No. 128004

IN THE SUPREME COURT OF ILLINOIS

LATRINA COTHRON, *Plaintiff-Appellee*,

v.

WHITE CASTLE SYSTEM, INC., *Defendant-Appellant*.

Question of Law Certified by the United States District Court of Appeals
for the Seventh Circuit, Case No. 20-3202

Question of Law ACCEPTED on December 23, 2021 under Supreme Court Rule 20

On appeal from the United States District Court for the Northern District of Illinois under
28 U.S.C. § 1292(b), Case No. 19 CV 00382
The Honorable Judge John J. Tharp, Judge Presiding

BRIEF AND APPENDIX OF DEFENDANT-APPELLANT WHITE CASTLE SYSTEM, INC.

ORAL ARGUMENT REQUESTED

Melissa A. Siebert
William F. Northrip
Matthew C. Wolfe
SHOOK, HARDY & BACON L.L.P.
111 South Wacker Drive, Suite 4700
Chicago, Illinois 60606
Tel: (312) 704 7700
masiebert@shb.com
wnorthrip@shb.com
mwolfe@shb.com

Counsel for Defendant-Appellant
White Castle System, Inc.

E-FILED
3/3/2022 5:16 PM
CYNTHIA A. GRANT
SUPREME COURT CLERK

POINTS AND AUTHORITIES

Page(s)

NATURE OF THE ACTION

This case is before the Court on a certified question from the United States Court of Appeals for the Seventh Circuit regarding claim accrual. The certified question raises important and recurring issues under Illinois law regarding when claims accrue under the Illinois Biometric Information Privacy Act ("the Act" or "BIPA").

The Court's decision here is critical because "the issue of claim accrual under the Act is a close, recurring, and hotly disputed question of great legal and practical consequence that requires authoritative guidance from the Illinois Supreme Court." *Cothron v. White Castle Sys., Inc.*, 20 F.4th 1156, 1166 n.2 (7th Cir. 2021). As of the filing of this brief, over 1,600 class actions have been filed in Illinois state and federal courts under the Act, and claim accrual is an important issue in many of them. A claim accrual determination in this case will significantly impact timeliness, class size, and damages in hundreds of pending cases.[1] While Plaintiff is only one of thousands of such plaintiffs, her claims mirror the vast majority of her fellow litigants—like them, she is an employee whose claims are based on her repeated, consensual use of common workplace technology.[2]

---

[1] The Seventh Circuit opinion correctly notes this appeal presents a dispositive legal question under the Act, not unique to Plaintiff's claims, and which has "already shown itself to frequently arise." *Cothron,* 20 F.4th at 1166.

[2] Plaintiff's claims involve authentication processes she uses to access her confidential pay information on, and to secure managerial access to, White Castle's systems, and to confirm her compliance with company policies. Many

As always, the starting point is this Court's precedent, under which claims accrue when a legal right is invaded and an injury inflicted. *Feltmeier v. Feltmeier*, 207 Ill. 2d 263, 279 (2003). When a "single overt act" occurs from which damages may flow, the statute of limitations begins to run "on the date the defendant invaded the plaintiff's interest and inflicted injury." *Id.*

In the last three years, the Court has addressed the nature of a biometric privacy interest in multiple cases, which control the outcome of this appeal. These cases explain that the Act protects a "secrecy interest" in biometric data, by establishing a notice-and-consent procedure that provides individuals with "the power to say no" to the collection and disclosure of biometrics. *Rosenbach v. Six Flags Entm't Corp.*, 2019 IL 123186, ¶¶ 33-34; *West Bend Mut. Ins. Co. v. Krishna Schaumburg Tan, Inc.*, 2021 IL 125978, ¶¶ 45-46; *McDonald v. Symphony Bronzeville Park, LLC*, 2022 IL 126511, ¶¶ 43-44. The injury inflicted, which flows from this interest, is the "loss of control" (secrecy) in one's data, without informed consent. *Rosenbach*, 2019 IL 123186, ¶ 34. It is at this point that "biometric privacy vanishes into thin air" and the "precise harm the Illinois legislature sought to prevent is then realized." *Id.*

As explained more fully below, a loss of control, or secrecy, can only occur once. When a party is alleged to have first violated one of the Act's

---

other BIPA lawsuits involve the use of "biometric" timekeeping systems that use a combination of employee ID and finger-scans to clock in and out from work.

provisions by the "overt act" of collecting or disclosing biometric data without the required notice or consent, the "power to say no" is lost, and the secrecy of the data, and the concomitant privacy interest vested in the data, is lost. *See id.*; *see also Feltmeier*, 207 Ill. 2d at 279. Claims under Sections 15(b) and 15(d) of the Act thus accrue once. When an entity "fails to adhere to [the Act's] statutory procedures," an individual's "biometric privacy vanishes into thin air," the "precise harm" occurs, and the claim accrues. *Rosenbach*, 2019 IL 123186, ¶ 34.

Additionally, the Act's text, real-world use of biometric technology, and constitutional and public policy considerations all lead to one conclusion—BIPA claims accrue once, upon the first purported collection or disclosure of biometrics. Any contrary conclusion would have effects not intended by the Legislature, including the creation of excessive, endlessly tolled statutes of limitations, which would not serve the Act's "prophylactic" purpose. Additionally, multiple claim accrual will lead to disproportionate and even catastrophic damages flowing from a "remedial" statute that was intended to decrease reluctance to use biometric technology. 740 ILCS 14/5(e). Surely, in seeking to promote responsible use of biometrics, the General Assembly did not intend to create an untenable litigation problem for Illinois businesses.

White Castle respectfully submits that the answer to the certified question is that BIPA Section 15(b) and Section 15(d) claims accrue upon the

first unauthorized scan or collection, or the first unauthorized disclosure or transmission, of purported biometric identifiers or biometric information.

ISSUE PRESENTED FOR REVIEW

This case is before this Court on a certified question from the United States Court of Appeals for the Seventh Circuit. The statute at issue is Section 15 of the Illinois Biometric Information Privacy Act, 740 ILCS 14/15. The certified question is:

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?

STANDARD OF REVIEW

The standard of review is *de novo*. *See Yang v. City of Chicago*, 195 Ill. 2d 96, 103 (2001) (certified question involving interpretation of a statute "is a question of law" and so "review is *de novo*").

STATEMENT OF JURISDICTION

On December 23, 2021, this Court accepted the certified question from the United States Court of Appeals for the Seventh Circuit. *See* Ill. S. Ct. R. 20.

STATUTE INVOLVED

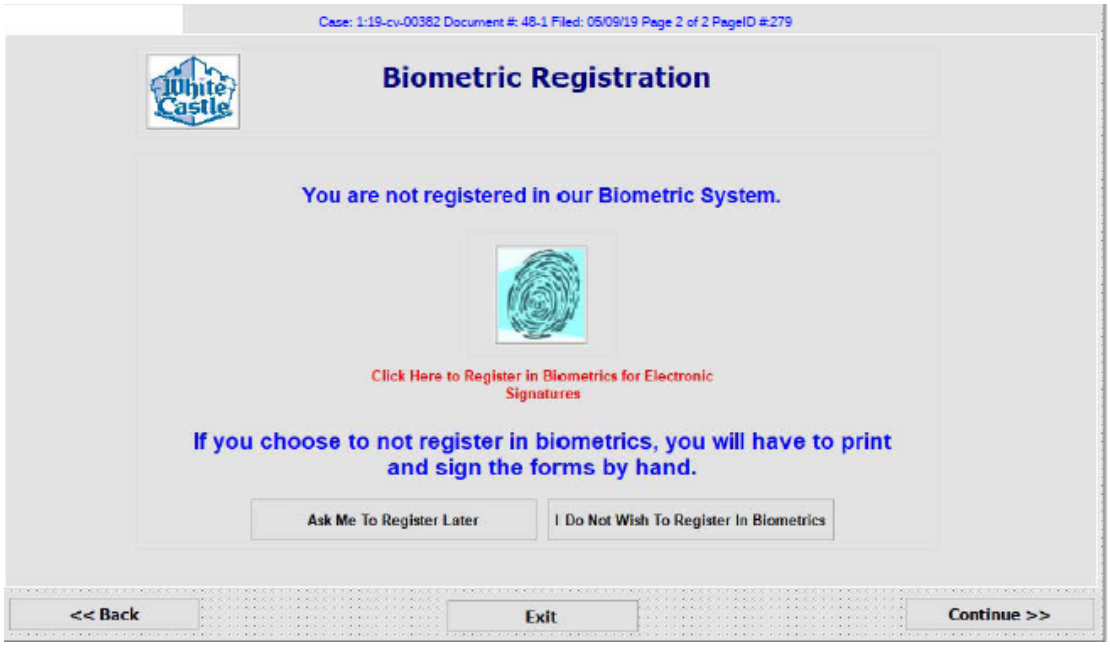
The Illinois Biometric Information Privacy Act, 740 ILCS 14/1 *et seq*. The full text of the statute is in the Appendix. (A001-04).

STATEMENT OF FACTS

I. Plaintiff consented to provide her biometrics to White Castle in 2004 and 2018.

White Castle is a family-owned restaurant group that employs thousands of Illinois residents. Over the timeframe potentially relevant to this lawsuit, over 9,500 White Castle employees have used the finger-scan timekeeping system.

Plaintiff has been a Chicago-based White Castle employee since 2004. (R118 at 23-24).[3] Within the first few months of employment, she began using White Castle's consent-based finger-scan system. (*Id.* at 24, ¶ 6). Plaintiff first consented to use the system in 2004, when White Castle presented her with the following registration screen:



[3] All "R__" citations refer to documents on the federal district court docket that are not included in White Castle's Appendix. For example, R1 refers to Docket Entry No. 1.

White Castle System Registration Screen (A005). The Registration Screen Plaintiff viewed gave her notice that if she registered in biometrics, her biometrics would be used as a form of "electronic signature." In bright red print, underneath a fingerprint image, Plaintiff was advised to "Click Here" if she wished to register her biometrics. *Id*. (A005). She was also given the option to select "I Do Not Wish To Register In Biometrics" or to select "Ask Me to Register Later." *Id.* (A005). In 2004, Plaintiff consented to use her biometrics by pressing the "Click Here" button, and voluntarily registered her biometrics in White Castle's system. (*See* R44; R118). Plaintiff has never withdrawn her voluntary consent, and to this day, continues to use her biometrics at work.

Almost fourteen years later, on October 15, 2018, Plaintiff again consented to use her finger-scan data to sign official forms and to access secure information systems, by signing a written consent form using her finger-scan electronic signature. White Castle Biometric Information Privacy Team Member Consent Form (Oct. 15, 2018) (A006). The consent form further advised Plaintiff that she could decline or even revoke a prior consent. *Id.* (A006). Plaintiff did not decline, nor has she ever revoked, her 2004 consent to use her biometrics at work. Instead, Plaintiff signed the consent form, providing her "voluntar[y] consent[] to White Castle's collection, storage, and use of biometric data and/or information through

White Castle's proprietary software," including any biometrics "as defined in the Illinois Biometric Privacy Act." *Id.* (A006).

II. Plaintiff sued White Castle fourteen years after her first consent, and several months after her second consent.

In December 2018, Plaintiff filed this putative class action contending that since 2007, White Castle had required her to use her "fingerprint" to access her work computer and weekly pay stubs, without her informed consent.[4] (R1-1, ¶¶ 2, 42-44, 56-60). According to Plaintiff, White Castle violated the Act's Sections 15(b) and 15(d) by collecting her biometric information without proper notice and consent and by "systematically" disclosing her biometrics to a technology vendor. (*Id.* ¶¶ 83-100).

White Castle then filed a motion to dismiss, challenging Plaintiff's pleading that she "never" received notice from or provided consent to White Castle to collect or disclose her biometric information. (*Id.* ¶¶ 60, 95; R37-R38). In support, White Castle attached Plaintiff's 2004 and 2018 consents. (R37-R38). Plaintiff then filed a Second Amended Complaint, contending that White Castle had not provided her with notice or obtained her consent to use her biometrics *before* collecting them. (A007-28). White Castle once again

[4] White Castle contests the allegations in Plaintiff's complaint, including that it ever collected or disclosed Plaintiff's "fingerprint," or any biometric information or identifiers as defined by BIPA. The record on appeal establishes only that White Castle uses a finger-scanning system to verify employees are properly seeking to access confidential information and systems, and can sign important documents such as IRS tax forms. (A005-06). There is no indication that White Castle transmits or discloses the information to any other entity. (A005-06).

highlighted Plaintiff's 2004 consent, in seeking to dismiss her lawsuit. (R47-R48).

III. The procedural history indicates confusion about the Act's meaning and intent.

The district court denied White Castle's motion to dismiss. (R117 at 17). Without citing any case law, the district court rejected Plaintiff's 2004 consent, because BIPA "did not exist yet," and concluded that her second, 2018 consent did not constitute consent or waiver, for her fourteen-year-long, repeated use of White Castle's finger-scan system. (*Id.* at 2, 9-10).[5]

White Castle then moved for judgment on the pleadings on the ground that Plaintiff's Section 15(b) and 15(d) claims were time barred because they accrued, if ever, in 2008, with her first scan after the Act's enactment. (R120 at 7; *see also* R118 at 26). On August 7, 2020, the district court denied White Castle's motion, holding that each use of the finger-scan system constituted two, separate violations of BIPA Section 15(b) and 15(d). *Cothron v. White Castle Sys., Inc.*, 477 F. Supp. 3d 723, 733 (N.D. Ill. 2020) (A066) ("*Cothron I*"). While focused on violations, the opinion held that a new claim, and resulting statutory damages, accrued with each purported collection of, and

[5] White Castle is unaware of any case law supporting the district court's conclusion that an entity cannot be deemed to have previously complied with a later-passed law. To the contrary, in *Miller v. Southwest Airlines Co.*, 926 F.3d 898, 904 (7th Cir. 2019), the Seventh Circuit rejected an argument that BIPA-compliant consent could not have been obtained in 2006, two years prior to BIPA's enactment, noting: "[p]erhaps in 2006 [defendant] supplied all of the information, and the union gave all of the consents, that the state later required."

every purported disclosure of, Plaintiff's biometrics. *Id.* (A066). However, the district court also encouraged White Castle to appeal, and to seek possible certification to this Court, for definitive guidance. *Id.* at 734 (A066).

On August 17, 2020, White Castle filed a timely motion to amend the district court's order to certify it for interlocutory appeal. (R134-R135). On October 1, 2020, the district court granted White Castle's motion, noting that "reasonable minds can and have differed as to the clarity of BIPA's statutory text," and that there were a "sufficient number of . . . contradictory opinions" on claim accrual under the Act to "conclude there is substantial ground for difference of opinion." (R141 at 3).

The Seventh Circuit then granted White Castle's petition for permission to appeal pursuant to 28 U.S.C. § 1292(b). (R144). After assessing BIPA's text itself, the Seventh Circuit was left puzzling over the Act's text and its impact not only on claim accrual, but on the damages resulting from such accrual. *Cothron v. White Castle Sys., Inc.*, 20 F.4th 1156, 1165 (7th Cir. 2021) (A076-77) ("*Cothron II*"). Calling BIPA claim accrual "novel," the Seventh Circuit expressed that it too was "genuinely uncertain" about the issue, and that there were "reasons to think that the Illinois Supreme Court might side with *either* Cothron or White Castle." *Id.* at 1159, 1165-66 (A076-77). As a result, the Seventh Circuit certified the question on December 20, 2021. *Id.* at 1167 (A077). Three days later, this Court accepted the certified question.

The Court's guidance is critical on two issues. First, whether its own precedent and the text of the Act provide, as White Castle submits, a clear answer of one-time claim accrual. Second, whether any other interpretation of claim accrual subverts the true intent of the Act, converting it from a prophylactic, remedial statute to an absurdly punitive one.

ARGUMENT

I. This Court's precedent establishes that Section 15(b) and 15(d) claims accrue once.

A. *Feltmeier* holds that a claim accrues when a legal right is invaded and an injury inflicted.

Throughout the present litigation, White Castle has argued that Plaintiff's claims are not timely. To evaluate a lawsuit's timeliness, courts must determine when the claim accrued. *See Brucker v. Mercola*, 227 Ill. 2d 502, 545 (2007) ("[A] statute of limitations governs the time within which lawsuits may be commenced after accrual."). A claim "accrues" when it comes "into existence as an enforceable claim or right." Black's Law Dictionary, "accrue," (11th ed. 2019).

