Why BIPA Litigation Could Be A Death Knell To Cannabis Cos.

By **Amy Rubenstein and Sarah Trevino** (November 23, 2022)

Amy Rubenstein

Sarah Trevino

Since 2021, Illinois courts have approved almost $1 billion in settlements for Biometric Information Privacy Act claims.

In 2008, the Illinois General Assembly adopted BIPA in response to increased commercial use of biometric data.[1] Biometric identifiers are biologically unique and include fingerprints, voiceprints, retina or iris scans, and face geometry.[2]

Between 2008 and 2017, about 40 cases were filed for alleged BIPA violations. But in the last five years, over 250 cases were filed for alleged BIPA violations — approximately a 525% increase.

This exponential spike in cases include consumer and employee class actions alleging that businesses ran afoul of BIPA while engaging in their lawful daily operations.

Many businesses must protect consumers and employees by using personal identifiers to enter or exit facilities, access computer systems, operate registers, or open cases.

For the relatively nascent legal cannabis industry in Illinois, risky and expensive BIPA litigation could be a fatal blow.

The Clash Between BIPA and the Cannabis Industry

The cannabis industry has placed a strong emphasis on security for grow facilities and dispensaries.

These enhanced security measures are a must to protect employees handling largely cash transactions and customers purchasing a heavily regulated product.

But, in taking these reasonable security measures, the cannabis industry has opened itself up to litigation surrounding BIPA's stringent requirements.

BIPA regulates how private entities may collect and handle biometric data and provides a private cause of action for any person aggrieved by a violation of the statute.[3]

Section 15(b) of BIPA prohibits a private entity from collecting, capturing, purchasing, receiving through trade, or otherwise obtaining a person's biometric data without first providing notice to and receiving consent from the person.[4] Section 15(d) prohibits a private entity from disclosing, redisclosing or otherwise disseminating biometric data without consent.[5]

A plaintiff can recover the greater of actual damages or statutory damages of $1,000 for each negligent violation and $5,000 for each reckless or willful violation, as well as attorney fees.[6]

But BIPA does not evaluate or balance the benefits created by enhanced security or that

other laws and regulations often require businesses to undertake appropriate security measures to safeguard consumers and employees.

Instead, this question matters most to BIPA: Did the business provide written notice and obtain consent? Both must happen to comply with BIPA.

While notice and consent requirements may not be too onerous in some contexts, often a company slapped with a BIPA claim stands several steps away from where the biometric information allegedly was collected and has never interacted with the claimants.

Among the alphabet soup of regulatory requirements for cannabis businesses, BIPA presents another trap for the unwary. As of 2020, Illinois has passed laws allowing for medicinal and adult-use recreational cannabis.

In just two years, Illinois has 110 dispensaries and in June, the Illinois Department of Agriculture awarded 48 licenses for adult-use craft growers, infusers and transporters.[7]

These new, legal, cannabis businesses must operate securely, particularly given their banking challenges and a regulated product. Modern security measures can implicate BIPA.

At least one cannabis retailer has been targeted under BIPA. A former employee has sued 4Front Ventures for alleged BIPA violations related to fingerprint scanning by the company's time clocks.[8]

The employee alleged that the company required employees to clock in and out on a device that used their fingerprints and failed to follow BIPA's detailed notice and consent requirements.

Although a motion to dismiss currently is pending, many courts have shown reluctance to grant motions on the pleadings.

BIPA Damages Could Be a Death Knell to Cannabis Operators

BIPA subjects private entities who fail to follow the statute's requirements to substantial potential liability, including:

- Liquidated damages;
- Injunctions;
- Attorney fees; and
- Litigation expenses for each violation of the law whether or not actual damages, beyond violation of the law's provisions, can be shown.[9]

But what counts as a violation of BIPA? Is each time an entity collects biometric information a violation or do all the collections from one person comprise one violation?

Because BIPA was enacted 14 years ago, several district courts have inferred, for pleading purposes, that a defendant was at least negligent for failing to comply with BIPA today — which carries a $1,000-per-violation price tag.[10]

Some courts have gone further, concluding that a defendant's alleged failure to comply with BIPA permits an inference of recklessness or intent — which carries a $5,000-per-violation price tag.[11] Further upping the ante, plaintiffs counsel can collect attorney fees as well, often upward of 15% of a settlement value.

This month, jurors in Rogers v. BNSF Railway Co. in the U.S. District Court for the Northern District of Illinois[12] handed down a $228 million verdict in favor of the lead plaintiff.

There, the jurors were asked to mark on the verdict form how many times BNSF violated the statute negligently or recklessly.

They found that BNSF recklessly or intentionally violated the law 45,600 times — the estimated number of drivers who had their fingerprints registered. If a per-class member verdict equals $228 million, imagine what a per-scan verdict looks like?

