



PROGRAM MATERIALS

Program #30139

June 9, 2020

Biometrics Class Actions

**Copyright ©2020 by Gregory Abrams, Esq. and Sylvia
Bokyoung St. Clair, Esq. - Faegre Drinker Baker & Reath
LLP.**

All Rights Reserved.

Licensed to Celesq®, Inc.

Celesq® AttorneysEd Center

www.celesq.com

5301 North Federal Highway, Suite 180, Boca Raton, FL 33487

Phone 561-241-1919

Fax 561-241-1969

Biometric Information Class Action Lawsuits – Is Your Company Ready?

Gregory P. Abrams

Sylvia Bokyoung St. Clair



Bio



Gregory P. Abrams
+1 312 356 5047
gregory.abrams@faegredrinker.com



Sylvia Bokyoung St. Clair
+1 312 356 5029
sylvia.stclair@faegredrinker.com

Overview of Webinar

- 1. Biometric Information Privacy Act**
- 2. Compliance, Policies, and Training**
- 3. Everchanging Landscape under BIPA**
- 4. Strategies for Navigating Class Action Lawsuits under BIPA**

What is BIPA?

- **740 ILCS 14 – Biometric Information Privacy Act**
- **Effective October 3, 2008**
- **“The use of biometrics is growing in the business and security screening sectors and appears to promise streamlined financial transactions and security screenings.”**
- **Biometrics are unlike other unique identifiers that are used to access finances or other sensitive information. For example, social security numbers, when compromised, can be changed. Biometrics, however, are biologically unique to the individual; therefore, once compromised, the individual has no recourse, is at heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions.**
- **Generally, BIPA regulates, but does not forbid, the collection and storage of biometrics.**

Defining Biometrics

- The law defines **biometric identifiers** as a “retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry.” 740 ILCS 14/10.
 - Affirmatively excludes other data points such as 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, donated parts, blood/serum, and biological materials regulated by state law.
- "**Biometric information**" means any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual.

Common Uses of Biometrics in the Workplace

- **Timekeeping**
- **Electronic security and building access**
- **Accessing workplace equipment**
- **Safety and security**

Covid-19 and Temperature Screening

- **Non-contact infrared thermometers that use lasers to measure temperature from a distance;**
- **Thermal imaging cameras that detect elevated skin temperatures compared against a sample of average temperature values;**
- **Monitoring systems that use thermal and color visual imaging to detect fevers in high-volume pedestrian areas; and**
- **“Wearables” that can use radiometric thermometry measuring electromagnetic wave emissions.**

The Requirements of Bipa

- **Under BIPA, private entities that possess biometric identifiers or biometric information must store, transmit, and protect the identifiers and information:**
 - Using the reasonable standard of care within the employer's industry
 - In the same (or a more protective) way that the entity stores, transmits, and protects other confidential and sensitive information
- **BIPA defines confidential and sensitive information as personal information that can be used to uniquely identify an individual or an individual's account or property, such as:**
 - A genetic marker.
 - Genetic testing information.
 - A unique identifier number to locate an account or property.
 - An account number.
 - A PIN number.
 - A passcode.
 - A driver's license number.
 - A social security number.

Complying with BIPA

- **Written notice that includes the purpose and length of the collection**
- **Obtain informed written consent**
- **Maintain a publicly available retention schedules and destruction guidelines**

Additional Consent Requirements

- **Before disclosing biometric data to third parties, an entity must first obtain consent, with certain exceptions. 740 ILCS 14/15(d)(1).**
- **Forbids organizations from “selling” or “otherwise profiting from” individuals’ biometric information.**

Why BIPA is a Big Deal

- **Sec. 20. Right of action.** Any person **aggrieved** by a violation of this Act shall have a right of action in a State circuit court or as a supplemental claim in federal district court against an offending party. A **prevailing party** may recover for each violation:
 - 1) against a private entity that negligently violates a provision of this Act, liquidated damages of \$1,000 or actual damages, whichever is greater;
 - 2) against a private entity that intentionally or reckless violates a provision of this Act, liquidated damages of \$5,000 or actual damages, whichever is greater;
 - 3) reasonable attorneys' fees and costs, including expert witness fees and other litigation expenses; and
 - 4) other relief, including an injunction, as the State or federal court may deem appropriate.

BIPA Litigation

- **To date, class action plaintiffs have focused most on allegations that organizations failed to comply with BIPA's notice and consent mandates, as well as not maintaining a publicly available retention policy. Some cases also allege improper disclosure.**
- **Two types of fact patterns have emerged: 1) improper use of facial recognition or similar technology; and 2) improper collection and use of fingerprints or handprints, primarily in the employment context.**

Fingerprint Litigation

- **This complaint arises in the employment context, where hourly employees use their fingerprints to clock in and out of work.**
- “Plaintiff arrived for work, and when he left or clocked in or out of work, at relevant times during his employment, Roundy’s required him to submit his fingerprint to its timekeeping computer system. The system captured, collected, extracted, recorded, stored, and used his biometrics. Roundy’s further required Plaintiff to scan his fingerprint and swipe an identification card in order to use the biometric system, so that the timekeeping system captured, collected and matched his fingerprint biometrics, and associated his biometrics with his identity.” See Complaint, Baron v. Roundy’s Supermarkets, Inc., 2017-CH-03281 at ¶ 29 (Cook Cty. March 7, 2017).