In Illinois, a claim accrues, and the limitations period begins to run, when "facts exist that authorize one party to maintain an action against another." *Feltmeier*, 207 Ill. 2d at 278. Specifically, where there is a "single overt act" from which subsequent damages may flow, a claim accrues "on the date the defendant invaded the plaintiff's interest and inflicted injury." *Id.* at 279.

Feltmeier relied in part on *Bank of Ravenswood v. City of Chicago*, 307 Ill. App. 3d 161, 167 (1st Dist. 1999), a case that illustrates how claim accrual actually works. In *Bank of Ravenswood*, the City of Chicago constructed a subway tunnel under the bank's property ending in 1988, at which time the bank learned that it would need to construct a vibration insulation system to mitigate the subway's effects. *Id.* at 163. More than a year later, the bank filed suit claiming trespass and seeking damages for the cost of the previously-installed vibration insulation system. *Id.* at 164. Applying a one-year statute of limitations, the First District held that the plaintiffs' claim accrued no later than 1988 and, therefore, was time barred. *Id.* at 168.

Adopting the reasoning of *Bank of Ravenswood*, the *Feltmeier* opinion explained that a plaintiff's "cause of action [arises] at the time its interest is invaded." *Feltmeier*, 207 Ill. 2d at 279. Thus, in *Bank of Ravenswood*, the tunnel's construction constituted the first invasion of the bank's interest and the injury to the bank. *Id.* As such, the bank's claim accrued upon the construction of the tunnel, which was the "single overt act" that gave rise to its claim. This was so even though the subway had not even started running, and the bank had yet not incurred any of the expenses for which it sought damages. The "fact that the subway was present below ground would be a continual effect from the initial violation but not a continual violation." *Id.* (citing *Bank of Ravenswood*, 307 Ill. App. 3d at 168).

Numerous Illinois courts have applied *Feltmeier*'s "single overt act" analysis in similar situations to conclude that subsequent statutory violations do not cause new claims to accrue. *Blair v. Nev. Landing P'ship, RBG, LP*, 369 Ill. App. 3d 318, 324-25 (2d Dist. 2006), held that allegedly unauthorized republications of the plaintiff's image in multiple different advertisements did not give rise to new claims, because the first publication was a single overt act under *Feltmeier*. *See also, e.g.*, *Troya Int'l, Ltd. v. Bird-X, Inc.*, No. 15 c 9785, 2017 WL 6059804, at *14 (N.D. Ill. Dec. 7, 2017) (relying on *Blair*, claims accrued upon first publication of a video, despite that defendant uploaded the video to multiple websites and YouTube channels); *Martin v. Living Essentials, LLC*, 160 F. Supp. 3d 1042, 1046 n.4 (N.D. Ill. 2016), *aff'd*, 653 F. App'x 482 (7th Cir. 2016) (relying on *Blair* and *Feltmeier*, holding that claim was time barred because repeated airing of a television commercial constituted a single overt act and plaintiff's claim accrued at the first invasion).

Applying *Feltmeier* here, Plaintiff's injury under Section 15(b) occurred, if at all, the first time that her biometrics were collected by White Castle without her consent, not each subsequent time that her finger was re-scanned. Once the train left the station, so to speak, any further harm to Plaintiff was what *Feltmeier* deems a "continual effect" of her initial loss of control over and privacy in her biometrics. *Feltmeier*, 207 Ill. 2d at 279. The

"precise harm" the Act seeks to prevent is the initial loss of control, not its subsequent effects. *See Rosenbach*, 2019 IL 123186, ¶¶ 33-34.[6]

B. *Rosenbach*, *West Bend*, and *McDonald* define a right to secrecy in and control over biometric data and define the injury as loss of control or secrecy.

"Fundamentally, this court is always concerned with discerning legislative intent . . . . Once we have determined that intent—and unless or until the legislature indicates otherwise—the law is what we say it is." *Int'l Ass'n of Fire Fighters, Local 50 v. City of Peoria*, 2022 IL 127040, ¶ 19. The Court has addressed the Act's legislative intent on three prior occasions, providing teachings that are dispositive of, and favorable to, White Castle's interpretation of BIPA claim accrual. *See Rosenbach*, 2019 IL 123186; *West Bend*, 2021 IL 125978; *McDonald, LLC*, 2022 IL 126511.

Rosenbach provided the Court with its first opportunity to interpret the Act. There, the Court explained that BIPA "imposes numerous restrictions on how private entities collect, retain, disclose, and destroy biometric identifiers." *Rosenbach*, 2019 IL 123186, ¶ 1. Importantly, the

---

[6] *Feltmeier*'s discussion of *Belleville Toyota, Inc. v. Toyota Motor Sales, U.S.A., Inc.*, 199 Ill. 2d 325 (2002), is instructive. *Belleville Toyota* addressed "discrete decision[s]" made each month regarding automobile allocations, each of which constituted a separate violation of the Franchise Act. *Feltmeier*, 207 Ill. 2d at 280. Applying *Feltmeier*'s analysis of *Belleville Toyota*, the "discrete decision" White Castle is alleged to have made—despite Plaintiff's 2004 and 2018 pre-suit consents—is to have committed the overt acts of obtaining and disclosing Plaintiff's biometrics without *first* obtaining her consent. 740 ILCS 14/15(b). This discrete decision caused the Act's statute of limitations to begin to run, at the latest, in 2008.

purpose of these restrictions is to "prevent problems before they occur." *Id.* ¶ 37; *see also McDonald*, 2022 IL 126511, ¶¶ 43-48 (BIPA is "prophylactic").

Rosenbach concerned whether a plaintiff has statutory standing to bring a BIPA claim based solely on a violation of Section 15's terms, without alleging "[a]dditional injury or adverse effect." *Rosenbach*, 2019 IL 123186, ¶¶ 14-15. *Rosenbach* held a plaintiff is "aggrieved" under Section 20 of BIPA, and thus has statutory standing to file a lawsuit, based purely on violations of Section 15's terms. *Id.* ¶ 33.

In so holding, and key to this case, *Rosenbach* evaluated the nature of a BIPA injury, explaining that through the Act, "our General Assembly has codified that individuals possess a right to privacy in and control over their biometric identifiers and biometric information." *Id*. *Rosenbach* further explained that an injury arises under the Act "when a private entity fails to comply with one of section 15's requirements." *Id.* A violation of Section 15 "constitutes an *invasion, impairment, or denial of the statutory rights* of any person or customer whose biometric identifier or biometric information" is subject to the statutory violation. *Id*. (emphasis added); *see also McDonald*, 2022 IL 126511, ¶ 24 (quoting and reaffirming this analysis).

Rosenbach also provides important guidance about "the nature of the harm our legislature is attempting to combat" through BIPA. *Rosenbach*, 2019 IL 123186, ¶ 34. The Act "vests in individuals and customers the *right to control* their biometric information by requiring notice before collection and

giving them the *power to say no* by withholding consent . . . . *When a private entity fails to adhere to the statutory procedures . . . the right of the individual to maintain his or her biometric privacy vanishes into thin air*. The precise harm the Illinois legislature sought to prevent is then realized." *Id.* (emphasis added; cleaned up).

West Bend reiterated these points. Although, as the Seventh Circuit noted, *West Bend* involved an insurance coverage dispute, to discard it as such would be a mistake because the opinion undertakes an analysis of the nature of the interest the Act itself protects. According to *West Bend*, the Act "protects a *secrecy interest*—here, the right of an individual to keep his or her personal identifying information like fingerprints secret." *West Bend*, 2021 IL 125978, ¶ 46 (emphasis added). Discussing BIPA Section 15(d) claims, the Court explained that "disclosing a person's biometric identifiers or information without their consent or knowledge necessarily violates that person's right to privacy in biometric information." *Id.* Once biometric data is allegedly obtained by or disclosed to a third party, the individual's "right to keep certain information confidential" is violated, and the data's "secrecy" is lost. *Id.* ¶ 45.

Secrecy cannot be recreated. Once information has been shared, it is no longer secret, and any confidentiality right is lost. As the Court has explained, once lost, the right to control biometric information—that is, to

maintain its confidentiality and secrecy—"vanishes into thin air." *Rosenbach*, 2019 IL 123186, ¶ 34.

Most recently, *McDonald* reaffirmed the analysis in *Rosenbach* and *West Bend*. *McDonald* explained that BIPA injuries are not compensable under the Illinois Workers' Compensation Act because they are "personal and societal injuries caused by violating the Privacy Act's prophylactic requirements . . . [t]he Privacy Act involves prophylactic measures to prevent compromise of an individual's biometrics." *McDonald*, 2022 IL 126511, ¶ 43 (citing *Rosenbach*, 2019 IL 123186, ¶ 36). Thus, a claim under the Act "seeks redress for the lost opportunity 'to say no by withholding consent.'" *Id.* (quoting *Rosenbach*, 2019 IL 123186, ¶ 34).

Combined, *Rosenbach*, *West Bend*, and *McDonald* make clear that the legislative intent of the Act is to protect the "power to say no" to the collection of biometrics. It does so by preventing problems "before they occur." *Rosenbach*, 2019 IL 123186, ¶ 36. As such, the Act's singular intent is to safeguard the privacy of biometric data by requiring valid notice and knowing consent. A BIPA injury is, quite simply, the loss of control over and secrecy in one's biometrics without knowing consent.

C. Under the Act, the invasion and the injury are one and the same, and occurred upon Plaintiff's initial loss of control of her biometrics.

The Court's decisions establish three key legal principles regarding claim accrual, which are determinative of when BIPA claims accrue. *First*, where there is a "single overt act" from which subsequent damages may flow,

a claim accrues "on the date the defendant invaded the plaintiff's interest and inflicted injury." *Feltmeier*, 207 Ill. 2d at 279. *Second*, BIPA claims are, at bottom, claims for the loss of the "right to control" one's biometric information, and once that control (secrecy) is lost, it cannot be recreated and any confidentiality right is lost as well. *Rosenbach*, 2019 IL 123186, ¶¶ 33-34; *West Bend*, 2021 IL 125978, ¶ 46 (BIPA protects a "secrecy interest"); *McDonald*, 2022 IL 126511, ¶ 43 (BIPA injuries are "personal and societal injuries caused by violating the Privacy Act's prophylactic requirements"). *Third*, any "invasion, impairment, or denial of the statutory rights" conferred by the Act creates, in and of itself, a "real and significant" injury that is immediately actionable. *Rosenbach*, 2019 IL 123186, ¶¶ 33-34.

These three key legal principles lead to the inevitable conclusion that claims accrue on the first loss of the right to control one's biometric information. Under *Rosenbach*, the Act confers upon Illinois residents the "power to say no" to the collection and disclosure of biometrics. *Id.* ¶ 34. When a party collects or discloses biometrics without complying with the Act's notice and consent requirements, an individual's rights have been invaded, a "real and significant" injury has occurred, and the plaintiff may immediately sue. *Id*. The invasion and injury are one and the same, because once the "power to say no" is lost, it is gone forever—it "vanishes into thin air" and a lawsuit is ripe. *See id.*

West Bend re-emphasizes this point, holding that the Act protects a "secrecy interest." *West Bend*, 2021 IL 125978, ¶ 46. A person cannot keep information secret from another person who already has it. Thus, the loss of an individual's right to control their biometrics is a "single overt act" that encompasses both the invasion of the interest and the infliction of the injury. *See Feltmeier*, 207 Ill. 2d at 279.

D. Plaintiff's allegations, which are similar to those already considered by the Court, indicate that her Section 15(b) and 15(d) claims accrued once.

Given the above precedent, Plaintiff's own allegations are dispositive—her alleged injury and claim accrual occurred simultaneously, upon White Castle's first purported BIPA violation. Leaving aside for a moment Plaintiff's undisputed 2004 consent (*supra* at 5), she now contends that White Castle began requiring her to scan her finger around 2007, when she enrolled her alleged "fingerprint" in White Castle's database, and continued to do so in 2008, when the Act made it a violation to do so without informed consent. (A013-15, ¶¶ 28-30, 40). According to Plaintiff, White Castle continues to use her stored finger scan as an "authentication method" to verify her manager-level computer access, and so that she can access her own, confidential pay information. (A015-16, ¶¶ 40, 42-44). Thus, according to her own allegations, White Castle collected and possessed her biometric data upon her very first finger-scan registration, and her subsequent scans are simply providing the same finger data she already provided in order to confirm she is who she claims to be. (*See id.*).

Plaintiff's complaint further supports a simultaneous injury and claim when it describes the source of her "aggrievement" under the Act. She claims to have suffered "*an* invasion" of her privacy interest "*when* White Castle secured her personal and private biometric data at *a time* when it had no legal right to do so." (A017-18, ¶ 52) (emphasis added). Moreover, Plaintiff asserts that the Act created a right to receive "certain information" from White Castle "prior to [White Castle] securing" her biometric data and "[an] injury—not receiving this extremely critical information." (A018, ¶ 54). Plaintiff correctly posits that the "precise conduct" giving rise to her claim occurred, if at all, exactly when White Castle first secured her data. (A017-18, ¶ 52). It was then that her privacy interest, or secrecy interest, "vanished into thin air," and the harm was "realized." *Rosenbach*, 2019 IL 123186, ¶ 34.

Plaintiff's factual allegations are no different from those involved in BIPA cases already considered by the Court, where biometrics are allegedly gathered once and then subsequently used for verification. *See, e.g.*, *id.* ¶ 6 (fingerprint allegedly used to verify individual authorized to enter amusement park: "The [season pass] card and his thumbprint, when used together, enabled him to gain access as a season pass holder."); *McDonald*, 2022 IL 126511, ¶ 4 (fingerprint allegedly used for "authenticating employees and tracking their time"). This is no surprise, because biometrics is "the measurement and analysis of unique physical or behavioral characteristics (such as fingerprint or voice patterns) especially as a means of verifying

personal identity." Merriam-Webster Dictionary, "biometrics," merriam-webster.com/dictionary/biometrics (last visited Feb. 25, 2022).

As a practical matter, before one can use biometrics to verify or "authenticate" an individual, the biometric data that will be used to identify that person must be captured. Plaintiff's complaint, along with *Rosenbach*, define the moment of capture as the injury. As explained in *Rosenbach*, BIPA protects the "power to say no" to the use of biometrics to verify one's identity. *Rosenbach*, 2019 IL 123186, ¶ 34. Thus, the *Rosenbach* plaintiff should have received notice and given informed consent (through his adult guardian), before his fingerprint was stored in Six Flags' database, where it would be used going forward to confirm that he had bought a season pass. *See id.* Because plaintiff did not receive the proper notice and consent, he (or his guardian) could sue right away for his lost "power to say no." *Id.*

Alexander Rosenbach never returned to Six Flags to scan his finger after the first time he did so. *Id*. ¶ 9. Had he done so, no new injury would have occurred, because Six Flags already had his biometric data. Rosenbach would have already lost his "power to say no." Subsequent scans would have been used simply to confirm that he was who he claimed to be, and therefore was authorized to enter the park using his season pass. *Id*. ¶ 6. Because Six Flags would not have received any new information from him, no further loss of control would have occurred, and no new claim could have accrued.

The same is true here. No new injury occurred after Plaintiff's initial finger scan. Plaintiff voluntarily consented to use finger-scan technology at work in 2004. She continues to use White Castle's finger-scan technology today. BIPA became effective on October 3, 2008. 740 ILCS 14/99. Putting aside Plaintiff's first consent, there was no "loss of control" under BIPA until 2008, the first time she used the finger-scan technology in 2008 following BIPA's effective date. At that point in 2008, if ever, her BIPA rights were allegedly invaded, her injury occurred, her claim accrued, and the statute of limitations began to run.

Subsequent scans since 2008 change nothing. Once White Castle had Plaintiff's finger scan, subsequent scans simply confirmed Plaintiff was who she claimed to be, and that she was authorized for managerial-level computer access, and could access her own confidential pay information. (*See* A008, ¶¶ 2-3; A016, ¶¶ 43-44). Those subsequent scans collected no new information from Plaintiff and led to no additional loss of control of her biometrics. Her control cannot "vanish" a second time. *Rosenbach*, 2019 IL 123186, ¶ 34; *see also Fox v. Dakkota Integrated Sys., LLC*, 980 F.3d 1146, 1155 (7th Cir. 2020) ("[O]nce compromised, [biometric information is] compromised forever."). Because the invasion and injury is the loss of control, and control cannot be lost twice, there is no second invasion or injury, the same as there is no thousandth invasion or injury.

