Littler | Workplace Policy Institute

BIPA'S Devastating Effects on Illinois Businesses

Authors:

Kwabena Appenteng
Cyle Catlett
David Haase
Orly Henry
Jennifer Jones
Michael Lotito
Shannon Meade
Yara Mroueh

Littler

As Illinois employers and businesses recover in a post-pandemic world, the continued and growing threat of The Illinois Biometric Information Privacy Act (BIPA) looms on the horizon. This paper demonstrates that, due to the statute's vague language and several court decisions interpreting the statutory language, Illinois businesses and employers have been assaulted by a deluge of lawsuits with few if any viable defenses, and the prospect of astronomical damages awards despite the lack of harm to plaintiffs. This paper further demonstrates that the failure to understand how Illinois businesses and employers utilize biometric technology for security, identification, and convenience in the workplace has resulted in an undue hardship placed on businesses. Lastly, this paper demonstrates how the exorbitant and ballooning settlements are unsustainable and crippling to businesses in the state of Illinois.

BIPA was intended as a consumer protection law after a database of biometric data belonging to thousands of people was sold following the bankruptcy of a technology company in 2007. In response, the Illinois General Assembly sought to protect consumers from the risk of having this unalterable data from being compromised. BIPA regulates the collection and handling of biometric identifiers and information by private companies. Though the statute remained largely unutilized for several years after being enacted in 2008, the number of BIPA lawsuits have exploded since 2015. One would imagine that this would result in greater protection against the unscrupulous exposure of consumers' biometric information. Instead, BIPA, which is recognized as the country's most stringent biometric privacy law, has simply been turned against Illinois employers. With the Illinois Supreme Court inviting the General Assembly to examine its provisions on damages and the ramifications thereof in its recent *Cothron v. White Castle System, Inc.* decision, now is the time to assess whether the initial goals of BIPA are being served by the statute as it currently stands and the legal landscape that has grown around it. Simply put, the answer is no. Under BIPA, there has been great financial harm to employers in response to little to no harm to employees. The Legislature should investigate the concerns of the Illinois employer community to ensure that BIPA is more tailored to protection of consumers and deterrence rather than the cataclysmic financial upheaval to Illinois employers.

Juxtaposed with the original purpose of BIPA, this paper explains how litigation under the statute has gone awry by providing a look at the history of BIPA, the courts' statutory interpretation of the language drafted by the Legislature, and a sampling of the alarming trend of filings and settlements.

A. The Current Landscape of BIPA Claims Is at Odds with Its Purpose.

1. *The History and Purpose Behind the Use of Biometric Data*

The practice of identifying individuals by their unique identifiers is not a recent phenomenon, as fingerprints have been used for identification purposes for over 100 years.[1] Today, systems can identify individuals by recognizing characteristics such as fingerprints, face, iris, and voice.[2] A general biometric system (1) creates a reference database when it acquires and stores a biometric sample from an individual and (2) matches information when it captures a sample and compares it to previously collected samples.[3]

Today, the use of biometric data has become ubiquitous. While conventional means of identification (*e.g.*, social security numbers, state identification cards, etc.) can be lost and replaced, biometric data cannot be changed because it is based on an individual's biological characteristics. Thus, as the use of biometric data spread through businesses and employers, greater protective measures were required to ensure the safety and protection of individuals' biometric information.