One thing is for certain: BIPA cases have become costly to defend, take to trial and settle. Fearing an exorbitant verdict like in BNSF, many companies have elected to settle, in the millions and hundreds of millions. For example:

- A $650 million settlement by Facebook Inc., now known as Meta Inc., called a "landmark result" in In re: Facebook Biometric Information Privacy Litigation in the U.S. District Court for the Northern District of California.[13]

- A $92 million class action settlement by video-sharing app TikTok Inc. in In re: TikTok Inc. Consumer Privacy Litigation in the U.S. District Court for the Northern District of Illinois.[14]

- A $100 million dollar settlement concerning allegations that Google LLC violated BIPA in Rivera v. Google LLC in the Circuit Court of Cook County, Illinois.[15]

- Snap Inc. recently agreed to a $35 million settlement for users of its lenses or filters, with a final hearing scheduled Nov. 17, in Boone v. Snap Inc. in the Circuit Court of DuPage County, Illinois.[16]

Two primary issues have generated significant BIPA arguments across Illinois: Claim accrual and whether an entity must take an active step to collect, capture, purchase, receive or otherwise obtain biometric data.

These issues directly affect cannabis companies that use biometric security.

Is there a claim for every time an employee opens a register with a fingerprint, or only a claim as to each employee? What party is responsible for BIPA compliance if a cannabis company uses a vendor and third party equipment for its security measures?

Claim Accrual

In Latrina Cothron v. White Castle System Inc. in the U.S. Court of Appeals for the Seventh Circuit in 2021, the issues related to claim accrual and damages resulting from such accrual arose.

The Seventh Circuit, calling BIPA claim accrual novel and expressing its genuine uncertainty

about the issue, certified the question to the Illinois Supreme Court on Dec. 20, 2021.

Three days later, the Illinois Supreme Court accepted the certified question.

White Castle argued that the claims accrue on the first loss of the right to control biometric information, and does not continuously accrue. Among many amicus briefs, the Illinois Chamber of Commerce and the U.S. Chamber of Commerce posed the following example:

> Suppose an employee works 5 days a week for 48 weeks a year and clocks in and out of work via a fingerprint scanner once each day. Over just a single year, a "per-scan" accrual rule would imply 480 violations of [BIPA] and a "per-disclosure" accrual rule would imply another 480 violations). ... That would result in a statutory award of $960,000 to $4,800,000 in liquidated damages for one plaintiff in one year. ... Moreover, depending on the applicable statute of limitations ... damages could extend for up to five years, producing a potential award of roughly $5 to $25 million for a single employee. If the employee similarly clocked in and out for lunch or other breaks, that amount could easily double or triple.[17]

It noted that many courts have recognized that, taken to its logical conclusion, a per-scan or per-disclosure accrual rule "would lead [defendants] to potentially face ruinous liability."[18]

Cothron argued that the claims accrue continually and that BIPA's ban on redisclosure forecloses White Castle's proposed accrual rule[19] and the Illinois Supreme Court's 2019 holding in Rosenbach v. Six Flags Entertainment Corp. supports continuous accrual.

There, the court explained that BIPA generally protects a person's right to privacy in and control over their biometric data, and that the provisions in Section 15 define the contours of that right.[20] A plaintiff may sue without showing injury beyond a simple violation of the statute.[21]

The Illinois Supreme Court has yet to rule on the issue, leaving open the devastating implications of an accrual rule based on Cothron's per-scan theory.[22]

Active Steps

Some courts are also beginning to require an active step to collect, capture, purchase, receive through trade or otherwise obtain biometric data.

In Heard v. Becton, Dickinson & Co., the U.S. District Court for the Northern District of Illinois held that Section 15(b) requires the company to take an active step to collect such data, and that "mere possession of biometric data is insufficient to trigger Section 15(b)'s requirements."[23]

Similarly, in Namuwonge v. Kronos Inc., the U.S. District Court for the Northern District of Illinois, Eastern Division, dismissed the Section 15(b) claim because the plaintiff had alleged that the employer, Brookdale, had used a system supplied by Kronos, to collect fingerprints.[24]

Such allegations did not show that Kronos collected, captured or otherwise obtained the biometric information.

More recently, in Stauffer v. Innovative Heights Fairview Heights LLC in 2020, the U.S.

District Court for the Southern District of Illinois dismissed Sky Zone Franchise Group LLC because the plaintiff failed to allege that Sky Zone used the franchise's biometric data device for its own purpose nor did it store the data on its own servers.[25]

Not Just Illinois: Other States Following Suit

In addition to Illinois, Texas[26] and Washington[27] have also enacted biometric laws, but those states do not currently allow for a private right of action.

This year, California, Kentucky, Maine, Maryland, Massachusetts, Missouri and New York have introduced similar biometric privacy legislation.