II. The Act's text confirms that Section 15(b) and 15(d) claims accrue once.

The statutory text also shows that BIPA claims accrue once, upon the first loss of control without informed consent, or the first unauthorized disclosure. Legislative intent "is best determined from the plain and ordinary meaning of the language used in the statute. When the statutory language is plain and unambiguous, we may not depart from the law's terms by reading into it exceptions, limitations, or conditions the legislature did not express, nor may we add provisions not found in the law." *Rosenbach*, 2019 IL 123186, ¶ 24.

Canons of statutory construction guide the interpretation of the Act here, and are the tools the Court uses to "grasp the intended meaning of statutory language." Black's Law Dictionary, "canon," (11th ed. 2019) (quoting Caleb Nelson, *Statutory Interpretation* 82 (2011)). "They are the principles that guide this [C]ourt's construction of statutes," and they "are utilized in every statutory construction case." *JPMorgan Chase Bank, N.A. v. Earth Foods Inc.*, 238 Ill. 2d 455, 462 (2010). In short, the Court always "necessarily look[s] to canons of statutory construction to glean [the legislature's] intent." *Int'l Ass'n of Fire Fighters*, 2022 IL 127040, ¶ 19.

A. The plain and ordinary meaning of Section 15(b)'s terms supports White Castle's position.

1. The words used in Section 15(b) establish a right to control biometrics that can only be lost once.

"The most reliable indicator of legislative intent is the language of the statute, which must be given its plain and ordinary meaning." *Haage v. Zavala*, 2021 IL 125918, ¶ 44 (citations omitted). Here, Section 15(b) provides that no private entity "may collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifier or biometric information, *unless it first*" provides notice and receives consent as outlined in the rest of Section 15(b). 740 ILCS 14/15(b) (emphasis added). The question for the Court, then, is what these undefined terms mean. To answer these questions, it is appropriate to begin by considering the plain and ordinary meaning of the words used in the statute, and, in doing so, to consult a dictionary. *See People v. Chapman*, 2012 IL 111896, ¶ 24 ("When a statute contains a term that is not specifically defined, it is entirely appropriate to look to the dictionary to ascertain the plain and ordinary meaning of the term."); *see also, e.g.*, *Rosenbach*, 2019 IL 123186, ¶ 32 (relying on Merriam-Webster's Collegiate Dictionary when interpreting BIPA's plain language).

"First" means "preceding all others in time, order or importance." Merriam-Webster Dictionary, "first," merriam-webster.com/dictionary/first (last visited Feb. 25, 2022). Section 15(b)'s language "*unless it first*" therefore refers to a singular point in time; notice and consent must precede, or occur

before, collection. *See, e.g.*, *Miller*, 926 F.3d at 900 ("*Before* obtaining any fingerprint, a 'private entity' must inform the subject . . . in writing about several things." (emphasis added)).

The active verbs used in Section 15(b) all have a similar plain and ordinary meaning as set forth in dictionary definitions, all of which involve *gaining control* of biometrics:

- "Collect" means "to bring together into one body or place" or "to gain or regain control of."
- "Capture" means "to gain control of" or "to record in a permanent file."
- "Purchase" means "to obtain by paying money."
- "Receive" means "to come into possession of."
- "Obtain" means "to gain or attain."

Merriam-Webster Dictionary, "collect," "capture," "purchase," "receive," and "obtain," www.merriam-webster.com (last visited Feb. 25, 2022). These verbs should be given their plain and ordinary meaning—they all mean to gain control, an action that only happens once.

Likewise, to the extent there is even a trace of ambiguity in any of the verbs used in Section 15(b), numerous canons of statutory construction show that this series of verbs must be read together in harmony. To begin, this Court has made clear that, "[w]hen construing a series of terms . . . [statutory interpretation is] guided by the commonsense principle 'that words grouped

in a list should be given related meaning.'" *Corbett v. County of Lake*, 2017 IL 121536, ¶ 31 (quoting *Third Nat'l Bank in Nashville v. Impac Ltd.*, 432 U.S. 312, 322 (1977)). This "commonsense principle" is "related to the canon of statutory construction known as *noscitur a sociis*, *i.e.*, 'a word is known by the company it keeps.'" *Corbett*, 2017 IL 121536, ¶ 31 (quoting *People v. Gaytan*, 2015 IL 116223, ¶ 30). Specifically, under *noscitur a sociis*, "[i]t is a general rule that words grouped in a list should be given related meaning." *Dynak v. Bd. of Educ. of Wood Dale Sch. Dist.*, 2020 IL 125062, ¶ 22 (citing *Corbett*, 2017 IL 121536, ¶ 31). Accordingly, each verb in Section 15(b) should be "given more precise content by the neighboring words with which it is associated." *Corbett*, 2017 IL 121536, ¶ 31 (quoting *United States v. Williams*, 553 U.S. 285, 294 (2008)). The canon of *noscitur a sociis* is important here because it ensures that a word is not ascribed "a meaning so broad that it is inconsistent with its accompanying words, thus giving 'unintended breadth to legislative acts.'" *Corbett*, 2017 IL 121536, ¶ 32 (quoting *Gustafson v. Alloyd Co.*, 513 U.S. 561, 575 (1995)) (brackets omitted).

When properly viewed in light of the series of verbs used, each verb used in Section 15(b) involves the moment at which an entity gains control of biometrics. This makes perfect sense in light of the purpose for which BIPA was enacted: to protect individuals' "control over" their biometrics. *Rosenbach*, 2019 IL 123186, ¶ 33. One loses control the moment another

gains it. That is the only moment that matters for accrual under Section 15(b).

The canon of *noscitur a sociis* is essential to interpreting Section 15(b)'s catchall phrase: "*or otherwise obtain*." 740 ILCS 14/15(b) (emphasis added). To "otherwise obtain" must read just like the verbs that precede it, which is to say actions that imply *gaining control*. This is clear not only under the doctrine of *noscitur a sociis*, but also under the doctrine of *ejusdem generis*, which this Court has described as "a cardinal rule of statutory and contract construction." *West Bend*, 2021 IL 125978, ¶ 57 (citing *Pooh-Bah Enters. v. County of Cook*, 232 Ill. 2d 463, 492 (2009)).

As the Court explained in *West Bend*, the *ejusdem generis* rule is that "where general words follow an enumeration of persons or things, by words of a particular and specific meaning, such general words are to be held as applying only to persons or things of the same general kind or class as those specifically mentioned." *Id.* (quoting Black's Law Dictionary 517 (6th ed. 1990)) (ellipses omitted). Said differently, under this doctrine, a statute's use of "other" or "otherwise" should be read as "other such like." *People v. Davis*, 199 Ill. 2d 130, 138 (2002); *see also Univ. of Chicago v. Dep't of Rev.*, 2020 IL App (1st) 191195, ¶ 52 (applying *ejusdem generis* doctrine to interpret plain meaning of phrase beginning with "otherwise").

Applying the doctrine here, the use of the phrase "otherwise obtain" in Section 15(b) was intended to refer only to actions to obtain biometrics "such

like" the series of verbs that precede the phrase. Put simply, "otherwise obtain" means to otherwise gain control.

All of the above "gains of control" happen at the point of collection, because the information is then stored and used for future identification of the individual. *See* Section I.D. Thus, at the point of collection, the "secrecy interest" held by the plaintiff in her biometrics "vanishes into thin air," the injury occurs, and the claim accrues.

2. Courts finding claim accrual on first collection correctly apply Section 15(b)'s plain language and common sense principles.

On facts materially identical to the ones here, three trial courts reached the same conclusion White Castle proposes, determining BIPA claims accrue once under Section 15(b) by interpreting the Act's plain language in light of common-sense principles. Those courts reasoned that the plain language of the statute implicates control, so the injury occurs upon the first collection or disclosure, when control is lost. Subsequent collection or disclosure of the same information does not create any new injury, because the collector of biometrics already has the information. In *Smith v. Top Die Casting Co.*, No. 2019-L-248, slip op. at 3 (Cir. Ct. Winnebago Cty. Mar. 12, 2020) (A037), the Circuit Court of Winnebago County hit the nail on the head:

> The biometric information is collected the one time, at the beginning of the plaintiff's employment, and thereafter the original print, or coordinates from the print, are used to verify the identity of the individual clocking in. Thus, the offending act is the initial collection of the print and at that time the

> cause of action accrues. To hold otherwise is contrary to the plain wording of the statute and common sense as to the manner the initially collected biometric information is utilized.

Similarly, a Circuit Court of Cook County judge explained that "all [of plaintiff's] damages flowed from that initial act of collecting and storing Plaintiff's handprint in Defendants' computer system without first complying with the statute. Plaintiff's handprint was scanned and stored in Defendants' system on Day 1, allowing for authentication every time he signed in." *Watson v. Legacy Healthcare Fin. Servs., LLC*, No. 19-CH-3425, slip op. at 3 (Cir. Ct. Cook Cty. Jun. 10, 2020) (A052), *rev'd*, 2021 IL App (1st) 210279. Accordingly, the plaintiff's Section 15(b) "cause of action accrued when his handprint allegedly was collected in violation of BIPA on his first day of work." *Id.* (A052).

In *Robertson v. Hostmark Hospitality Group, Inc.*, No. 18-CH-5194, slip op. at 5 (Cir. Ct. Cook Cty. Jan. 27, 2020) (A033) ("*Robertson I*"), another Circuit Court of Cook County judge explained that under the plain language of Section 15(b), a collector or possessor of biometrics may comply with BIPA by obtaining consent at the first collection or disclosure. The failure to do so, at the first collection, gives rise to an actionable BIPA violation. Thus, the interest is invaded and the actionable injury happens in a "single overt act" occurring upon the first violation. *Id.* (A033); *see also Robertson v. Hostmark Hospitality Group, Inc.*, No. 18-CH-5194, slip op. at 4-7 (Cir. Ct. Cook Cty. May 29, 2020) (A043-46) ("*Robertson II*") (denying motion for reconsideration).

3. Courts that reached the opposite conclusion ignored *Rosenbach*'s textual analysis of the Act.

Unfortunately, other courts have gotten it wrong by failing to follow basic statutory construction principles when determining claim accrual. On appeal in *Watson*, the First District's opinion failed to interpret the Act's plain language consistent with its legislative intent, as set forth in *Rosenbach*, which instructs that an injury occurs under the Act when the "power to say no" is lost. The First District in *Watson* ignored *Rosenbach*'s key statement of legislative intent, instead focusing on *Rosenbach*'s low pleading bar. *See Watson*, 2021 IL App (1st) 210279, ¶ 69. While it is true that a BIPA claim may be pled based on a plain violation of the statute's terms, without any additional injury to the plaintiff, there is no text in BIPA supporting the conclusion that each subsequent data verification gives rise to a new violation and claim. Rather, a new BIPA claim arises only when a new BIPA injury occurs—that is, a new loss of control, like biometrics coming into the possession of a new third party.

This leads to the second key error of the First District in *Watson*. The First District misapprehended how biometrics work. As the circuit court in *Watson* had recognized, subsequent scans serve merely to verify identity using the same information already in the biometrics collector's control. *See* Section I.D. The First District never so much as mentioned this fact, which was central to the circuit court's analysis, and which is true in every BIPA case. Instead, the First District assumed without support that every scan of a

finger works a new loss of control. *See Watson*, 2021 IL App (1st) 210279, ¶¶ 58-60.

The district court in this case, also purporting to apply a textual analysis, made the same errors as the First District in *Watson*. The district court also did not address *Rosenbach*'s holding that BIPA protects the "power to say no." Instead, the district court formalistically concluded that because "[e]ach time an employee scans her fingerprint to access the system, the system must capture her biometric information and compare that newly captured information to the original scan," and each new "capture" must be a new violation. *Cothron I*, 477 F. Supp. 3d at 732 (A065). That analysis misses the point of *Rosenbach*. A BIPA injury is the loss of control. From the correct starting point, it follows that subsequent scans of the same information change nothing, because control already has been lost.

B. The statutory text of Section 15(d) supports White Castle's position.

1. The plain language of Section 15(d) shows that a claim accrues once upon initial disclosure.

Section 15(d) states that no private entity "in possession of a biometric identifier or biometric information may disclose, redisclose, or otherwise disseminate a person's or a customer's biometric identifier or biometric information unless" the private entity has obtained consent, or certain exceptions apply. 740 ILCS 14/15(d).

Like Section 15(b), Section 15(d) requires consent. As the Court put it in *West Bend*, Section 15(d) protects a "secrecy interest . . . the right of an

individual to keep his or her personal identifying information like fingerprints secret," and an individual may thus decline to consent to their disclosure. *West Bend*, 2021 IL 125978, ¶ 46. The plain language of Section 15(d) makes clear that the relevant injury is the loss of control of one's biometric information.

Section 15(d) requires consent in order for a private entity to "disclose, redisclose, or otherwise disseminate" an individual's biometrics. Each of those verbs implicates the disclosure of biometrics by one party to a new, third party—said differently, a party that has not previously possessed the relevant biometric identifier or biometric information.

Just as in Section 15(b), in Section 15(d) the plain and ordinary meaning of the verbs controls:

- "Disclose" means "to make known or public." Merriam-Webster Dictionary, "disclose," merriam-webster.com/dictionary/disclose (last visited Feb. 25, 2022); *see also* Black's Law Dictionary (11th ed. 2019) ("disclose" means to "make (something) known or public; to show (something) after a period of inaccessibility or of being unknown; to reveal").
- "Redisclose" means to "disclose what has been disclosed to the discloser." WordSense Dictionary, "redisclose," wordsense.eu/redisclose (last visited Feb. 25, 2022).[7] In case

[7] "Redisclose" does not appear in the Merriam-Webster Dictionary.

there is any doubt, this is the meaning given "redisclose" in other Illinois statutes. *Cothron II*, 20 F.4th at 1164 n.1 (A078) (collecting statutes). In other words, the term redisclose is meant to ensure that downstream entities are subject to Section 15(d).

- "Disseminate" means "to spread abroad" or "to disperse throughout." Merriam-Webster Dictionary, "disseminate," merriam-webster.com/dictionary/disseminate (last visited Feb. 25, 2022).

Based on the plain meaning of the above words, Section 15(d) bars the disclosure of biometrics, without consent, to a new party that did not previously have them.

Plaintiff argued in the federal courts that "redisclose" is ambiguous and should be read to mean "disclose to the same party again." Plaintiff is wrong for several reasons.

First, the prefix "re" means "again" or "anew." Merriam-Webster Dictionary, "re," merriam-webster.com/dictionary/re (last visited Feb. 25, 2022). "Disclose" means "to make known or public." Merriam-Webster Dictionary, "disclose," merriam-webster.com/dictionary/disclose (last visited Feb. 25, 2022); *see also Cothron II*, 20 F.4th at 1163 (A075) ("The ordinary meaning of 'disclose' connotes a new revelation."). Putting "re" and "disclose" together, then, the plain meaning of "redisclose" is to newly make known,

which necessarily implicates a new entity. Indeed, as the Seventh Circuit observed, "repeated transmissions of the same biometric identifier to the same third party are not new revelations." *Id.* (A076).

Second, the "commonsense principle 'that words grouped in a list should be given related meaning'" applies again here. *Corbett*, 2017 IL 121536, ¶ 31. Specifically, each verb used in Section 15(d) must be read in harmony with the other verbs that surround it under the doctrine of *noscitur a sociis*. Because both other verbs (*i.e.*, disclosure and disseminate) contemplate a new revelation from one entity to another, not repeated publications of the same information between the same entities, "redisclose" must be read in the same manner. *See, e.g.*, *id.* It would be antithetical to this Court's precedent (and plain English) to read "redisclose" to meaning anything substantially different than to "disclose" or to "disseminate."

Third, all of the above is consistent with *Rosenbach*, *West Bend*, and *McDonald* that the Act confers a right to a "secrecy interest" and the "power to say no," and that an injury arises from the "loss of control." *See* Section I.A-B. A person or entity only can lose control of information to *someone else*. Because Section 15(d) requires the presence of a third party, it makes sense for Section 15(d) to speak to that potential third party's conduct—redisclosure to another. Under this reading, "redisclose" would mean that the first third party to receive the biometrics may not subsequently disclose the biometrics to another without consent.