2. *The Fall of Pay By Touch Leads to the Rise of BIPA*

Founded in 2002, Pay By Touch was a technology company that operated the largest fingerprint scan system in Illinois, allowing consumers to pay for goods and services with a swipe of their finger on a biometric sensor.[4] Its pilot program was used in grocery stores, gas stations, and even school cafeterias.[5] Having their financial accounts linked to their fingerprints, individuals were able to pay for items without reaching for cash or a card. Despite its innovative technology, though, the company was a financial failure. In 2007, Pay By Touch filed for bankruptcy. As part of the bankruptcy proceedings, the company sold its database containing fingerprint data of thousands of Illinois residents, without providing any information on how the data would be used.[6]

---

[1] Anna L. Metzger, *The Litigation Rollercoaster of BIPA: A Comment On the Protection of Individuals From Violations Of Biometric Information Privacy*, 50 Loy. U. Chi. L.J. 1051 (2019).
[2] Dept' of Comput. Sci. & Eng'g, Biometrics Research Grp., *What Is Biometrics?,* MICH. ST. U., https://biometrics.cse.msu.edu/info/index.html (last visited May 12, 2023).
[3] Metzger, *supra* note 1 at 1059.
[4] Charles N. Insler, *Understanding the Biometric Information Privacy Act Litigation Explosion*, 106 ILL. BAR. J. 34, 35 (2018).
[5] Erica Gunderson, *Biometric Data: Are We Safer in Illinois, or Just Having Less Fun?*, WTTW NEWS: SCI.-TECH. (Jan. 22, 2018, 5:07 PM), https://chicagotonight.wttw.com/2018/01/22/biometric-data-are-we-safer-illinois-or-just-havingless-fun (last visited on 5/09/2023)
[6] Metzger, *supra* note 1 at 1063.

3. BIPA Is Introduced

Introducing Senate Bill 2400 (which would later be known as BIPA) to the Illinois Senate in 2008, Representative Kathleen Ryg stated the following:

> This Bill is especially important because one of the companies that has been piloted in Illinois, Pay By Touch, is the largest fingerprint scan system in Illinois and they have recently filed for bankruptcy and wholly stopped providing verification services in March of 2008. This pullout leaves thousands of customers . . . wondering what will become of their biometric and financial data. The California Bankruptcy Court recently approved the sale of their Pay By Touch database. So, we are in very serious need of protections for the citizens of Illinois when it comes to biometric information.[7]

As demonstrated by the debate transcript, Representative Ryg was concerned about the sale of Pay By Touch's database, which contained biometric data belonging to Illinois citizens. The sale of biometric data potentially left individuals in a compromised position and BIPA was intended to protect against those vulnerabilities.

4. The Legislative Process Surrounding BIPA

The General Assembly passed BIPA without debate. There was no discussion or debate on what BIPA protected against, the ramifications of imposing such wide-ranging liability on Illinois employers, the drawbacks of the statute as drafted, or any of the potential consequences of enacting BIPA. No questions were asked about damage amounts or the potential impact on Illinois employers. There was no discussion about the effects of allowing a private right of action as opposed to leaving the enforcement to the Attorney General's office, as other states have. No one explained why certain groups, such as financial institutions or state actors, are exempted from BIPA.[8] Following Representative Ryg's introduction, Speaker Joseph Lyons stated the following:

> Is there any discussion? Seeing none, the question is, 'Should Senate Bill 2400 pass?' All those in favor signify by voting 'yes;' those opposed vote 'no'. The voting is open. Have all voted who wish? Have all voted who wish? Have all voted who wish? Mr. Clerk, take the record. On this Bill, there are 113 Members voting 'yes', 0 voting 'no'. This Bill, having received the Constitutional Majority, is hereby declared passed.[9]

---

[7] *See* H.R. Debate Transcript, 95th Gen. Assemb. No. 276, at 249 (Ill. 2008) (statement of Rep. Kathy Ryg).

[8] "Nothing in this Act shall be deemed to apply in any manner to a financial institution or an affiliate of a financial institution that is subject to Title V of the federal Gramm-Leach-Bliley Act of 1999 and the rules promulgated thereunder" 740 ILCS 14/25(c). "Nothing in this Act shall be construed to apply to a contractor, subcontractor, or agent of a State agency or local unit of government when working for that State agency or local unit of government." *Id.* at 14/25(e).

[9] *See* H.R. Debate Transcript, 95th Gen. Assemb. No. 276, at. at 250.

