customers. "Commercial establishments" include places of entertainment (i.e., any privately or publicly owned and operated entertainment facilities such as theaters, stadiums, racetracks, museums, amusement parks, etc.), retail stores, and food or drink establishments.

§22-1202(a) of the New York City Administrative Code requires that any commercial establishment that collects, retains, converts, stores or shares biometric identifier information of customers must disclose such collection, retention, conversion, storage or sharing, as applicable, by placing a clear and conspicuous sign near all of the commercial establishment's customer entrances notifying customers in plain, simple language, in a form and manner prescribed by the commissioner of consumer and worker protection by rule, that customers' biometric identifier information is being collected, retained, converted, stored or shared, as applicable.

Moreover, §22-1202(b) of the New York City Administrative Code provides that it shall be unlawful to sell, lease, trade, share in exchange for anything of value or otherwise profit from the transaction of biometric identifier information.

Like the Illinois BIPA statute, the New York City Administrative Code gives consumers a *private right of action* for violation of the law. Damages range from $500 per violation for negligent violations to $5,000 per violation for intentional/reckless violations, plus attorneys' fees (including expert witness fees and other litigation expenses). That said, before an aggrieved person can file suit for failure to disclose under §22-1202(a), they must give the offending party written notice at least 30 days prior to initiating any action accusing a commercial establishment of violating the Code. If, within 30 days, the commercial establishment cures the violation and provides the aggrieved person an express written statement that the violation has been cured and that no further violations shall occur, no action may be initiated against the commercial establishment for such violations. If, on the other hand, the commercial establishment continues to violate §22-1202(a), the aggrieved person may initiate an action against such establishment. No prior written notice is required for alleged wrongdoing in violation of §22-1202(b) for the alleged selling, sharing or profiting from a customer's biometric information (as discussed above).

As anticipated, New York City followed Illinois in allowing a private right of action for aggrieved consumers. With additional legislation being passed allowing for a private right of action that includes an award of attorneys' fees, we will see continued efforts by plaintiffs' firms to capitalize on the evolution and expansion of state regulated biometrics.

Given the number of lawsuits filed in Illinois alone – and the significant costs associated with defending and settling those lawsuits (not to mention the recent $228M jury verdict) – if any other states, like Arizona, Hawaii, Kentucky, Maryland, Massachusetts, Minnesota, New York, Tennessee, and Vermont mentioned above, successfully pass legislation that mirrors BIPA, plaintiffs' firms will seize the opportunity for a payout in this niche industry. Therefore,

companies need to mitigate the risk of biometrics litigation by creating robust internal biometrics policies, obtaining written consent, prohibiting the sale of information, and staying current on new laws, among other things. Even with careful management and planning, however, companies should prepare to be the subject of biometrics litigation.

## COVERAGE CONSIDERATIONS

Insurance carriers have also been hit hard with BIPA claims under policies issued to insureds doing business in Illinois. Settlements have ranged from $1.8 million to $650 million, with plaintiffs' attorneys recovering, on average, 30-40% of that amount. Along with the recent *BNSF* jury verdict and *White Castle* decision, it is no wonder why these firms are continually looking for class representatives to file suit, especially given that there remains no requirement that plaintiffs prove actual harm under the Illinois Supreme Court's decision in *Rosenbach*.

It is important to understand what coverage an insured may have under its insurance policies for BIPA claims. Recently, carriers have been pulling back on coverage for BIPA claims in a myriad of ways. Insurance policies that may respond to a BIPA lawsuit include the Cyber liability and Employment Practices Liability ("EPL") policies.[9] EPL policies may be triggered if the plaintiffs are employees of the insured and allege that the insured invaded their privacy in connection with their employment in violation of BIPA. Cyber policies may be triggered whether the plaintiffs are employees or consumers of the insured. As discussed, however, the Cyber and EPL policies could include limiting language and create roadblocks to coverage. For example, Cyber policies may contain a "collections exclusion," and limitations to the definition of "Loss" for fines and penalties. Carriers may attempt to apply these terms of the Cyber policies to limit or preclude coverage for defense costs and/or settlements. EPL policies may narrow the definition of Employment Practices Wrongful Acts to limit or eliminate coverage for privacy violation claims and may also rely on the limitations to the definition of "Loss" for fines and penalties, among other things.

At renewal, carriers are requesting that many businesses fill out questionnaires related to BIPA exposures. Carriers that have been impacted by BIPA litigation and resulting payouts have also added BIPA sub-limits or BIPA exclusions. Insureds that collect or store data (fingerprint, facial recognition) can expect to see some modification of coverage.

As the state of biometrics litigation continues to evolve, it is crucial for businesses to understand their coverage, seek guidance from their brokers regarding their coverage, and work with qualified claims advocates in the event they are the subject of a BIPA lawsuit that could be covered under their insurance policies. HUB's **Professional & Executive Risks –**

[9] In addition to Cyber and EPL policies, companies should also review their General Liability policies for potential coverage (although coverage may be precluded by, among other things, the employment exclusion that is common to General Liability policies).

ProEx practice works closely with Cyber and EPL carriers in connection with BIPA exposures, both on the placement and claims side. The ProEx Claims & Legal Risks Group has a tremendous amount of experience handling BIPA litigation and navigating the coverage available. If you have any questions regarding BIPA claims, risk exposures or coverage options, please reach out to:

**David Garrigus**
Executive Vice President & North American Practice Leader
Professional & Executive Risks – ProEx
david.garrigus@hubinternational.com | LinkedIn

## About the Authors

***Whitney Ross*** is an Executive Vice President and North American Claims Leader for HUB International. Whitney specializes in management liability and cyber insurance coverage. Whitney is a licensed attorney, and previously worked at Chicago-based law firms as coverage counsel for various domestic and international insurance companies. **LinkedIn**

***Robin Ann Nowicki*** is a Senior Vice President and National Cyber Claims Leader at HUB International. Robin Ann is a licensed attorney and has her LL.M. in Information Technology & Privacy Law. Robin Ann's experience includes policy negotiations and drafting, and litigating coverage disputes at both the trial and appellate levels. **LinkedIn**