2. Repeated disclosures of biometrics to the same third party are not a new injury, because they do not result in a new loss of control.

In this case, the district court struggled with the presence of the term "redisclosure," ultimately ruling that "redisclose" meant repeated disclosures to the same party. *Cothron I*, 477 F. Supp. 3d at 733 (A066); *but see Cothron II*, 20 F.4th at 1163 (A076) ("Repeated transmissions of the same biometric identifier to the same third party are not new revelations."). That is not what "redisclose" means in the context of biometrics or under the Act, especially when looking to the Act as a whole.

Plaintiff alleges that White Castle repeatedly disclosed the same biometric information to the same entities (White Castle's technology vendors). (A014, ¶ 31; A026, ¶ 96). The alleged subsequent disclosures did nothing to change the position between White Castle, the technology vendors, and Plaintiff regarding control of her finger-scan data. Accordingly, subsequent disclosures do not cause additional invasion and do not create additional injury. *See Fox*, 980 F.3d at 1155 ("[O]nce compromised, [biometric information is] compromised forever.").

Looking to BIPA as a whole, which this Court must do,[8] BIPA itself actually anticipates that a party or parties might repeatedly use the

[8] In construing the statute, the Court must view it "as a whole, construing words and phrases in light of other relevant statutory provisions and not in isolation." *Evans v. Cook County State's Atty.*, 2021 IL 125513, ¶ 27. Thus, it is appropriate to look to Section 15(a) to help interpret the nature of the interest protected by Section 15(d).

biometric data after the initial collection. Section 15(a) provides that biometric information must be permanently destroyed when the *initial* purpose for collecting or obtaining the information has been satisfied or within three years of the individual's *last* interaction with the entity. *See* 740 ILCS 14/15(a). Thus, the plain language of Section 15(a) envisions ongoing interaction with the entity collecting and disclosing the information.

Section 15(a) thus reflects the reality of the Act's regulatory scheme. Once collection or disclosure has occurred for an initial purpose, continued collection or disclosure of that same information for the same purpose is allowed. The only requirements are consent and a biometrics policy. If repeated disclosure of the same information to the same third party were a problem, Section 15(a) would require destruction after every interaction, not just at the end of the relationship. Against this background, it follows that "redisclosure" as used in Section 15(d) means disclosure to a new third party.

3. Illinois courts consistently hold that repeated disclosure of the same private information is not a new injury.

Moreover, under established Illinois law, redisclosure of private information to an entity that already has it is not a new invasion or a new injury for accrual purposes. Addressing allegations materially identical to the ones here, the circuit court in *Robertson* got this issue exactly right, ruling that failure to obtain consent before disclosure was a "single overt act" and the plaintiff's Section 15(d) claim accrued upon the initial failure to obtain consent. *Robertson I*, slip op. at 6 (A034). In that case, just like this one, the

plaintiff alleged that the defendant "systematically and automatically" disclosed his biometrics. *Robertson II*, slip op. at 6-7 (A045-46).

The *Robertson* court twice held that repeated disclosure to the same third party was not a new invasion or injury. *Robertson I*, slip op. at 6 (A034); *Robertson II*, slip op. at 7 (A046). On a motion for reconsideration, plaintiff argued that the defendant could violate Section 15(d) "multiple times by disseminating his biometric data to multiple third parties on many occasions." *Id.* (A046). The court acknowledged that this could be the case, but held that generalized allegations of "systematic and automatic" disclosure did not adequately plead separate, additional violations of Section 15(d). *Id.* (A046). As the *Robertson* court astutely realized, repeated disclosures of the *same* information to the *same* third party do not create any new injury.

Indeed, Illinois courts have long recognized that privacy claims involving disclosure or publication accrue upon the first disclosure, because subsequent invasions of the same privacy interest (*i.e.*, disclosure or publication of the same information for the same purpose) do not give rise to new claims. Illinois was the first state to adopt this rule. *See Winrod v. Time, Inc.*, 334 Ill. App. 59, 72 (1st Dist. 1948) (libel claim accrued upon first publication of magazine and subsequent distributions did "not constitute a new publication or create a new cause of action"). Today, it is so fundamental that the Illinois legislature has codified it as the Uniform Single Publication

Act. *See* 740 ILCS 165/1 ("No person shall have more than one cause of action for . . . invasion of privacy . . . founded upon any single publication.").

In privacy claims involving publication, where a protected interest is invaded through disclosure or publication, such as under Section 15(d), subsequent disclosure or publication of the same information does not create a new injury and does not give rise to new claims. *See, e.g.*, *Blair*, 369 Ill. App. 3d at 324-25 (in right-of-publicity case, republication of same image in numerous advertisements did not give rise to new claims); *see also Winrod*, 334 Ill. App. at 72; *Troya Int'l, Ltd.*, 2017 WL 6059804, at *14 (claims accrued upon first publication of a video, despite that defendant uploaded the video to multiple websites and YouTube channels); *Martin*, 160 F. Supp. 3d at 1046 n.4 (noting repeated airing of a television commercial constituted a single overt act and plaintiff's claim accrued at the first invasion).

Just last year, the Court again emphasized the importance of the single publication rule. In *Ciolino v. Simon*, 2021 IL 126024, ¶ 43, the Court observed that "the single-publication rule would not serve its purpose if it were applied to encompass the subsequent screenings [of the same defamatory film to the same target audiences] in Cleveland and Chicago." *Ciolino* explained that showing the same material repeatedly to the same target audience could not give rise to separate claims for liability, because it would create the situation the single-publication rule is explicitly designed to prevent—namely, "ungovernable piecemeal liability and [a] potentially

endless tolling of the statute of limitations." *Id.* (citations omitted and alteration in original).

Indeed, this case squarely presents the endlessly tolled statute of limitations the Court cautioned against. Plaintiff began using White Castle's finger-scan system in 2004, and has ever since. BIPA was enacted in 2008. Plaintiff filed suit in December 2018, shortly after she provided her written consent to White Castle in October 2018. The district court has essentially ruled that each scan causes a new claim to accrue, and the statute of limitations begins to run anew. Applying this reasoning to Plaintiff's final, pre-consent scan in October 2018, she can delay until October 2023 to bring a BIPA lawsuit, despite the fact that she has been scanning her finger for nineteen years (since 2004), and that fifteen years will have passed since BIPA's enactment. Surely an almost twenty-year limitations period (or even a fifteen-year limitations period) does nothing to serve BIPA's intended purpose of "imposing safeguards to insure that individuals' and customers' privacy rights in the their [biometrics] are properly honored and protected to begin with, before they are or can be compromised." *Rosenbach*, 2019 IL 123186, ¶ 36.

To prevent problems before they occur, the General Assembly instituted a notice-and-consent regime meant to provide biometric users with the "power to say no" to collection and disclosure. *See id.* ¶ 34. A BIPA injury occurs when the power to say no is denied, resulting in the loss of the "secrecy

interest" the Act protects. *See West Bend*, 2021 IL 125978, ¶ 46. Upon the first time biometrics are disclosed without consent, the "power to say no" is gone, the injury occurs, and the single BIPA claim accrues absent a re-disclosure or other broad dissemination of the same biometric data to additional parties.

III. BIPA should be construed in a manner that affirms its legislative purpose and avoids significant constitutional, public policy, and practical problems.

A. Interpreting BIPA claims as accruing once affirms the statute's constitutionality and legislative purpose.

Courts have a "duty to construe a statute so as to affirm the statute's . . . validity, if reasonably possible." *People v. Shephard*, 152 Ill. 2d 489, 499 (1992); *see also People v. Austin*, 2019 IL 123910, ¶ 14. To ensure validity, courts assess the rationality of the relationship between their interpretation of the statute, and the legislature's purpose and intent. *See People v. Zaibak*, 2014 IL App (1st) 123332, ¶ 33 (courts must remember to "ascertain and give effect to the legislature's intent in enacting the statute") (citing *People v. Bailey*, 167 Ill. 2d 210, 225 (1995)). The rationality analysis "examine[s] the problems that the legislature intended to remedy with the law and the consequences of construing it one way or the other." *Watson*, 2021 IL App (1st) 210279, ¶ 38. The goal is to adopt a statutory interpretation that is reasonably related to the statute's fundamental purpose. *See id*.

Here, the Act contains express legislative findings stating its intent. *See* 740 ILCS 14/5(a)-(g). Those findings explain that the "growing" use of

biometrics shows "promise," but that the use of biometrics also presents unique risks. Accordingly, given those risks, skepticism among the public, and the fact that the "full ramifications of biometric technology are not fully known," the "public welfare, security, and safety will be served by regulating the collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and information." *Id.*

To achieve those goals, the Act, among other things, requires informed consent for collection and disclosure; prohibits the sale of biometrics; and requires collectors and possessors of biometrics to adopt and comply with retention and destruction policies. As this Court has noted, BIPA is a *remedial* statute that implements *prophylactic* measures to prevent the compromise of biometrics by allowing individuals to choose to provide (or not to provide) their data after being advised that it is being collected, stored, and potentially disclosed. *See McDonald*, 2022 IL 126511, ¶ 43; *Rosenbach*, 2019 IL 123186, ¶ 36 (discussing General Assembly's goal, through BIPA, of preventing problems "before they occur").[9] Remedial statutes "are designed to grant remedies for the protection of rights, introduce regulation conducive to the public good, or cure public evils." *Standard Mut. Ins. Co. v. Lay*, 2013 IL

[9] Courts consistently have recognized BIPA's remedial nature. *See, e.g.*, *Burlinski v. Top Golf USA Inc.*, No 19-cv-06700, 2020 WL 5253150, at *7 (N.D. Ill. Sept. 3, 2020) (BIPA has a remedial purpose to protect biometric privacy); *Meegan v. NFI Indus., Inc.*, No. 20 C 465, 2020 WL 3000281, at *4 (N.D. Ill. June 4, 2020) ("BIPA's provision for actual damages and the regulatory intent of its enactment show that it is a remedial statute[.]").

114617, ¶ 31. Remedial statutes are distinct from penal statutes, which operate as "punishment for the nonperformance of an act or for the performance of an unlawful act" and "require[] the transgressor to pay a penalty without regard to proof of any actual monetary injury sustained." *Goldfine v. Barack, Ferrazzano, Kirschbaum & Perlman*, 2014 IL 116362, ¶ 28 (citations omitted).

As a remedial statute, BIPA's liquidated damages provision is simply "one part of the regulatory scheme, intended as a supplemental aid to enforcement rather than as a punitive measure." *Scott v. Ass'n for Childbirth at Home, Int'l*, 88 Ill. 2d 279, 288 (1981). In fact, damages under BIPA are the "greater" of actual damages or liquidated damages, which is indicative of the fact that liquidated damages are intended to be awarded only where actual damages are too small and difficult to prove, not as a multiplier by thousands for each time technology is used. 740 ILCS 14/20.

In *Smith*, also cited earlier in this brief, the court reached the same conclusion. In response to the plaintiff's per-scan accrual argument, the court found that "as a matter of public policy, 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) and had its employees clocking in at the start of the shift, out for lunch, in for the afternoon and out for the end of the shift." *Smith*, slip op. at 3 (A037). According to the court's calculation, "[o]ver a

period of 50 weeks (assuming a two week vacation) at $1,000 for each violation it adds up to $1,000,000 *per employee* in a year's time." *Id*. (A037). As the court recognized, these astronomical damages "would appear to be contrary" to the legislative intent expressed in the preamble to the statute. *Id*. (A037).

Further, *Smith* is consistent with long-standing Illinois law that liquidated damages are understood to refer to a *reasonable* estimate of harm—one that "bear[s] some relation to the damages that might occur." *Smart Oil, LLC v. DW Mazel, LLC*, 970 F.3d 856, 863 (7th Cir. 2020). When a liquidated sum is "far in excess of the probable damage on breach, it is almost certainly a penalty." Black's Law Dictionary, "damages" (11th ed. 2019). The Illinois legislature authorized "liquidated damages"—not "penalties"—and the Act should be interpreted in accordance with the meaning of that statutory term.

Claim accrual under the Act thus must be tied to the *preventative* privacy protections provided by the statute and not motivated by punitive means. Accrual upon the initial collection or disclosure of biometrics supports the prophylactic legislative purpose this Court and other Illinois courts have consistently recognized. Any interpretation to the contrary, like that advocated by Plaintiff, is untethered from the legislative purpose of BIPA.

B. A single-accrual rule also avoids constitutional problems.

The canon of constitutional avoidance requires the Court to construe a statute in a way that "promote[s] its essential purposes and [avoids], if

possible, a construction that would raise doubt as to its validity." *People v. Glenn*, 2018 IL App (1st) 161331, ¶ 22 (citing *People v. Nastasio*, 19 Ill. 2d 524, 529 (1960)); *see also Maddux v. Blagojevich*, 233 Ill. 2d 508, 516 (2009) ("[T]he General Assembly cannot acquiesce to a construction that is at odds with the constitution."). This Court routinely applies the constitutional avoidance canon when interpreting statutory terms. *People v. Hernandez,* 2016 IL 118672, ¶ 10 (recognizing and applying canon of constitutional avoidance to statute); *Maddux,* 233 Ill. 2d at 516 (concluding that "the General Assembly cannot acquiesce to a construction that is at odds with the constitution"); *Nastasio,* 19 Ill. 2d at 529 (noting the duty of the courts to "interpret [a] statute as to . . . avoid, if possible, a construction that would raise doubts as to its validity").

As a remedial statute intended to prevent injury, BIPA is not punitive and its purpose is not to punish private entities with unreasonably high multiples of damages. Moreover, the Due Process Clause of the Fourteenth Amendment to the U.S. Constitution imposes constitutional limitations, in the context of punitive damages, which must be reduced if they are "so severe and oppressive as to be wholly disproportioned to the offense or obviously unreasonable." *St. Louis, I. M. & S. Ry. Co. v. Williams*, 251 U.S. 63, 67

(1919); *accord State Farm Mut. Auto. Ins. Co. v. Campbell*, 538 U.S. 408, 416-17 (2003).[10]

In this case, if BIPA claims and damages accrue with each scan of a finger and each transmission to the same technology vendors, the results would vastly exceed acceptable ratios between the damages awarded and the offense at issue. Plaintiff alleges she had to scan her finger each time she accessed a work computer and each time she accessed her weekly pay stub. (A008, ¶ 2; A015-16, ¶¶ 40, 43-44). Assuming Plaintiff worked 5 days per week for 50 weeks per year and accessed the computer each day and her pay stub weekly, her total scans would exceed 1,500 over a five-year limitations period, and the total number of disclosures would exceed 300 over a one-year limitations period.[11] If Plaintiff were to succeed in proving her claims at trial, that could result in damages between $1.8 million and $9 million for Plaintiff alone despite the fact that Plaintiff has not alleged a data breach or any costs associate with identity theft or compromised data.

The excessive nature of Plaintiff's potential damages is exacerbated in the class-action context. Here, Plaintiff seeks to represent as many as 9,500 current and former White Castle employees. Multiplying $1.8 million by

---

[10] The Illinois Constitution provides similar protections. *See* Ill. Const., art. I, § 2.

[11] On January 26, 2022, this Court accepted an appeal relating to the statute of limitations applicable to BIPA claims. *Tims v. Black Horse Carriers, Inc.*, No. 127801. These calculations assume a five-year statute of limitations for Section 15(b) claims.

9,500 class members, class-wide damages could equate to $17.1 billion or more.[12] Simply put, $17.1 billion in damages is grossly disproportionate to the statutory injury alleged by Plaintiff here, and the potential for such an award would create absurd, unreasonably punitive results. *See State Farm*, 538 U.S. at 416-17.

The Seventh Circuit questioned whether a "one and done" approach to accrual would sufficiently incentivize employers such as White Castle to comply with BIPA. Here, Plaintiff purports to allege two violations of the Act, for up to 9,500 current and former White Castle employees. Even under a single accrual method, damages could equate to between $19 million and $95 million if Plaintiff's claims had been timely made, assuming that Plaintiff could recover separately under Section 15(b) and 15(d). Even under a "one violation per employee" calculation of $1,000 per employee, damages could equal $9.5 million. These numbers, in and of themselves, are sufficient to incentivize BIPA compliance.