5. What Does BIPA Require?

BIPA requires an entity that possesses biometric data to develop a publicly available policy for the retention and destruction of the data.[10] Companies may obtain biometric information only if they first inform individuals—in writing—of the collection of their biometric data and receive informed written consent.[11] Additionally, BIPA regulates the disclosure of biometric data to third parties.[12] Further, companies must use a reasonable standard of care to store, transmit, and protect from disclosure the biometric information in its possession and in a manner that is at least as protective of other confidential and sensitive information.[13] And unsurprisingly, BIPA prohibits private companies from selling or profiting from individuals' biometric data.[14] Finally, BIPA allows for liquidated damages of the greater amount of $1,000 or actual damages[15] per negligent violation and $5,000 or actual damages for every intentional or reckless violation.[16] As written, BIPA does not limit the liquidated damages available to each individual.[17]

B. An Understanding of How Biometric Technology Actually Works Undermines its Current Application

As previously mentioned, the practice of identifying individuals by their biological information is not new. Fingerprints have been used for identification purposes for over a century.[18] Today, employers utilize biometric-enabled clocking systems to identify their employees, track employee time, and for security, monitoring and convenience purposes.

BIPA defines "Biometric Information" as "…any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual."[19] It further defines "Biometric Identifier" as "…a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry."

These broad definitions of "Biometric Information" and "Biometric Identifier" fail to adequately capture the proprietary and advanced technology in use and fail to distinguish between a fingerprint and finger-scan technology.[20] Fingerprinting and finger-scanning are different

[10] 740 ILL. COMP. STAT. 14/5(a).
[11] *Id*. at 14/15(b).
[12] *Id*. at 14/15(d).
[13] *Id*. at 15/15(e).
[14] *Id*. at 14/15/(c).
[15] We are unaware of any cases where actual damages have been at issue.
[16] *Id*. at 14/20.
[17] *Id.*
[18] *See Biometrics*, U.S. DEP'T HOMELAND SECURITY (Feb. 6, 2017), https://www.dhs.gov/biometrics.
[19] 740 ILCS 14/10.
[20] While this Paper primarily focuses on finger-scanning technology, other technologies pose an issue under BIPA, including facial recognition technology. For reference, facial recognition technology digitally maps out an individual's face "geometry" and creates a mathematical formula known as a "facial template" or "facial map." This stored template or signature is then used to compare the physical structure of an individual's face to confirm their identity or uniquely identify that individual. *See* David J. Oberly, *How to Avoid Becoming the Next Major BIPA Class Action Target When Using Facial Recognition for Security and Surveillance*, Biometric Update (Sept. 16, 2020),

technologies – the distinction is crucial. Fingerprinting is the "collection and hard-copy storage of the fingertip image."[21] Fingerprinting is extremely limited in use. For example, it is commonly and uniquely used by law enforcement for forensic purposes. Finger-scanning technology does not retain the fingerprint image; instead, it stores specific data about the fingertip in a smaller template.[22] It is finger-scanning technology that is used by Illinois employers. The data retained from the clocking system does not contain a fingerprint or image of any kind. Instead, it consists only of encrypted or encoded templates with numbers created from proprietary mathematical algorithms.

The use of finger-scanning technology in the workplace serves many purposes for employers, including reducing time fraud, preventing buddy-punches, assisting with monitoring remote workers, assisting with accurate payroll, and functioning as a time-saving method for Payroll and Human Resources Departments.[23] Employees also benefit as the use of this technology prevents accidental over- or underpaying of wages due to erroneous timesheets.[24] Other biometric technologies, such as Smart Drive video technology, help prevent collisions and lower risk, assist in identifying risks, improve driver performance, lower operations costs, and provide predictive analytics.[25]

1. *What "Harm" Does BIPA Protect Against?*

A scan of an individual's fingerprint is created during the enrollment process for the biometric-enabled clocking system in use.[26] This enrollment process does not actually collect and store fingerprints or anything that falls within the definitions of Biometric Identifier or Biometric Information as those terms are used in the statute.[27] The enrollment process simply generates a finger scan that is immediately converted into a numerical template using the proprietary mathematical algorithm.[28] The following illustrates the work behind finger-scanning technology:[29]

---

https://www.biometricupdate.com/202009/how-to-avoid-becoming-the-next-major-bipa-class-action-target-when-using-facial-recognition-for-security-and-surveillance (last visited on May 18, 2023).