Despite BIPA's age, several states have used BIPA as a guide for their proposed laws, including the private right of action and the actual, $1,000 or $5,000 statutory damages scheme for negligent or intentional violations.

Illinois soon may lose its place as the favored territory for enterprising counsel looking for ways to sue businesses — especially in industries like cannabis where personal identifiers often are a best practice or even a business necessity.

And, given the public's concern with privacy, it is anticipated that other states may seek to enact similar legislation.

Conclusion

Combining legal uncertainty and windfall-type damages leaves a burgeoning BIPA litigation docket that relies on a statute passed in 2008 — shortly after the first iPhone became publicly available in June 2007.

BIPA has not been amended for advancements in technology, its generally accepted uses or the new realities for certain growing industries, like cannabis.

Unfortunately, BIPA issues are both real and expensive for business operating in Illinois, and are not going away any time soon. The 110 dispensaries and over 48 grow licensees in Illinois can take action to mitigate the risks and be prepared should a BIPA issue arise.

Amy Rubenstein is a partner and Sarah Trevino is a managing associate at Dentons US LLP.

[1] 740 Ill. Comp. Stat. 14/1 et seq.

[2] Id. § 14/5(c).

[3] Id. § 14/20

[4] Id. § 14/15(b).

[5] Id. § 14/15(d).

[6] Id.

[7] See https://www2.illinois.gov/sites/agr/Plants/Pages/Adult-Use-Cannabis.aspx#:~:text=There%20are%2021%20licensed%20early%20approval%20adult%20use%20cultivation%20centers.

[8] Chester v. 4Front Ventures Corp., No. 2022-L-001586 (Cook Cnty. Cir. Ct.).

[9] Rosenbach v. Six Flags Entm't Corp., 129 N.E.3d 1197, 1207 (Ill. 2019).

[10] See Namuwonge v. Kronos, Inc., 418 F. Supp. 3d 279, 286 (N.D. Ill. 2019); Figueroa v. Kronos Inc., 454 F. Supp. 3d 772 (N.D. Ill. 2020) ("Because a motion to dismiss under Rule 12(b)(6) doesn't permit piecemeal dismissals of parts of claims, that the complaint's factual allegations give rise to an inference of negligence is enough to withstand dismissal.").

[11] See Neals v. PAR Tech Corp., 419 F. Supp. 3d 1088, 1092–93 (N.D. Ill. 2019); Marsh v. CSL Plasma, Inc., 503 F. Supp. 3d 677, 685–86, No. 19 C 6700 (N.D. Ill. 2020); Rogers v. BNSF Ry. Co., 2019 WL 5635180, at *5 (N.D. Ill. Oct. 31, 2019).

[12] Rogers v. BNSF Railway Corp., No. 1:19-cv-03083 (N.D. Ill.).

[13] In re Facebook Biometric Information Privacy Litig., No. 3:15-cv-03747-JD (N.D. Ca. Feb. 26, 2021) ("It is one the largest settlements ever for a privacy violation, and it will put at least $345 into the hands of every class member interested in being compensated.").

[14] In re TikTok, Inc., Consumer Privacy Litig., No. 1:20-cv-04699 (N.D. Ill. Aug. 22, 2022).

[15] Lindabeth Rivera v. Google, LLC, No. 2019-CH-00990 (Cook Cnty. Cir. Ct.).

[16] Boone, et al. v. Snap Inc., No. 2022LA000708 (DuPage Cnty. Cir. Ct.).

[17] Brief of the Illinois Chamber of Commerce and The Chamber of Commerce of the United States, 2022 WL 1227069.

[18] Mem. 5, Robertson v. Hostmark Hosp. Grp., No. 18-CH-5194 (Cook Cnty. Cir. Ct. May 29, 2020); see also Mem. 3, Smith v. Top Die Casting Co., No. 19-L-248 (Winnebago Cir. Ct. Mar. 12, 2020) ("the interpretation plaintiff desires would likely force out of business—in droves—violators who without any nefarious intent installed new technology and began using it without complying with section (b)").

[19] Cothron v. White Castle System, Inc., 20 F4th 1156 (7th Cir. 2021).

[20] Id. at 1206.

[21] Id. at 1207.

[22] Separately, the Illinois Supreme Court is considering whether claims under BIPA are subject to a one or five-year statute of limitations. Tims v. Black Horse Carriers, No. 127801 (Ill. Sup. Ct.).

[23] Heard v. Becton, Dickinson & Co., 440 F. Supp. 3d 960 (2020).

[24] Id. at 967.

[25] Stauffer v. Innovative Heights Fairview Heights, LLC, et al., 2022 WL 3139507 (S.D. Ill. Aug. 5, 2022).

[26] https://statutes.capitol.texas.gov/Docs/BC/htm/BC.503.html.

[27] https://app.leg.wa.gov/RCW/default.aspx?cite=19.375.