In summary, the reasonableness of damages under the Act is interwoven with the certified question of whether accrual occurs at the first violation. Single claim accrual aligns the answer to the certified question

[12] It would take White Castle 165 years to generate $17.1 billion in sales in Illinois. And, sales numbers do not include White Castle's costs of sales, operational expenses to keep its restaurants running, or taxes paid to Illinois and the federal government. In an industry where profits (actual cash in hand from sales) range from 6% to 9% annually, White Castle literally will *never* generate enough cash in Illinois to cover such damages.

with the due process clauses of the U.S. and Illinois Constitutions, and thus satisfies the constitutional avoidance canon.

C. Public policy and practicality further support White Castle's position.

Interpreting claim accrual under the Act on a per-scan basis also would create unreasonable and absurd results that violate public policy. In construing BIPA, the Court can consider "not only the language of the statute but also the reason and necessity for the law, the problems sought to be remedied, the purpose to be achieved, and the consequences of construing the statute one way or another." *Lakewood Nursing & Rehab. Ctr., LLC v. Dep't of Pub. Health*, 2019 IL 124019, ¶ 17.

While per-scan accrual and damages would lead to absurd and unjust results for all BIPA defendants, not just White Castle, the outcome is especially absurd here given that Plaintiff twice consented to the use of White Castle's finger-scan system. Moreover, like most employees asserting BIPA claims, Plaintiff has not alleged a data breach or any costs associated with identity theft or compromised data. In fact, considering that over 1,600 BIPA class actions have been filed in Illinois, White Castle is not aware of a single one that alleges an actual data breach.

Additionally, when interpreting the Act, consideration should be given to the "real-world results" of the interpretation, and it must be assumed that "the legislature did not intend unjust consequences." *People v. Fort*, 2017 IL

118966, ¶ 35; *Austin*, 2019 IL 123910, ¶ 15 (courts "must presume that the legislature did not intend to create absurd, inconvenient, or unjust results").

In enacting BIPA, the General Assembly did not outlaw the use of biometrics. It simply intended to incentivize notice of, and consent to, biometrics' use. Overlaying per-scan accrual and damages onto the Act's damages provision fundamentally alters and distorts the nature of the statute and ignores how the Court has defined a BIPA injury. It converts the liquidated damages provision in BIPA from a supplemental enforcement aid to a harshly punitive measure. Under the district court's reading, the Act's liquidated damages provisions no longer function as an alternative mode of relief where damages are small or unquantifiable. Rather, the provisions generate windfall damages that are punitive and wholly untethered to the actual facts (the 2004 and 2018 consents), Plaintiff's injury (she continues to use her biometrics at work and has never revoked consent), and BIPA's plain language.

Other Illinois courts have rejected "per scan" accrual, finding the practical and financial results would be absurd and unsustainable. For example, in *Robertson II*, cited earlier in this brief, the plaintiff advanced the same argument as Plaintiff makes in this case, arguing that each time the defendant collected or disseminated his biometric data constituted a separate, actionable violation of BIPA. *Robertson II*, slip op. at 5 (A044). The court rejected plaintiff's argument, explaining that the interpretation is

"contrary to the unambiguous language of the statute and taken to its logical conclusion would inexorably lead to an absurd result" and "ruinous liability." *Id*. (A044).

According to the allegations in that case, "there exist[ed] at least two potentially recoverable violations for each day [the plaintiff] worked." *Id*. at 6 (A045). In that case, the court calculated that the plaintiff could potentially seek a total of $500,000 for negligent violations of BIPA or $2.5 million for intentional or reckless violations for each year the defendants allegedly violated the statute. *Id*. (A045). The court concluded: "nothing in the statute as it is written or as it was enacted to indicate it was the considered intent of legislature in passing BIPA to impose fines so extreme as to threaten the existence of any business." *Id*. (A045); *see also Smith*, slip op. at 3 (A037) ("the interpretation plaintiff desires would likely force out of business—in droves—violators who without any nefarious intent installed new technology").

Plaintiff has insisted throughout this case that absent a per-scan theory of injury, there is no incentive to protect privacy information under BIPA or that entities with access to personal information are unconcerned with privacy. That's not the case. There is a penalty if an individual is harmed under BIPA, and the damages assessed from an initial violation of the statute ($1,000 or $5,000 per individual) are a sufficient deterrent that disincentives a company from failing to protect biometric data. If a company

fails to abide by BIPA and an individual is aggrieved, the penalties are triggered.

Indeed, that a single-accrual rule provides a sufficient deterrent effect is demonstrated by the numerous BIPA class action settlements to date. For example, following this Court's ruling in *Rosenbach*, Six Flags settled its case for $36 million. Of that, $12 million was paid to class counsel and $24 million to about 1.1 million Six Flags visitors who entered the park between 2013 and 2018. Per-claimant awards were calculated on a *pro rata* basis, not to exceed $200 per plaintiff. *See* Theme Park Class Action Settlement, themeparksettlement.com (last visited Feb. 25, 2022). Thus, in *Rosenbach*, even awarding each claimant a small fraction of the $1,000 or $5,000 in statutory damages they could have gotten for *one* violation resulted in Six Flags paying $36 million. Here, White Castle ultimately could be subject to damages of almost $10 million under a single violation, single accrual damages calculation, and be subject to attorneys' fees, costs, and expert costs. There is no need to exponentially increase the damages that could be available in BIPA cases. The deterrent effect of a single BIPA violation is plenty.

CONCLUSION

The answer to the certified question is that BIPA Section 15(b) and Section 15(d) claims accrue upon the first unauthorized scan or collection, or the first unauthorized disclosure or transmission, of purported biometric identifiers or biometric information.

Dated: March 3, 2022

Respectfully submitted,

WHITE CASTLE SYSTEM, INC.

By: */s/Melissa A. Siebert*

Melissa A. Siebert
William F. Northrip
Matthew C. Wolfe
SHOOK, HARDY & BACON L.L.P.
111 South Wacker Drive
Suite 4700
Chicago, Illinois 60606
Tel: (312) 704 7700
Fax: (312) 558-1195
masiebert@shb.com
wnorthrip@shb.com
mwolfe@shb.com

Counsel for Defendant-Appellant White Castle System, Inc.

CERTIFICATE OF COMPLIANCE

I certify that this brief conforms to the requirements of Rules 341(a) and (b). The length of this brief, excluding the pages or words contained in the Rule 341(d) cover, the Rule 341(h)(1) table of contents and statement of points and authorities, the Rule 341(c) certificate of compliance, the certificate of service, and those matters to be appended to the brief under Rule 342(a), is 50 pages.

Dated: March 3, 2022 */s/ Melissa A. Siebert*

NOTICE OF FILING AND CERTIFICATE OF SERVICE

I, Melissa A. Siebert, an attorney, hereby certify that on **March 3, 2022**, I caused a true and complete copy of the foregoing **BRIEF AND APPENDIX OF DEFENDANT-APPELLANT WHITE CASTLE SYSTEM, INC.** to be filed electronically with the Clerk's Office of the Illinois Supreme Court, using e-filing provider **Odyssey eFileIL**, which sends notification and a copy of this filing by electronic mail to all counsel of record.

I further certify I caused an additional courtesy copy of this filing to be served by electronic mail upon the following:

Ryan F. Stephan
(rstephan@stephanzouras.com)
James B. Zouras
(jzouras@stephanzouras.com)
Andrew C. Ficzko
(aficzko@stephanzouras.com)
Teresa M. Becvar
(tbecvar@stephanzouras.com)
STEPHAN ZOURAS, LLP
100 North Riverside Plaza, Suite 2150
Chicago, IL 60601
Tel: (312) 233-1550

Attorneys for Plaintiff-Appellee Latrina Cothron, Individually, and on Behalf of All Others Similarly Situated

Under penalties as provided by law pursuant to Section 1-109 of the Illinois Code of Civil Procedure, I certify that the above statements set forth in this instrument are true and correct.

/s/ Melissa A. Siebert

No. 128004

IN THE SUPREME COURT OF ILLINOIS

LATRINA COTHRON, *Plaintiff-Appellee*,

v.

WHITE CASTLE SYSTEM, INC., *Defendant-Appellant*.

Question of Law Certified by the United States District Court of Appeals for the Seventh Circuit, Case No. 20-3202

Question of Law ACCEPTED on December 23, 2021 under Supreme Court Rule 20

On appeal from the United States District Court for the Northern District of Illinois under 28 U.S.C. § 1292(b), Case No. 19 CV 00382
The Honorable Judge John J. Tharp, Judge Presiding

APPENDIX TO BRIEF OF DEFENDANT-APPELLANT WHITE CASTLE SYSTEM, INC.

TABLE OF CONTENTS TO APPENDIX

( )

(740 ILCS 14/1)

Sec. 1. Short title. This Act may be cited as the Biometric Information Privacy Act.

(Source: P.A. 95-994, eff. 10-3-08.)

(740 ILCS 14/5)

Sec. 5. Legislative findings; intent. The General Assembly finds all of the following:

(a) The use of biometrics is growing in the business and security screening sectors and appears to promise streamlined financial transactions and security screenings.

(b) Major national corporations have selected the City of Chicago and other locations in this State as pilot testing sites for new applications of biometric-facilitated financial transactions, including finger-scan technologies at grocery stores, gas stations, and school cafeterias.

(c) 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.

(d) An overwhelming majority of members of the public are weary of the use of biometrics when such information is tied to finances and other personal information.

(e) Despite limited State law regulating the collection, use, safeguarding, and storage of biometrics, many members of the public are deterred from partaking in biometric identifier-facilitated transactions.

(f) The full ramifications of biometric technology are not fully known.

(g) The public welfare, security, and safety will be served by regulating the collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and information.

(Source: P.A. 95-994, eff. 10-3-08.)

(740 ILCS 14/10)

Sec. 10. Definitions. In this Act:

"Biometric identifier" means a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry. 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. Biometric identifiers do not include donated organs, tissues, or parts as defined in the Illinois Anatomical Gift Act or blood or serum stored on behalf of recipients or potential recipients of living or cadaveric

transplants and obtained or stored by a federally designated organ procurement agency. Biometric identifiers do not include biological materials regulated under the Genetic Information Privacy Act. Biometric identifiers do not include 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 federal Health Insurance Portability and Accountability Act of 1996. Biometric identifiers do not include an X-ray, roentgen process, computed tomography, MRI, PET scan, mammography, or other image or film of the human anatomy used to diagnose, prognose, or treat an illness or other medical condition or to further validate scientific testing or screening.

"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. Biometric information does not include information derived from items or procedures excluded under the definition of biometric identifiers.

"Confidential and sensitive information" means personal information that can be used to uniquely identify an individual or an individual's account or property. Examples of confidential and sensitive information include, but are not limited to, a genetic marker, genetic testing information, a unique identifier number to locate an account or property, an account number, a PIN number, a pass code, a driver's license number, or a social security number.

"Private entity" means any individual, partnership, corporation, limited liability company, association, or other group, however organized. A private entity does not include a State or local government agency. A private entity does not include any court of Illinois, a clerk of the court, or a judge or justice thereof.

"Written release" means informed written consent or, in the context of employment, a release executed by an employee as a condition of employment.

(Source: P.A. 95-994, eff. 10-3-08.)

(740 ILCS 14/15)

Sec. 15. Retention; collection; disclosure; destruction.

(a) A private entity in possession of biometric identifiers or biometric information must develop a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 3 years of the individual's last interaction with the private entity, whichever occurs first. Absent a valid warrant or subpoena issued by a court of competent jurisdiction, a private entity in possession of biometric identifiers or biometric information must comply with its established retention schedule and destruction guidelines.

(b) No private entity may collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifier or biometric information, unless it first:

(1) informs the subject or the subject's legally authorized representative in writing that a biometric identifier or biometric information is being collected or stored;

(2) informs the subject or the subject's legally authorized representative in writing of the specific purpose and length of term for which a biometric identifier

or biometric information is being collected, stored, and used; and

(3) receives a written release executed by the subject of the biometric identifier or biometric information or the subject's legally authorized representative.

(c) No private entity in possession of a biometric identifier or biometric information may sell, lease, trade, or otherwise profit from a person's or a customer's biometric identifier or biometric information.

(d) No private entity in possession of a biometric identifier or biometric information may disclose, redisclose, or otherwise disseminate a person's or a customer's biometric identifier or biometric information unless:

(1) the subject of the biometric identifier or biometric information or the subject's legally authorized representative consents to the disclosure or redisclosure;

(2) the disclosure or redisclosure completes a financial transaction requested or authorized by the subject of the biometric identifier or the biometric information or the subject's legally authorized representative;

(3) the disclosure or redisclosure is required by State or federal law or municipal ordinance; or

(4) the disclosure is required pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction.

(e) A private entity in possession of a biometric identifier or biometric information shall:

(1) store, transmit, and protect from disclosure all biometric identifiers and biometric information using the reasonable standard of care within the private entity's industry; and

(2) store, transmit, and protect from disclosure all 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.

(Source: P.A. 95-994, eff. 10-3-08.)

(740 ILCS 14/20)

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 recklessly 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.

(Source: P.A. 95-994, eff. 10-3-08.)

(740 ILCS 14/25)

Sec. 25. Construction.

(a) Nothing in this Act shall be construed to impact the admission or discovery of biometric identifiers and biometric information in any action of any kind in any court, or before

any tribunal, board, agency, or person.

(b) Nothing in this Act shall be construed to conflict with the X-Ray Retention Act, the federal Health Insurance Portability and Accountability Act of 1996 and the rules promulgated under either Act.

(c) 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.

(d) Nothing in this Act shall be construed to conflict with the Private Detective, Private Alarm, Private Security, Fingerprint Vendor, and Locksmith Act of 2004 and the rules promulgated thereunder.

(e) 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.

(Source: P.A. 95-994, eff. 10-3-08.)

(740 ILCS 14/30)

Sec. 30. (Repealed).

(Source: P.A. 95-994, eff. 10-3-08. Repealed internally, eff. 1-1-09.)

(740 ILCS 14/99)

Sec. 99. Effective date. This Act takes effect upon becoming law.

(Source: P.A. 95-994, eff. 10-3-08.)

WHITE CASTLE BIOMETRIC INFORMATION PRIVACY TEAM MEMBER CONSENT FORM

The team member named below has been advised and understands that White Castle System, Inc. and its affiliates ("White Castle") collects, retains, and uses biometric data and/or information for the purpose of identifying a team member's signature when utilizing White Castle's proprietary software. Biometric scanners are computer-based systems that scan a team member's finger for purposes of identification. The computer system extracts unique data points and creates a unique mathematical representation used to verify the team member's identity when the team member, for example, signs a document such as a Form I-9 or IRS Form W-4 or has a need to access secure information systems. White Castle deletes such biometric data and/or information when a team member's employment with White Castle ends.

The team member understands that he or she is free to decline to provide biometric identifiers and biometric information to White Castle through its biometrics software. Electing not to provide such consent will not result in any adverse effects on his or her employment with White Castle. Further, the team member may revoke this consent at any time by notifying White Castle in writing.

The undersigned team member voluntarily consents to White Castle's collection, storage, and use of biometric data and/or information through White Castle's proprietary software, including to the extent that it utilizes the team member's biometric identifiers or biometric information as defined in the Illinois Biometric Information Privacy Act (BIPA).

LATRINA L COTHRON	10/15/2018
Print Name	Date
LATRINA L COTHRON	10/15/2018
Signature	Date

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

LATRINA COTHRON, individually, and on behalf of all others similarly situated,	)	
Plaintiff,	)	**Case No. 1:19-cv-00382**
v.	)	**Honorable John J. Tharp Jr.**
WHITE CASTLE SYSTEM, INC. d/b/a WHITE CASTLE,	)	
Defendant.	)	

SECOND AMENDED CLASS ACTION COMPLAINT

Plaintiff Latrina Cothron ("Plaintiff" or "Cothron") individually and on behalf of all others similarly situated (the "Class"), by and through her attorneys, brings the following Second Amended Class Action Complaint ("Complaint") pursuant to Rule 23 of the Federal Rules of Civil Procedure against White Castle System, Inc. d/b/a White Castle, ("White Castle" or "Defendant"), its subsidiaries and affiliates, to redress and curtail Defendant's unlawful collection, use, storage, and disclosure of Plaintiff's sensitive and proprietary biometric data. Plaintiff alleges as follows upon personal knowledge as to herself, her own acts and experiences and, as to all other matters, upon information and belief, including investigation conducted by her attorneys.