[21] *Help Ease Employees' Privacy Concerns about Biometric Technology*, ADP® TIME AND LABOR MANAGEMENT.

[22] *Id.*

[23] Lauren Christiansen, *Biometric Scanners and Fingerprint Identification in the Workplace*, Zipclock (Sept. 18, 2020), https://zipclock.com/en/biometric-time-clock/biometric-fingerprint.html#:~:text=Employers%20utilize%20fingerprint%20recognition%20technology,and%20verifies%20identity (last visited on May 19, 2023).

[24] *Id.*

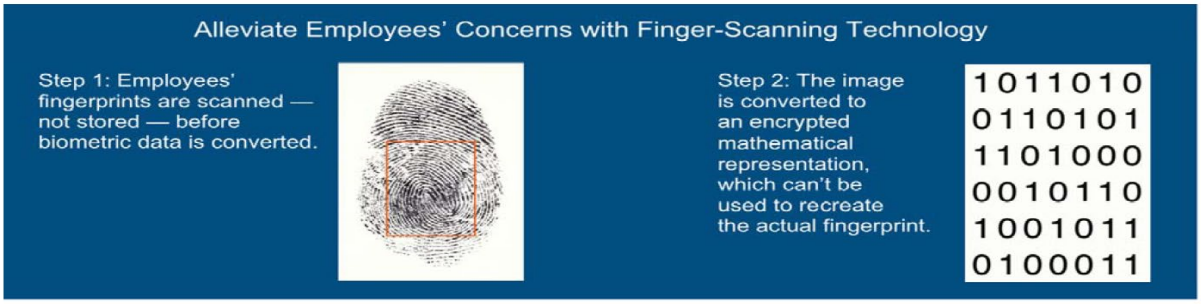
[25] SmartDrive, Solera Fleet Solutions, https://www.smartdrive.net/#:~:text=Prevent%20collisions%20and%20lower%20risk,collisions%2C%20by%20improving%20driver%20performance.

[26] *Kronos Incorporated Statement with Respect to the Illinois Biometric Information Privacy Act and Other Biometric Privacy Laws*, © 2017, Kronos Incorporated.

[27] *Id.*

[28] *Id.*

[29] *Ease Employees' Privacy Concerns about Kronos' Biometric Technology*, ©2005, Kronos Incorporated.



When that person scans in again, the results of the later scan can be compared to those of the earlier scan to determine whether there is a match.[30] This individual template is then encrypted and safeguarded from unauthorized access. The encryption safeguards against inadvertent disclosure.

As a result of the finger-scanning process and the encrypted numerical template, it is virtually *impossible* to reverse engineer an employee's original fingerprint.[31] The only biometric information utilized by employers to identify employees is an encrypted string of numbers, systemically created as a result of the mathematical algorithm. There is no biometric identifier being stored or disseminated.

No biometric information is accessible to bad actors because an employee's fingerprint is not maintained or stored by the employer nor by the provider of the biometric-enabled clocking system. Instead, in the case of an inadvertent disclosure of information, the information is limited to a nonsensical string of numbers that is unable to identify an individual outside of its intended purpose.[32]

C. Biometric Privacy Laws in Other States

There are critical differences between BIPA and how other states protect individuals' biometric data. Most other states with biometric privacy laws do not provide a private right of action. By leaving enforcement up to the Attorney General, litigation is reserved for serious violations because the focus is on protecting vulnerable information, not enormous legal fees for plaintiffs' attorneys. Further, other territories give entities an opportunity to cure the breach,[33] rather than allowing what amounts to strict liability. These differences demonstrate a focus on protecting individuals rather punishing private entities.