Actual Damages Not Required

- ***Rosenbach v. Six Flags Entertainment Corp.*, 129 N.E.3d 1197 (Ill. 2019)).**
- The Illinois Supreme Court has held that a person whose rights under BIPA were violated can be considered "aggrieved" under the statute.
- Such an individual need not plead actual damages, and may recover liquidated damages, attorneys' fees and costs, and injunctive relief under BIPA.

Since Rosenbach

- ***Rottner v. Palm Beach Tan* (1st Dist. March 4, 2019):**
 - “We believe that the Supreme Court was clear, and will apply the holding of *Rosenbach*...we find that Rottner, like *Rosenbach*, has standing to sue and has adequately stated a claim for liquidated damages ... even if she has alleged only a violation of the Act and not any actual damages beyond violation of law.”
- **Since *Rosenbach* was decided on Jan. 25, 2019 hundreds of cases have been filed in state and federal courts.**

Article III Standing Under Spokeo

- To establish Article III standing to sue in federal court, a plaintiff must suffer an injury in fact (*Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1547 (2016) (Article III standing requires a concrete injury even in the context of a statutory violation)). Some federal courts have held mere technical violations of BIPA, without more, are insufficient to confer Article III standing.
- The Ninth Circuit has found technical violations are sufficient for standing. *Patel v. Facebook, Inc.*, 932 F.3d 1264 (9th Cir. 2019).

Seventh Circuit Finds Article III Standing

- ***Bryant v. Compass Group USA, Inc.*, 958 F.3d 617 (7th Cir. 2020)**
 - Section 15(b) of BIPA protects personal legal rights in individuals' unique biometric information and the right to give informed consent prior to relinquishing such rights.
 - Allegations of a violation of Section 15(b) asserts a violation of personal legal rights sufficient to establish the concrete-harm requirement under the Article III standing inquiry.
 - Section 15(a) of BIPA imposes a duty to the general public to publish retention schedules and destruction guidelines. The court concluded that standing did not exist for claims made under Section 15(a) where the plaintiff alleged "no particularized harm."

How to Minimize Risk in a BIPA Lawsuit

- **The best way to avoid BIPA penalties is to comply with BIPA's requirements, specific disclosures, and receipt of a written release prior to the collection of biometric data**
- **Initiate an internal audit to determine if your company is using biometric data for any reason**
- **Best practices for developing BIPA compliance policies, procedures, and training**

The Constitutionality of BIPA

- **Constitutionality of BIPA**
- **Personal Jurisdiction**
 - Despite being an Illinois law, the plaintiffs' bar has been aggressive in pursuing organizations based outside of Illinois, or with only minimal operations in the state. This has naturally given rise to disputes over personal jurisdiction. These arguments typically arrive in the context of website operators without a physical presence in the state.

Does the Data Constitute Biometric Information?

- **The scope of what is considered a “biometric identifier” is largely untested**
 - While this issue has been discussed in the facial recognition context, it is likely to expand as BIPA litigation continues to expand.
 - For instance, in the fingerprint context, some complaints allege that the storing of mathematical representations of fingerprints fall under BIPA’s definition of biometric information, while defendants argue that such representations fall outside of BIPA.

What Statute of Limitations Applies

- **One year**: Under 735 ILCS 5/13-201, one year SOL applies to certain privacy rights such as “slander, libel, and publication of matter violating the right of privacy.”
- **Two years**: Under 735 ILCS 5/13-202, two-year SOL applies to both personal injury suits and statutes which provide for a “statutory penalty.”
- **Five years**: Under Illinois’ “catch-all” SOL, a period of five years applies. 735 ILCS 5/13-205.
- ***Tims v. Black Horse Carriers, Inc.*, 2019-CH-03522 (Ill. Cir. Ct. Cook Cnty.)**

You've Been Sued with a Class Action Lawsuit Alleging Violations of BIPA – Now What?

- **But if a lawsuit has been filed, and the company is faced with allegations that it has not complied with BIPA, here are a few strategies to help minimize the potential damage.**

Initial Considerations

- **Removal to federal court?**

Potential Defenses to the Merits of a BIPA Claim

- **Sources for express or implied consent**
- **Challenge jurisdiction**
 - BIPA applies only to conduct that occurs primarily and substantially in Illinois
- **Statute of limitations**
- **Workers Compensation Exclusivity**
- **No Negligence or Recklessness**

How Various Class Action Defenses Might be Used in BIPA Actions

- **Limit the scope of the class by geography and time**
- **Rule 23 requirements**
- **Federal due process violation**

Questions and Answers