NATURE OF THE ACTION

1. Defendant White Castle System, Inc. d/b/a White Castle ("White Castle") is an Ohio corporation that owns and operates hundreds of White Castle fast-food restaurants throughout the country, including Illinois.

2. When White Castle hires an employee, he or she is enrolled in its DigitalPersona employee database, provided by Cross Match Technologies, Inc.,[1] using a scan of his or her fingerprint. White Castle uses the DigitalPersona employee database to distribute its employees' paystubs, among other things, on a weekly basis.

3. While many employers use conventional methods for payroll (direct deposit or paper check), White Castle's employees are required to have their fingerprints scanned by a biometric device to retrieve their paystubs.

4. Biometrics are not relegated to esoteric corners of commerce. Many businesses – such as White Castle – and financial institutions have incorporated biometric applications into their workplace in the form of biometric authenticators, and into consumer products, including such ubiquitous consumer products as checking accounts and cell phones.

5. Unlike ID badges– which can be changed or replaced if stolen or compromised – fingerprints are unique, permanent biometric identifiers associated with each employee. This exposes White Castle's employees to serious and irreversible privacy risks. For example, if a database containing fingerprint data or other sensitive, proprietary biometric data is hacked, breached, or otherwise exposed – like in the recent Yahoo, eBay, Google, Equifax, Uber, Home Depot, Panera, Whole Foods, Chipotle, Trump Hotels, Facebook/Cambridge Analytica, and Marriott data breaches or misuses – employees have ***no*** means by which to prevent identity theft, unauthorized tracking or other unlawful or improper use of this highly personal and private information.

6. In 2015, a data breach at the United States Office of Personnel Management exposed the personal identification information, including biometric data, of over 21.5 million

[1] Cross Match Technologies, Inc. ("Cross Match") is a technology company that provides software and hardware that tracks and monitors employees' biometric data to companies worldwide.

federal employees, contractors, and job applicants. U.S. Off. of Personnel Mgmt., *Cybersecurity Incidents* (2018), *available at* www.opm.gov/cybersecurity/cybersecurity-incidents.

7. An illegal market already exists for biometric data. Hackers and identity thieves have targeted Aadhaar, the largest biometric database in the world, which contains the personal and biometric data – including fingerprints, iris scans, and a facial photograph – of over a billion Indian citizens. *See* Vidhi Doshi, *A Security Breach in India Has Left a Billion People at Risk of Identity Theft*, The Washington Post (Jan. 4, 2018), *available at* https://www.washingtonpost.com/news/worldviews/wp/2018/01/04/a-security-breach-in-india-has-left-a-billion-people-at-risk-of-identity-theft/?utm_term=.b3c70259fl38.

8. In January 2018, an Indian newspaper reported that the information housed in Aadhaar was available for purchase for less than $8 and in as little as 10 minutes. Rachna Khaira, *Rs 500, 10 Minutes, and You Have Access to Billion Aadhaar Details*, The Tribune (Jan. 4, 2018), *available at* http://www.tribuneindia.com/news/nation/rs-500-10-minutes-and-you-have-access-to-billion-aadhaar-details/523361.html.

9. Recognizing the need to protect its citizens from situations like these, Illinois enacted the Biometric Information Privacy Act ("BIPA"), 740 ILCS 14/1, *et seq.*, specifically to regulate companies that collect, store and use Illinois citizens' biometrics, such as fingerprints.

10. Notwithstanding the clear and unequivocal requirements of the law, White Castle disregards its employees' statutorily protected privacy rights and unlawfully collects, stores, disseminates, and uses employees' biometric data in violation of BIPA. Specifically, White Castle has violated and continues to violate BIPA because it did not and continues not to:

a. Properly inform Plaintiff and others similarly situated in writing of the specific purpose(s) and length of time for which their fingerprints were being collected, stored, and used, as required by BIPA;

b. Receive a written release from Plaintiff and others similarly situated to collect, store, or otherwise use their fingerprints, as required by BIPA;

c. Provide a publicly available retention schedule and guidelines for permanently destroying Plaintiff's and other similarly-situated individuals' fingerprints, as required by BIPA; and

d. Obtain consent from Plaintiff and others similarly situated to disclose, redisclose, or otherwise disseminate their fingerprints to a third party as required by BIPA.

11. Accordingly, Plaintiff, on behalf of herself as well as the putative Class, seeks an Order: (1) declaring that White Castle's conduct violates BIPA; (2) requiring White Castle to cease the unlawful activities discussed herein; and (3) awarding statutory damages to Plaintiff and the proposed Class.

PARTIES

12. Plaintiff Latrice Cothron is a natural person and a citizen of the State of Illinois.

13. Defendant White Castle is an Ohio corporation that is registered with the Illinois Secretary of State and conducts business in the State of Illinois, including Cook County.

JURISDICTION AND VENUE

14. This Court has jurisdiction under the Class Action Fairness Act, 28 U.S.C § 1332(d)(2)(A), (d)(5)(B) because the proposed class has 100 or more members, the amount in controversy exceeds $5,000,000.00, and the parties are minimally diverse.

15. Venue is proper in this District under 28 U.S.C. § 1391(b)(2) because a substantial part of the events giving rise to these claims occurred in this judicial district.

FACTUAL BACKGROUND

I. The Biometric Information Privacy Act

16. In the early 2000s, major national corporations started using Chicago and other locations in Illinois to test "new applications of biometric-facilitated financial transactions,

including finger-scan technologies at grocery stores, gas stations, and school cafeterias." 740 ILCS § 14/5(c). Given its relative infancy, an overwhelming portion of the public became weary of this then-growing yet unregulated technology. *See* 740 ILCS § 14/5.

17. In late 2007, a biometrics company called Pay by Touch, which provided major retailers throughout the State of Illinois with fingerprint scanners to facilitate consumer transactions, filed for bankruptcy. That bankruptcy was alarming to the Illinois Legislature because suddenly there was a serious risk that millions of fingerprint records – which, like other unique biometric identifiers, can be linked to people's sensitive financial and personal data – could now be sold, distributed, or otherwise shared through the bankruptcy proceedings without adequate protections for Illinois citizens. The bankruptcy also highlighted the fact that most consumers who used the company's fingerprint scanners were completely unaware that the scanners were not actually transmitting fingerprint data to the retailer who deployed the scanner, but rather to the now-bankrupt company, and that their unique biometric identifiers could now be sold to unknown third parties.

18. Recognizing the "very serious need [for] protections for the citizens of Illinois when it [came to their] biometric information," Illinois enacted BIPA in 2008. *See* Illinois House Transcript, 2008 Reg. Sess. No. 276; 740 ILCS § 14/5.

19. Additionally, to ensure compliance, BIPA provides that, for each violation, the prevailing party may recover $1,000 or actual damages, whichever is greater, for negligent violations and $5,000, or actual damages, whichever is greater, for intentional or reckless violations. 740 ILCS 14/20.

20. BIPA is an informed consent statute which achieves its goal by making it unlawful for a company to, among other things, collect, capture, purchase, receive through trade, or

otherwise obtain a person's or a customer's biometric identifiers or biometric information, unless it first:

a. Informs the subject in writing that a biometric identifier or biometric information is being collected, stored and used;

b. Informs the subject in writing of the specific purpose(s) and length of term for which a biometric identifier or biometric information is being collected, stored, and used; and

c. Receives a written release executed by the subject of the biometric identifier or biometric information.

See 740 ILCS § 14/15(b).

21. BIPA specifically applies to employees who work in the State of Illinois. BIPA defines a "written release" specifically "in the context of employment [as] a release executed by an employee as a condition of employment." 740 ILCS 14/10.

22. Biometric identifiers include retina and iris scans, voiceprints, scans of hand and face geometry, and – most importantly here – fingerprints. *See* 740 ILCS § 14/10. Biometric information is separately defined to include any information based on an individual's biometric identifier that is used to identify an individual. *Id*.

23. BIPA also establishes standards for how companies must handle Illinois citizens' biometric identifiers and biometric information. *See, e.g.,* 740 ILCS § 14/15(c)-(d). For example, BIPA prohibits private entities from disclosing a person's biometric identifier or biometric information without first obtaining consent for such disclosure. *See* 740 ILCS § 14/15(d)(1).

24. BIPA also prohibits selling, leasing, trading, or otherwise profiting from a person's biometric identifiers or biometric information (740 ILCS § 14/15(c)) and requires companies to develop and comply with a written policy – made available to the public – establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric

information when the initial purpose for collecting such identifiers or information has been satisfied or within three years of the individual's last interaction with the company, whichever occurs first. 740 ILCS § 14/15(a).

25. The Illinois legislature enacted BIPA due to the increasing use of biometric data in financial and security settings, the general public's hesitation to use biometric information, and – most significantly – the unknown ramifications of biometric technology. Biometrics are biologically unique to the individual and, once compromised, an individual is at heightened risk for identity theft and left without any recourse. Biometric data, unlike other personal identifiers such as a social security number, cannot be changed or replaced if hacked or stolen.

26. BIPA provides individuals with a private right of action, protecting their right to privacy regarding their biometrics as well as protecting their rights to know the precise nature for which their biometrics are used and how they are being stored and ultimately destroyed. Unlike other statutes that only create a right of action if there is a qualifying data breach, BIPA strictly regulates the manner in which entities may collect, store, use, and disseminate biometrics and creates a private right of action for lack of statutory compliance.

II. Defendant Violates the Biometric Information Privacy Act.

27. By the time BIPA passed through the Illinois legislature in mid-2008, most companies who had experimented using individuals' biometric data stopped doing so.

28. However, Defendant failed to take note of the shift in Illinois law governing the collection, use and dissemination of biometric data. As a result, White Castle continues to collect, store, use and disseminate employees' biometric data in violation of BIPA.

29. Specifically, when employees are hired by White Castle, they are required to have their fingerprints captured and stored to enroll them in its DigitalPersona employee database(s).

30. White Castle uses an employee authentication software system supplied by Cross Match that requires employees to use their fingerprints as a means of authentication.

31. Upon information and belief, White Castle fails to inform its employees that it discloses or disclosed their fingerprint data to at least two out-of-state third-party vendors: Cross Match and DigitalPersona, and likely others; fails to inform its employees that it discloses their fingerprint data to other, currently unknown, third parties, which host the biometric data in their data centers; fails to inform its employees of the purposes and duration for which it collects their sensitive biometric data; and fails to obtain written releases from employees before collecting their fingerprint data.

32. Furthermore, White Castle fails to provide employees with a written, publicly available policy identifying its retention schedule and guidelines for permanently destroying employees' fingerprint data when the initial purpose for collecting or obtaining their fingerprint data is no longer relevant, as required by BIPA.

33. The Pay by Touch bankruptcy that catalyzed the passage of BIPA highlights why such conduct – where individuals are aware that they are providing biometric information but not aware to whom or for what purposes they are doing so – is dangerous. That bankruptcy spurred Illinois citizens and legislators into realizing that it is crucial for individuals to understand when providing biometric identifiers, such as their fingerprints, who exactly is collecting their biometric data, where it will be transmitted and for what purposes, and for how long. White Castle disregards these obligations, and its employees' statutory rights, and instead unlawfully collects, stores, uses and disseminates its employees' biometric identifiers and information, without ever receiving the individual's informed written consent required by BIPA.

34. Upon information and belief, White Castle lacks retention schedules and guidelines for permanently destroying Plaintiff's and other similarly-situated individuals' biometric data and has not and will not destroy Plaintiff's and other similarly-situated individuals' biometric data when the initial purpose for collecting or obtaining such data has been satisfied or within three years of the employee's last interaction with the company.

35. White Castle's employees are not told what might happen to their biometric data if and when it merges with another company or worse, if and when its business folds, or when the other third parties that have received their biometric data businesses fold.

36. Since White Castle neither publishes BIPA-mandated data retention policies nor discloses all purposes for its collection of biometric data, White Castle's employees have no idea the extent to whom it sells, discloses, re-discloses, or otherwise disseminates their biometric data. Moreover, Plaintiff and the putative Class are not told to whom White Castle currently discloses their biometric data, or what might happen to their biometric data in the event of a merger or a bankruptcy.

37. These violations have raised a material risk that Plaintiff's and other similarly-situated individuals' biometric data will be unlawfully accessed by third parties.

38. By and through the actions detailed above, White Castle disregards Plaintiff's and other similarly-situated individuals' legal rights in violation of BIPA.

III. Plaintiff Latrina Cothron's Experience

39. Plaintiff Latrina Cothron was hired by White Castle in 2004 and is currently working as a manager.

40. Approximately three years into Plaintiff's employment with White Castle, Plaintiff ***was required*** to scan and register her fingerprint(s) so White Castle could use them as an

authentication method for Plaintiff to access the computer as a manager and to access her paystubs as an hourly employee as a condition of employment with White Castle.

41. At this time, White Castle did not inform Plaintiff in writing or otherwise of the purpose(s) and length of time for which her fingerprint data was being collected, did not receive a written release from Plaintiff to collect, store or use her fingerprint data, did not provide a publicly available retention schedule and guidelines for permanently destroying Plaintiff's fingerprint data, nor did White Castle obtain Plaintiff's consent before disclosing or disseminating her biometric data to third parties.

42. White Castle subsequently stored Plaintiff's fingerprint data in its DigitalPersona employee database(s).

43. Plaintiff was required to scan her fingerprint each time she accessed a White Castle computer.

44. Plaintiff was also required to scan her fingerprint each time she accessed her paystubs.

45. It was not until October of 2018—approximately 11 years after collecting, storing, using, disclosing and disseminating her biometric data—that White Castle provided Plaintiff with an apparent "consent form".

46. Further, Plaintiff ***was required*** to scan her already registered fingerprint in order to electronically sign the apparent "consent form" provided by White Castle.

47. Plaintiff had never been informed, **prior** to the collection of her biometric identifiers and/or biometric information, of the specific purposes or length of time for which White Castle collected, stored, used, and/or disseminated her biometric data.

48. **Prior** to the collection of her biometric identifiers and/or biometric information, Plaintiff had never been informed of any biometric retention policy developed by White Castle, nor had she ever been informed whether White Castle will ever permanently delete her biometric data.

49. **Prior** to the collection of her biometric identifiers and/or biometric information, Plaintiff had never been provided with nor ever signed a written release allowing White Castle to collect, store, use, or disseminate her biometric data.

50. Plaintiff has continuously and repeatedly been exposed to the risks and harmful conditions created by White Castle's multiple violations of BIPA alleged herein.

51. No amount of time or money can compensate Plaintiff if her biometric data is compromised by the lax procedures through which White Castle captured, stored, used, and disseminated her and other similarly-situated individuals' biometric data. Moreover, Plaintiff would not have provided her biometric data to White Castle if she had known that it would retain such information for an indefinite period of time without her consent.

52. A showing of actual damages is not necessary in order to state a claim under BIPA. *See Rosenbach v. Six Flags Ent. Corp.*, 2019 IL 123186, ¶ 40 ("[A]n individual need not allege some actual injury or adverse effect, beyond violation of his or her rights under the Act, in order to qualify as an "aggrieved" person and be entitled to seek liquidated damages and injunctive relief pursuant to the Act"). Nonetheless, Plaintiff has been aggrieved because she suffered an injury-in-fact based on White Castle's violations of her legal rights. White Castle intentionally interfered with Plaintiff's right to possess and control her own sensitive biometric data. Additionally, Plaintiff suffered an invasion of a legally protected interest when White Castle secured her personal and private biometric data at a time when it had no legal right to do so, a gross invasion of her right to

privacy. BIPA protects employees like Plaintiff from this precise conduct. White Castle had no lawful right to secure this data or share it with third parties absent a specific legislative license to do so.

53. Plaintiff's biometric information is economically valuable, and such value will increase as the commercialization of biometrics continues to grow. As such, Plaintiff was not sufficiently compensated by White Castle for its retention and use of her and other similarly-situated employees' biometric data.

54. Plaintiff also suffered an informational injury because White Castle failed to provide her with information to which she was entitled by statute. Through BIPA, the Illinois legislature has created a right: an employee's right to receive certain information prior to an employer securing their highly personal, private and proprietary biometric data: and in injury – not receiving this extremely critical information.

55. Plaintiff also suffered an injury in fact because White Castle improperly disseminated her biometric identifiers and biometric information to third parties, including Cross Match and DigitalPersona, and others that hosted the biometric data in their data centers, in violation of BIPA.