[30] *Id.*
[31] *Id.*
[32] *Id.*
[33] NYC Admin. Code §n. Code § 22-1203

1. Texas

In 2009, Texas passed the Capture or Use of Biometric Identifier Act (CUBI). CUBI requires informed consent before collection, sets time restrictions for retention and destruction, and prohibits companies from selling, leasing, or disclosing biometric data unless an exception applies.[34] However, only the Texas Attorney General may enforce the Act.[35] Violators of CUBI face penalties of up to $25,000 per violation.[36]

2. Washington

Washington has placed its biometric privacy act under the umbrella of its Consumer Protection Act. In Washington, an entity may not "enroll" an individual's biometric data without first obtaining informed, written consent.[37] The statute contains retention requirements. However, the statute does not provide a private right of action and is enforceable only by the attorney general.[38]

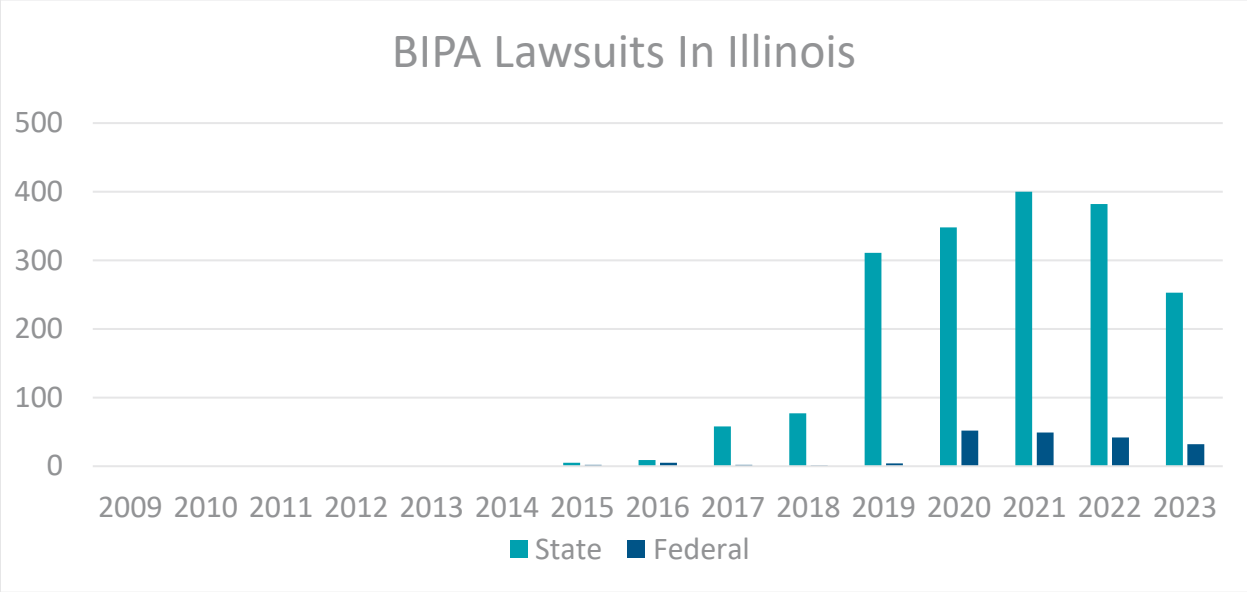
3. New York's Attempts to Pass Biometric Privacy Laws

New York state has introduced four biometric privacy bills since 2018, with all four bills failing to pass due to the devastating effects they would have on employers.[39] However, New York City passed an ordinance on July 9, 2021, which included a new regulation covering the use of biometric identifier information used by businesses within the city.[40] The law prohibits the use of biometric identifier information for transactional purposes to sell, lease, trade, or otherwise profit from the transaction of biometric information. The law affords a private right of action to "aggrieved" individuals whose data is unlawfully sold by noncompliant entities.[41] Each negligent violation can result in damages up to $500 per violation and each intentional or reckless violation can result in damages up to $5,000 per violation.[42] However, business may avoid suit by curing the violation within 30 days of the complaint and providing an express written statement that the violation has been remedied.[43]

[34] Tex. Bus. & Com. Code Ann. § 503.001(b)-(c) (West 2017).
[35] *Id*. § 503.001(d).
[36] *Id*.
[37] Wash. Rev. Code § 19.375.020(1) (2020).
[38] *Id*. § 19.375.030(2).
[39] New York State to Consider Biometric Privacy Law, Again, New York State to Consider Biometric Privacy Law, Again | Fisher Phillips – JDSupra (last visited May 18, 2023).
[40] NYC Admin. Code §n. Code § 22-1201-1205.
[41] Id. § 22-1203.
[42] *Id*.
[43] *Id*.

D. BIPA Lawsuits Explode in Illinois

As demonstrated in the graph below, BIPA litigation remained dormant for years following the statute's enactment.[44] This changed in 2015 when a few initial class actions were filed in Illinois.[45] But since the Illinois Supreme Court in 2019 held that a party alleging a "technical" violation qualifies as an aggrieved party and could bring a cause of action, a new wave of BIPA class actions have been filed with no indication of slowing down.[46]



E. Illinois Supreme Court Delivers Death Blow to Employers

BIPA has long been described as a "plaintiff-friendly" statute[47] based on its statutory language and Illinois court decisions interpreting the Act. However, a recent court decision has opened the door for possible substantial damage awards against Illinois employers that are caught in the crosshairs of BIPA litigation absent intervention by the General Assembly.

In *Cothron v. White Castle*, the Illinois Supreme Court held that BIPA violations accrue each time a private company scans a person's biometric identifier. Prior to this February 17, 2023 decision, there was a question as to whether violations of BIPA accrue each time a private company scans a person's biometric identifier, or upon on the first scan and first transmission. This case arose from a putative class action lawsuit filed by Latrina Cothron, on behalf of herself and a putative

[44] Emma Graham, *Burdened By BIPA: Balancing Consumer Protection and the Economic Concerns of Businesses*, 2022 U.Ill.L. Rev. 929.
[45] *Id*.
[46] *Id*.
[47] RoseAnn Source, *More BIPA Litigation Likely In Illinois*, The RDM Knowledge Blog (last visited May 19, 2023).

class of all Illinois employees of defendant, White Castle System, Inc.[48] Cothron worked as a manager at a White Castle restaurant and was required to scan her finger each time she accessed her pay stubs and the system's computers.[49] Cothron alleged that White Castle did not seek her consent to acquire her fingerprint biometric data until 2018, more than 10 years after BIPA took effect. Cothron asserted that White Castle violated Sections 15(b) for capturing her biometric data without providing notice and receiving consent and 15(d) for disclosing her biometric data without consent.

After the lawsuit was filed in the Circuit Court of Cook County, White Castle removed the action to federal court under the Class Action Fairness Act. After White Castle lost its motion for judgment on the pleadings at the district court level, it sought an interlocutory appeal at the Seventh Circuit. The Seventh Circuit certified the question to the Illinois Supreme Court, asking:

> Do section 15(b) and 15(d) claims accrue each time a private entity scans a person's biometric identifier and each time a private entity transmits such a scan to a third party, respectively, or only upon the first scan and first transmission?[50]