56. Pursuant to 740 ILCS 14/15(b), Plaintiff was entitled to receive certain information prior to White Castle securing her biometric data; namely, information advising her of the specific limited purpose(s) and length of time for which White Castle collects, stores, uses, and disseminates her biometric data; information regarding White Castle's biometric retention policy; and, a written release allowing White Castle to collect, store, use, and disseminate her private biometric data. By depriving Plaintiff of this information, White Castle injured her. *Public Citizen*

v. U.S. Department of Justice, 491 U.S. 440, 449 (1989); *Federal Election Commission v. Atkins*, 524 U.S. 11 (1998).

57. Plaintiff has plausibly inferred actual and ongoing harm in the form of monetary damages for the value of the collection and retention of her biometric data; in the form of monetary damages by not obtaining additional compensation as a result of being denied access to material information about White Castle's policies and practices; in the form of the unauthorized disclosure of her confidential biometric data to third parties, including but not limited to Cross Match and DigitalPersona; in the form of interference with her right to control and possess her confidential biometric data; and, in the form of the continuous and ongoing exposure to substantial and irreversible loss of privacy.

58. As Plaintiff is not required to allege or prove actual damages in order to state a claim under BIPA, she seeks statutory damages under BIPA as compensation for the injuries caused by White Castle. *Rosenbach*, 2019 IL 123186, ¶ 40.

CLASS ALLEGATIONS

59. Pursuant to Rule 23(a) and 23(b) of the Federal Rules of Civil Procedure, Plaintiff brings claims on her own behalf and as representative of all other similarly-situated individuals pursuant to BIPA, 740 ILCS 14/1 *et seq.*, to recover statutory penalties, prejudgment interest, attorneys' fees and costs, and other damages owed.

60. As discussed *supra*, Section 14/15(b) of BIPA prohibits a company from, among other things, collecting, capturing, purchasing, receiving through trade, or otherwise obtaining a person's or a customer's biometric identifiers or biometric information, unless it **first** (1) informs the individual in writing that a biometric identifier or biometric information is being collected or stored; (2) informs the individual in writing of the specific purpose and length of time for which a

biometric identifier or biometric information is being collected, stored, and used; ***and*** (3) receives a written release executed by the subject of the biometric identifier or biometric information. 740 ILCS § 14/15.

61. Plaintiff seeks class certification for the following class of similarly-situated individuals under BIPA:

> All individuals working for White Castle in the State of Illinois who had their fingerprints collected, captured, received, obtained, maintained, stored or disclosed by White Castle during the applicable statutory period.

62. This action is properly maintained as a class action under Rule 23 because:

A. The class is so numerous that joinder of all members is impracticable;

B. There are questions of law or fact that are common to the class;

C. The claims of the Plaintiff are typical of the claims of the class; and,

D. The Plaintiff will fairly and adequately protect the interests of the class.

Numerosity

63. The total number of putative class members exceeds 100 individuals. The exact number of class members can easily be determined from White Castle's payroll records.

Commonality

64. There is a well-defined commonality of interest in the substantial questions of law and fact concerning and affecting the Class in that Plaintiff and all members of the Class have been harmed by Defendant's failure to comply with BIPA. The common questions of law and fact include, but are not limited to the following:

A. Whether Defendant collected, captured or otherwise obtained Plaintiff's and the Class's biometric identifiers or biometric information;

B. Whether Defendant properly informed Plaintiff and the Class of its purposes for collecting, using, storing and disseminating their biometric identifiers or biometric information;

C. Whether Defendant obtained a written release (as defined in 740 ILCS § 14/10) to collect, use, store and disseminate Plaintiff's and the Class's biometric identifiers or biometric information;

D. Whether Defendant has disclosed or re-disclosed Plaintiff's and the Class's biometric identifiers or biometric information;

E. Whether Defendant has sold, leased, traded, or otherwise profited from Plaintiff's and the Class's biometric identifiers or biometric information;

F. Whether Defendant developed a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within three years of their last interaction with the individual, whichever occurs first;

G. Whether Defendant complies with any such written policy (if one exists);

H. Whether Defendant used Plaintiff's and the Class's fingerprints to identify them;

I. Whether Defendant's violations of BIPA have raised a material risk that Plaintiff's biometric data will be unlawfully accessed by third parties;

J. Whether the violations of BIPA were committed negligently; and

K. Whether the violations of BIPA were committed intentionally and/or recklessly.

65. Plaintiff anticipates that Defendant will raise defenses that are common to the class.

Adequacy

66. Plaintiff will fairly and adequately protect the interests of all members of the class, and there are no known conflicts of interest between Plaintiff and class members. Plaintiff, moreover, has retained experienced counsel that are competent in the prosecution of complex litigation and who have extensive experience acting as class counsel.

Typicality

67. The claims asserted by Plaintiff are typical of the class members she seeks to

represent. Plaintiff has the same interests and suffers from the same unlawful practices as the class members.

68. Upon information and belief, there are no other class members who have an interest individually controlling the prosecution of his or her individual claims, especially in light of the relatively small value of each claim and the difficulties involved in bringing individual litigation against one's employer. However, if any such class member should become known, he or she can "opt out" of this action pursuant to Rule 23(b)(3).

Predominance and Superiority

69. The common questions identified above predominate over any individual issues, which will relate solely to the quantum of relief due to individual class members. A class action is superior to other available means for the fair and efficient adjudication of this controversy because individual joinder of the parties is impracticable. Class action treatment will allow a large number of similarly-situated persons to prosecute their common claims in a single forum simultaneously, efficiently and without the unnecessary duplication of effort and expense if these claims were brought individually. Moreover, as the damages suffered by each class member are relatively small in the sense pertinent to class action analysis, the expenses and burden of individual litigation would make it difficult for individual class members to vindicate their claims.

70. Additionally, important public interests will be served by addressing the matter as a class action. The cost to the court system and the public for the adjudication of individual litigation and claims would be substantially more than if claims are treated as a class action. Prosecution of separate actions by individual class members would create a risk of inconsistent and varying adjudications, establish incompatible standards of conduct for Defendant and/or substantially impair or impede the ability of class members to protect their interests. The issues in

this action can be decided by means of common, class-wide proof. In addition, if appropriate, the Court can and is empowered to fashion methods to efficiently manage this action as a class action.

FIRST CAUSE OF ACTION
Violation of 740 ILCS § 14/15(a): Failure to Institute, Maintain and Adhere to Publicly-Available Retention Schedule

71. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

72. BIPA mandates that companies in possession of biometric data establish and maintain a satisfactory biometric data retention – and, importantly, deletion – policy. Specifically, those companies must: (i) make publicly available a written policy establishing a retention schedule and guidelines for permanent deletion of biometric data (at most three years after the company's last interaction with the individual); and (ii) actually adhere to that retention schedule and actually delete the biometric information. *See* 740 ILCS § 14/15(a).

73. Defendant fails to comply with these BIPA mandates.

74. Defendant White Castle is an Ohio corporation registered to do business in Illinois and thus qualifies as a "private entity" under BIPA. *See* 740 ILCS § 14/10.

75. Plaintiff and the Class are individuals who have had their "biometric identifiers" collected by White Castle (in the form of their fingerprints), as explained in detail in Sections II and III, *supra*. *See* 740 ILCS § 14/10.

76. Plaintiff's and the Class's biometric identifiers were used to identify them and, therefore, constitute "biometric information" as defined by BIPA. *See* 740 ILCS § 14/10.

77. Defendant failed to provide a publicly available retention schedule or guidelines for permanently destroying biometric identifiers and biometric information as specified by BIPA. *See* 740 ILCS § 14/15(a).

78. Upon information and belief, Defendant lacked retention schedules and guidelines for permanently destroying Plaintiff's and the Class's biometric data.

79. On behalf of herself and the Class, Plaintiff seeks: (1) declaratory relief; (2) injunctive and equitable relief as is necessary to protect the interests of Plaintiff and the Class by requiring Defendant to comply with BIPA's requirements for the collection, storage, use and dissemination of biometric identifiers and biometric information as described herein; (3) statutory damages of $5,000 for each intentional and/or reckless violation of BIPA pursuant to 740 ILCS 14/20(2) or, in the alternative, statutory damages of $1,000 for each negligent violation of BIPA pursuant to 740 ILCS 14/20(1); and (4) reasonable attorneys' fees and costs and other litigation expenses pursuant to 740 ILCS 14/20(3).

SECOND CAUSE OF ACTION
Violation of 740 ILCS § 14/15(b): Failure to Obtain Informed Written Consent and Release Before Obtaining Biometric Identifiers or Information

80. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

81. BIPA requires companies to obtain informed written consent from employees **before** acquiring their biometric data. Specifically, BIPA makes it unlawful for any private entity to "collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifiers or biometric information unless [the entity] first: (1) informs the subject…in writing that a biometric identifier or biometric information is being collected or stored; (2) informs the subject…in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; ***and*** (3) receives a written release executed by the subject of the biometric identifier or biometric information…" 740 ILCS 14/15(b) (emphasis added).

82. Defendant failed to comply with these BIPA mandates.

83. Defendant White Castle is an Ohio corporation registered to do business in Illinois and thus qualifies as a "private entity" under BIPA. *See* 740 ILCS § 14/10.

84. Plaintiff and the Class are individuals who have had their "biometric identifiers" collected by White Castle (in the form of their fingerprints), as explained in detail in Sections II and III, *supra*. *See* 740 ILCS § 14/10.

85. Plaintiff's and the Class's biometric identifiers were used to identify them and, therefore, constitute "biometric information" as defined by BIPA. *See* 740 ILCS § 14/10.

86. Defendant systematically and automatically collected, used, and stored Plaintiff's biometric identifiers and/or biometric information without first obtaining the written release required by 740 ILCS 14/15(b)(3).

87. Prior to collecting their biometric data, Defendant did not inform Plaintiff and the Class in writing that their biometric identifiers and/or biometric information were being collected, stored and used, nor did Defendant inform Plaintiff and the Class in writing of the specific purpose and length of term for which their biometric identifiers and/or biometric information were being collected, stored, and used as required by 740 ILCS 14/15(b)(1)-(2).

88. By collecting, storing, and using Plaintiff's and the Class's biometric identifiers and biometric information as described herein, Defendant violated Plaintiff's and the Class's rights to privacy in their biometric identifiers or biometric information as set forth in BIPA. *See* 740 ILCS 14/1, *et seq*.

89. On behalf of herself and the Class, Plaintiff seeks: (1) declaratory relief; (2) injunctive and equitable relief as is necessary to protect the interests of Plaintiff and the Class by requiring Defendant to comply with BIPA's requirements for the collection, storage, use and dissemination of biometric identifiers and biometric information as described herein; (3) statutory

damages of $5,000 for each intentional and/or reckless violation of BIPA pursuant to 740 ILCS 14/20(2) or, in the alternative, statutory damages of $1,000 for each negligent violation of BIPA pursuant to 740 ILCS 14/20(1); and (4) reasonable attorneys' fees and costs and other litigation expenses pursuant to 740 ILCS 14/20(3).

THIRD CAUSE OF ACTION
Violation of 740 ILCS § 14/15(d): Disclosure of Biometric Identifiers and Information Before Obtaining Consent

90. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

91. BIPA prohibits private entities from disclosing a person's or customer's biometric identifier or biometric information without **first** obtaining consent for that disclosure. *See* 740 ILCS 14/15(d)(1).

92. Defendant fails to comply with this BIPA mandate.

93. Defendant White Castle is an Ohio corporation registered to do business in Illinois and thus qualifies as a "private entity" under BIPA. *See* 740 ILCS § 14/10.

94. Plaintiff and the Class are individuals who have had their "biometric identifiers" collected by White Castle (in the form of their fingerprints), as explained in detail in Sections II and III, *supra*. *See* 740 ILCS § 14/10.

95. Plaintiff's and the Class's biometric identifiers were used to identify them and, therefore, constitute "biometric information" as defined by BIPA. *See* 740 ILCS § 14/10.

96. Defendant systematically and automatically disclosed, redisclosed, or otherwise disseminated Plaintiff's biometric identifiers and/or biometric information without first obtaining the consent required by 740 ILCS 14/15(d)(1).

97. By disclosing, redisclosing, or otherwise disseminating Plaintiff's and the Class's biometric identifiers and biometric information as described herein, Defendant violated Plaintiff's

and the Class's rights to privacy in their biometric identifiers or biometric information as set forth in BIPA. *See* 740 ILCS 14/1, *et seq.*

98. On behalf of herself and the Class, Plaintiff seeks: (1) declaratory relief; (2) injunctive and equitable relief as is necessary to protect the interests of Plaintiff and the Class by requiring Defendant to comply with BIPA's requirements for the collection, storage, use and dissemination of biometric identifiers and biometric information as described herein; (3) statutory damages of $5,000 for each intentional and/or reckless violation of BIPA pursuant to 740 ILCS § 14/20(2) or, in the alternative, statutory damages of $1,000 for each negligent violation of BIPA pursuant to 740 ILCS § 14/20(1); and (4) reasonable attorneys' fees and costs and other litigation expenses pursuant to 740 ILCS § 14/20(3).

PRAYER FOR RELIEF

Wherefore, Plaintiff Latrina Cothron respectfully requests that this Court enter an Order:

A. Certifying this case as a class action on behalf of the Class defined above, appointing Plaintiff Latrina Cothron as Class Representative, and appointing Stephan Zouras, LLP, as Class Counsel;

B. Declaring that Defendant's actions, as set forth above, violate BIPA;

C. Awarding statutory damages of $5,000 for *each* reckless and/or intentional violation of BIPA pursuant to 740 ILCS § 14/20(2) or, in the alternative, statutory damages of $1,000 for *each* negligent violation of BIPA pursuant to 740 ILCS § 14/20(1);

D. Declaring that Defendant's actions, as set forth above, were intentional or reckless;

E. Awarding injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and the Class, including an Order requiring Defendant to collect, store, use and disseminate biometric identifiers and/or biometric information in compliance with BIPA;

F. Awarding Plaintiff and the Class their reasonable attorneys' fees and costs and other litigation expenses pursuant to 740 ILCS § 14/20(3);

G. Awarding Plaintiff and the Class pre- and post-judgment interest, to the extent allowable; and,

H. Awarding such other and further relief as equity and justice may require.

JURY TRIAL

Plaintiff demands a trial by jury for all issues so triable.

Date: April 11, 2019

Respectfully Submitted,

/s/ Andrew C. Ficzko

Ryan F. Stephan
Andrew C. Ficzko
STEPHAN ZOURAS, LLP
100 N. Riverside Plaza
Suite 2150
Chicago, Illinois 60606
312.233.1550
312.233.1560 *f*
rstephan@stephanzouras.com
aficzko@stephanzouras.com

ATTORNEYS FOR PLAINTIFF

CERTIFICATE OF SERVICE

I, the attorney, hereby certify that on April 11, 2019, I filed the attached with the Clerk of the Court using the electronic filing system which will send such filing to all attorneys of record.

/s/ Andrew C. Ficzko

IN THE CIRCUIT COURT OF COOK COUNTY, ILLINOIS
COUNTY DEPARTMENT, CHANCERY DIVISION

THOMAS ROBERTSON, individually, and on behalf of all others similarly situated,	)	
Plaintiff,	)	
v.	)	**Case No. 18-CH-5194**
HOSTMARK HOSPITALITY GROUP, INC., et al,	)	
Defendants,	)	

MEMORANDUM AND ORDER

Defendants Hostmark Hospitality Group, Inc. and Raintree Enterprises Mart Plaza, Inc. have filed a motion to reconsider this court's July 31, 2019 Memorandum and Order pursuant to 735 ILCS 5/2-1203(a).

I. Background

On April 20, 2018, Plaintiff Thomas Robertson ("Robertson") filed his original complaint alleging Defendants Hostmark Hospitality Group, Inc. ("Hostmark") and Raintree Enterprises Mart Plaza, Inc. ("Raintree") (collectively "Defendants") violated the Biometric Information Privacy Act ("BIPA").

On April 1, 2019, this court granted Robertson's motion for leave to file an amended class action complaint (the "Amended Complaint"). The Amended Complaint now alleges three counts, each alleging a violation of a different subsection of section 15 of BIPA. 740 ILCS 14/15.