The Illinois Supreme Court disagreed with White Castle that "collection" or "capture" of biometric data occurs only once when an entity first acquires an individual's fingerprint, holding that Section 15(b) is violated the "first time an entity scans a fingerprint or otherwise collects biometric information, but it is no less true with each subsequent scan or collections."[51] Likewise, the Court found that Section 15(d) is violated in "every instance" the plaintiff's biometric information is disclosed to a third party without consent. In short, the Court held, "[w]e believe that the plain language of section 15(b) and 15(d) demonstrates that such violations occur with every scan or transmission."[52]

The Illinois Supreme Court urged the Legislature to act. Acknowledging that its decision has the possibility of astronomical damages awards, the majority stated, "we continue to believe that policy-based concerns about potentially excessive damage awards under the Act are best addressed by the legislature."[53] Further: "We respectfully suggest that the legislature review these policy concerns and make clear its intent regarding the assessment of damages under the Act."[54]

Justice David Overstreet (whose dissent was joined by Justice Mary Jane Theis and Justice Lisa Holder White) stated that, "[t]he majority's interpretation cannot be reconciled with the plain

[48] *Cothron v. White Castle Systems, Inc.*, 2023 IL 128004, ¶ 4, 2023 WL 2052410 (Feb. 17. 2023).
[49] *Id*.
[50] *Cothron v. White Castle System, Inc.*, 20 F.4th 1156, 1167 (7th Cir. 2021).
[51] *Cothron*, 2023 IL 128004 at ¶ 24.
[52] *Id*. at ¶ 30.
[53] *Id*. at ¶ 43.
[54] *Id*.

language of the statute" and "**will lead to consequences that the legislature could not have intended**." I respectfully disagree with my colleagues' answer to the certified question.[55]

The dissent further states that "the majority's construction of the Act could easily lead to annihilative liability for businesses." Explaining further:

> The majority acknowledges White Castle's estimate that, if plaintiff is successful in her claims on behalf of as many as 9500 current and former White Castle employees, ***damages in this action may exceed $17 billion***. (emphasis added) Supra ¶ 40. Nevertheless, the majority brushes this concern aside by stating that "policy-based concerns about potentially excessive damage awards under the Act are best addressed by the legislature." . . . Surely the potential imposition of crippling liability on businesses is a proper consequence to consider. . . .

In an attempt to reconcile the majority's decision with the purpose of BIPA, the dissent stated that "**[i]mposing punitive, crippling liability on businesses could not have been a goal of the Act.**"[56] Finally, the dissent crystallized the devastating effect the majority's opinion could have on Illinois employers:

> The majority's interpretation would lead to the absurd result that an entity that commits what most people would probably consider the worst type of violation of the Act—intentionally selling their biometric information to a third party with no knowledge of what the third party intended to do with it—would be subject to liquidated damages of $5000, while an employer with no ill intent that used that same person's fingerprint as an authentication method to allow access to his or her computer could be subject to damages hundreds or thousands of times that amount. This could not have been the legislature's intent.[57]

Both the majority opinion and dissent in *Cothron* recognize the need for the General Assembly to clarify its intention behind the issue of damages.

F. Who Is BIPA Actually Protecting?

The current breakdown of settlement monies between the settlement class and attorneys' fees should cause lawmakers to wonder to whom the benefits of BIPA accrue, as it is currently drafted. The General Assembly and courts have left Illinois businesses and employers defenseless against ruthless claims for unlimited liquidated damages. As a result, Illinois businesses and employers effectively have no choice but to settle BIPA claims in the tens of millions – why? Who is at the receiving end of the bulk of the settlement funds?

[55] *Id*. at ¶ 48. (emphasis added).
[56] *Id*. at ¶ 63 (emphasis added).
[57] *Id*.

The following are examples of actual, publicly available BIPA settlement awards:

- Award per class member - $251; attorneys' fee award - $5,583,333;
- Award per class member - $286; attorneys' fee award - $18,500,000;
- Award per class member - $200; attorneys' fee award - $12,000,000;
- Award per class member - $71; attorneys' fee award - $8,750,000; and
- Award per class member - $7; attorneys' fee award - $2,362,500.

The private right of action in Illinois has created perverse incentives not seen in other states where biometric privacy laws are enforced by the Attorneys General. As discussed further below, the potential for colossal damages has created a demonstrably grossly uneven playing field.

G. Astronomical Damages and the Bleak Future Ahead for Illinois Businesses and Employers

As of March 23, 2023, 140 BIPA class actions have been filed against Illinois businesses in 2023 alone. Curiously, many are filed by the same core group of law firms and attorneys.[58] Compare the number of BIPA lawsuits filed in the first three months of 2023 with the total amount filed in 2022 – approximately 300. Approximately 310 BIPA claims were filed in 2021. Illinois business are bracing for a record number of filings in 2023. Following the *White Castle* decision holding that violations accrue each time a private company scans a person's biometric identifier, settlements in 2023 are likely to continue ballooning.

Is this alarming trend sustainable?

1. *Senate Bill 3053*

In February of 2018, Senator Bill Cunningham proposed Senate Bill 3053 to amend BIPA so that:

> nothing in the Act shall be deemed to apply to a private entity collecting, storing, or transmitting biometric information if: (i) the biometric information is used exclusively for employment, human resources, fraud prevention, or security purposes; (ii) the private entity does not sell, lease, trade, or similarly profit from the biometric identifier or biometric information collected; or (iii) the private entity stores, transmits, and protects the biometric identifiers and biometric information in a manner that is the same as or more protective than the manner in which the private entity stores, transmits, and protects other confidential and sensitive information.[59]

Though Senate Bill 3053 failed on January 9, 2019,[60] the legal landscape surrounding BIPA has drastically changed. In summary, since then, Illinois courts have found that: standing under BIPA

[58] One Illinois law firm has filed approximately 32 BIPA claims and obtained $23,225,030.50 in attorneys' fees.
[59] *See Illinois Senate Bill 3053,* LegiScan, Bringing People to the Process, https://legiscan.com/IL/bill/SB3053/2017.
[60] *Id.*

does not require showing injury-in-fact,[61] BIPA is subject to a five-year statute of limitations,[62] and liquidated damages accrue on a per-scan basis.[63] As a result, Illinois businesses and employers, left without defense to these claims, have been hit with multi-million dollar claims and forced into multi-million-dollar settlements.

The future for Illinois businesses grappling with BIPA looks bleak – White Castle is potentially liable for liquidated damages in excess of $17 billion.[64]

H. Conclusion

BIPA passed without debate or fanfare, and without consideration of the potential for unintended consequences. Since BIPA's passing, plaintiffs' attorneys zeroed in on the language of the statute – "A prevailing party may recover for ***each violation***…"[65] Courts have interpreted the language of the statute to allow for exorbitant damages against Illinois businesses. As a result, Illinois has seen astronomical settlements – $650M, $100M, $50M, $36M, $25M, $16.75M,[66] and the list goes on and on.

Illinois is alone in allowing such astronomical and continuous settlements. It is time to re-visit BIPA and put a stop to this alarming trend threatening Illinois businesses' fiscal security.

[61] *Rosenbach v. Six Flags Ent. Corp.,* 2019 IL 123186, 129 N.E.3d 1197 (Jan. 25, 2019) (holding that mere collection of an individual's biometric information may be enough to state a claim under BIPA.).
[62] *Tims v. Black Horse Carriers, Inc.,* 2023 IL 127801 (Feb. 2, 2023) (holding that that all cases filed pursuant to BIPA are subject to a five-year statute of limitations period.).
[63] *Cothron*, 2023 WL 2052410 at ¶ 4 (holding BIPA violations accrue on a per-scan basis).
[64] *Id*. at ¶ 61.
[65] 740 ILCS 14/20(1)-(4)
[66] All of the listed settlement amounts are publicly available via a court docket search.