Count I alleges a violation of subsection 15(a) based upon Defendants alleged failure to institute, maintain, and adhere to a publicly available retention and deletion schedule for biometric data. 740 ILCS 14/15(a). Count II alleges a violation of subsection 15(b) based upon Defendants alleged, failure to obtain written consent prior to collecting and releasing biometric data. 740 ILCS 14/15(b). Count III alleges a violation of subsection 15(d) based upon Defendants alleged, failure to obtain consent before disclosing biometric data. 740 ILCS 14/15(d).

On July 31, 2019, this court issued its Memorandum and Order denying Defendants' motion to dismiss Robertson's Amended Complaint. In summary, this court held that: (1) Robertson's claim was not preempted by the Illinois Worker's Compensation Act; (2) the applicable statute of limitations was five years, as provided for in 735 ILCS 5/13-205; and (3) Robertson had adequately pled his claim.

As part of this court's ruling, this court addressed the parties' arguments regarding the date Defendants stopped collecting Robertson's biometric information, but did not address their arguments regarding when Robertson's claims accrued.

On August 30, 2019, Defendants filed their motion to reconsider and certify questions to the appellate court. In their motion to reconsider, Defendants argued, *inter alia*, that this court erred in applying a five year statute of limitations to Robertson's claim. On September 4, 2019, this court denied the majority of Defendants' motion, but allowed briefing on the issue of the application of the five year statute of limitation.

II. Motion to Reconsider

"The intended purpose of a motion to reconsider is to bring to the court's attention newly discovered evidence, changes in the law, or errors in the court's previous application of existing law." Chelkova v. Southland Corp., 331 Ill. App. 3d 716, 729-30 (1st Dist. 2002). A party may not raise a new legal or factual argument in a motion to reconsider. North River Ins. Co. v. Grinnell Mut. Reinsurance Co., 369 Ill. App. 3d 563, 572 (1st Dist. 2006).

Defendants argue this court erred in holding that the five year statute of limitations was triggered by the date Defendants *stopped* collecting Robertson's biometric data, instead of the date they *started* doing so since that was the date the cause of action first accrued.

Robertson responds that the court was correct in focusing on the date Defendants *stopped* collecting his biometric data because, they argue, when Defendants' actions constitute a "continuing injury" or "continuing violation" the cause of action does not accrue until the commission of the last act in the series.

A. Accrual date

"Generally, in tort, a cause of action accrues and the limitations period begins to run when facts exist that authorize one party to maintain an action against another." Blair v. Nevada Landing Partnership, 369 Ill. App. 3d 318, 323 (2nd Dist. 2006) (citing Feltmeier v. Feltmeier, 207 Ill. 2d 263, 278 (2003)). "Indeed, a plaintiff's cause of action in tort usually accrues at the time his or her interest is invaded." Blair, 369 Ill. App. 3d at 323.

"[A]n exception to the general rule exists when the tort at issue involves a continuing or repeated injury." Blair, 369 Ill. App. 3d at 323 (citing Feltmeier, 207 Ill. 2d at 278). "Under the [']continuing violation rule,['] where a tort involves a continuing or repeated injury, the limitations period does not begin to run until the date of the last injury or the date the tortious acts cease." Blair, 369 Ill. App. 3d at 323-24. "A continuing violation or tort is occasioned by continuing unlawful acts and conduct, not by continual ill effects from an initial violation." Feltmeier, 207 Ill. 2d at 278. "A continuing tort, therefore, does not involve tolling the statute of limitations because of delayed or continuing injuries, but instead involves viewing the defendant's conduct as a continuous whole for prescriptive purposes." Feltmeier, 207 Ill. 2d at 279.

However, "where there is a single overt act from which subsequent damages may flow, the statute begins to run on the date the defendant invaded the plaintiff's interest and inflicted injury, and this is so despite the continuing nature of the injury." Feltmeier v. Feltmeier, 207 Ill. 2d at 279.

Section 20 of BIPA provides that a person aggrieved by a violation of the Act shall have a cause of action and may recover for each violation as provided for in section 20. 740 ILCS 14/20. Because Robertson's Amended Complaint pleads three distinct violations of BIPA the court will address each in turn.

1. Section 14/15 (a) – Publicly available retention and deletion policy (Count I)

Robertson's Amended Complaint specially alleges that Defendants began collecting his biometric data in 2010 without having first adopted any guidelines for permanently destroying his biometric data, in violation of the requirements of section 15(a). (Amended Compl. at ¶¶33, 36, 38); 740 ILCS 15(a)

Section 15 (a) of BIPA provides, in the salient part:

> (a) A private entity in possession of biometric identifiers or biometric information **must** develop a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information **when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 3 years of the individual's last interaction with the private entity, whichever occurs first.**

740 ILCS 14/15 (a) (emphasis ours).

Simply put, the statute requires that at the time Defendants first acquired Robertson's biometrics, they were required to have in place a written scheduled for the retention of the biometric data they collected, as well as guidelines for destruction of that biometric data in conformance with stated written policy or, if no written policy existed, within 3 years of Robertson's last interaction with the Defendants.

Here, Defendants alleged collected Robertson's biometric data without having in place any written scheduled for the retention of the data they collected and without having in place any written guidelines for its destruction. So, per the statute, Defendants – having no destruction policy in place, were required to destroy the data within 3 years of Robertson's final interaction with them.

Robertson alleges they failed to do so.

Defendants have asserted under oath that they stopped collecting Robertson's biometric data in 2013. Per the statute, this claim could not begin accruing until three years afterward, in 2016. Calculating the 5 year statute of limitations from 2016, the year of accrual, Robertson had until 2021 to file his claim.

Since Robertson first filed his original complaint on April 20, 2018, he was well within the statute of limitations when he did so. Therefore, this court did not err in so holding.

2.Section 14/15 (b) – Written consent prior to collection (Count II)

Section 15 (b) provides:

> (b) No private entity may collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifier or biometric information, *unless it first*:
>
> > (1) informs the subject or the subject's legally authorized representative in writing that a biometric identifier or biometric information is being collected or stored;
> >
> > (2) informs the subject or the subject's legally authorized representative in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; and
> >
> > (3) receives a written release executed by the subject of the biometric identifier or biometric information or the subject's legally authorized representative.

740 ILCS 14/15 (b) (emphasis added). Section 10 of BIPA defines "written release" "[. . .] in the context of employment, [as] a release executed by an employee as a condition of employment." 740 ILCS 14/10.

Here, the court did err in its application of the five year statute of limitations. Robertson alleges, and Defendants do not dispute, that Defendants began collecting his biometric data in 2010 as a requirement of his employment. (Amended Compl. at ¶¶41-42). Section 15 (b) of BIPA unambiguously provides that before a private entity can collect an individual's biometric data it must *first* obtain, among other things, a written release as defined by section 10 of BIPA. 740 ILCS 14/15 (b); 740 ILCS 14/10.

As the Illinois Supreme Court stated in Rosenbach, "[c]ompliance [with BIPA] should not be difficult." Rosenbach v. Six Flags Entertainment Corp., 2019 IL 123186, ¶ 37. The most reasonable and practical reading of section 15 (b) requires an employer to obtain a single written release as a condition of employment from an employee or his or her legally authorized representative to allow the collection of his or her biometric data for timekeeping purposes for the duration of his or her employment. Such a release need not be executed before every instance an employee clocks-in and out, rather a single release should suffice to allow the collection of an employee's biometric data. An employer's failure to obtain written consent *first* before collecting an employee's biometric data violates section 15 (b)'s dictates.

In the case at bar, Robertson's statutory rights were first invaded in 2010 when Defendants took his biometric data without first obtaining his consent as required by section 15 (b). 740 ILCS 14/15 (b). Therefore, under the general rule Robertson's claim began accruing in 2010. Blair, 369 Ill. App. 3d at 323.

Robertson's argument that because Defendants have "continuously violated" section 15 (b) during Robertson's employment, the statute of limitations date continued to advance with each subsequent violation is contrary to the underlying rationale of the "continuing violation doctrine."

In this regard, the court finds persuasive and instructive the Seventh Circuit's characterization of the continuing violation doctrine in Limestone Development Corp. v. Village of Lemont, 520 F.3d 797 (7th Cir. 2008). In Limestone, Judge Posner speaking for the Seventh Circuit characterized the continuing violation doctrine as follows:

> Like too many legal doctrines, the "continuing violation" doctrine is misnamed. Suppose that year after year, for ten years, your employer pays you less than the minimum wage. That is a continuing violation. But it does not entitle you to wait until year 15 (assuming for the sake of illustration that the statute of limitations is five years) and then sue not only for the wages you should have received in year 10 but also for the wages you should have received in years 1 through 9. *The statute of limitations begins to run upon injury [. . .] and is not tolled by subsequent injuries.*
>
> The office of the misnamed doctrine is to allow suit to be delayed until a series of wrongful acts blossoms into an injury on which suit can be brought. [citations]. It is thus a doctrine not about a continuing, but about a cumulative, violation.

Limestone Development Corp. v. Village of Lemont, 520 F.3d 797, 801 (7th Cir. 2008) (emphasis added) (citations omitted).

The Seventh Circuit's characterization is in accord with Illinois law, which holds that "where there is a single overt act from which subsequent damages may flow, the statute begins to run on the date the defendant invaded the plaintiff's interest and inflicted injury, and this is so despite the continuing nature of the injury." Feltmeier v. Feltmeier, 207 Ill. 2d at 279.

Because Robertson's statutory rights were first invaded in 2010 (a single overt act), his claim began accruing in 2010 despite the continuing nature of his injury. Robertson's argument ignores the underlying rationale of the "continuing violation" doctrine. It is not the alleged fact that Defendants were in violation of or out of compliance with section 15 (b)'s requirements for the duration of Robertson's employment viewed as a whole which gives rise to the cause of action. Rather, it is Defendants' alleged failure to first obtain Robertson's written consent before collecting his biometric data which gives rise to the cause of action.

Applying the five year statute of limitation from the date when Defendants allegedly first violated Robertson's statutory rights (2010), the statute of limitations on Robertson's claim ran in 2015. Because Robertson did not first file his claim until April 20, 2018, his claim is time barred.

3. Section 14/15 (d) – Disclosure of biometric data without consent (Count III)

Section 15 (d) of BIPA provides:

(d) No private entity in possession of a biometric identifier or biometric information may disclose, redisclose, or otherwise disseminate a person's or a customer's biometric identifier or biometric information unless:

(1) the subject of the biometric identifier or biometric information or the subject's legally authorized representative consents to the disclosure or redisclosure;

* * * * *

740 ILCS 14/15 (d).

Here, this court erred in its application of the five year statute of limitations for the same reasons as above. See *supra*. Again, Robertson's statutory rights were first invaded in 2010, a single overt act. Thus, Robertson's claim began accruing in 2010, despite the continuing nature of the injury. Applying the five year statute of limitations, the statute of limitations on Robertson's claim ran in 2015. Because Robertson first filed his claim on April 20, 2018, Robertson's claim in Count III is time barred.

III. Conclusion

The court GRANTS IN PART and DENIES IN PART Defendants' motion for reconsideration.

The court grants Defendants' motion as to Counts II and III and dismisses those counts pursuant to 735 ILCS 5/2-619 (a)(5) as barred by the statute of limitations, with prejudice.

The court denies Defendants' motion as to Count I.

The status date of January 28, 2020 stands.

Entered: _____

_____

Judge Neil H. Cohen

STATE OF ILLINOIS
CIRCUIT COURT
SEVENTEENTH JUDICIAL CIRCUIT

DONNA R. HONZEL
Associate Judge

Winnebago County Courthouse
400 West State Street
Rockford, Illinois 61101
PHONE (815) 319-4804* FAX (815) 319-4809

March 12, 2020

David Fish
The Fish Law Firm, P.C.
200 East Fifth Ave., Ste.123
Naperville, IL 60563

Jeffrey R. Hoskins
Hinshaw & Culbertson LLP
151 North Franklin Street, Ste. 2500
Chicago, IL 60606

Marcia Smith vs. Top Die Casting Co.
2019-L-248

MEMORANDUM OF DECISION AND ORDER

Plaintiff has filed suit alleging defendant violated sections 15 (a) and (b) of the Biometric Information Privacy Act (BIPA), 740 ILCS 14/1 *et seq.* Defendant has filed a 2-619 Motion to Dismiss the complaint on the basis that defendant believes suit has been brought outside the statute of limitations. The matter has been fully briefed and argued. The court finds and orders as follows:

I. Violation of section 15(a)

740 ILCS 14/15 deals with "Retention; collection; disclosure; destruction" Section (a) states,

"A private entity in possession of biometric identifiers or biometric information must develop a written policy, made available to the public, establishing *a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied* **or within 3 years of the** individual's **last interaction with the private entity, whichever occurs first**. Absent a valid warrant or subpoena issued by a court of competent jurisdiction, a private entity in possession of biometric identifiers or biometric information must comply with its established retention schedule and destruction guidelines." (Emphasis added.)

The parties agree that the plaintiff began working for the defendant in August of 2017. It also appears without dispute that the plaintiff's last day on the job was February 28, 2019. Her assignment "officially" ended March 5, 2019. It also appears uncontroverted that when the

plaintiff began working for the defendant and defendant acquired her biometric information, there was no written policy in place for the retention and destruction of that data. Under the wording of the statute, and the use of the "or" connector, either there are written guidelines for permanently destroying the biometric information once the purpose for having it/using it have been satisfied or in the absence of written guidelines, destruction must take place within 3 years of the individual's last interaction with the entity. The latter applies here.

The United States Supreme Court has said, "a cause of action does not become 'complete and present' until the plaintiff can file suit and obtain relief." *Bay Area Laundry and Dry Cleaning Pension Trust Fund v Febar Corp. of California, Inc.*, 522 U.S. 192 at 193. In *Blair v Nevada Landing Partnership*, 369 Ill.App.3d 318, 323 our Second District Appellate Court stated, "Generally, in tort, a cause of action accrues and the limitations period begins to run when facts exist that authorize one party to maintain an action against another [citing *Feltmeier*, infra." At this point, only approximately 1 year after the plaintiff's last interaction with the defendant, the plaintiff's claim has not ripened as there is still a considerable time (at minimum until February 28, 2022), for the defendant to comply with the statute, regardless of what the statute of limitations is.

Defendant's motion to dismiss is granted as it pertains to paragraph 47 as well as any other paragraphs alleging a violation of section 15(a).

II. Violation of section 15(b)

740 ILCS 14/15(b) states, "No private entity may collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifier or biometric information, **unless it first**:

(1) informs the subject or the subject's legally authorized representative in writing that a biometric identifier or biometric information is being collected or stored;

(2) informs the subject or the subject's legally authorized representative in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; and

(3) receives a written release executed by the subject of the biometric identifier or biometric information or the subject's legally authorized representative."

The plain language of the statute indicates when a claim accrues for violating this section. The offense, and thus the cause of action for the offense, occurs the first time the biometric information is collected without meeting the requirements of paragraphs (1) – (3).

The Illinois Supreme Court has said, "At this juncture, we believe it important to note what does *not* constitute a continuing tort. A continuing violation or tort is occasioned by continuing unlawful acts and conduct, not by continual ill effects from an initial violation. See *Pavlik*, 326 Ill.App.3d at 745, 260 Ill.Dec. 331, 761 N.E.2d 175; *Bank of Ravenswood*, 307 Ill.App.3d at 167, 240 Ill.Dec. 385, 717 N.E.2d 478; *279 *Hyon*, 214 Ill.App.3d at 763, 158 Ill.Dec. 335, 574 N.E.2d 129. Thus, where there is a single overt act from which subsequent damages may flow, the statute begins to run on the date the defendant invaded the plaintiff's interest and inflicted injury, and this is so despite the continuing nature of the injury. See *Bank of Ravenswood*, 307 Ill.App.3d at 167–68, 240 Ill.Dec. 385, 717 N.E.2d 478; *Hyon*, 214 Ill.App.3d at 763, 158

Ill.Dec. 335, 574 N.E.2d 129; *Austin v. House of Vision, Inc.*, 101 Ill.App.2d 251, 255, 243 N.E.2d 297 (1968). For example, in *Bank of Ravenswood,* the appellate court rejected the plaintiffs' contention that the defendant city's construction of a subway tunnel under the plaintiff's property constituted a continuing trespass violation. The plaintiffs' cause of action arose at the time its interest was invaded, *i.e.*, during the period of the subway's construction, and the fact that the subway was present below ground would be a continual effect from the initial violation, but not a continual violation. *Feltmeier v Feltmeier*, 207 Ill.2d 263 at 278-279." (Emphasis in original) See also *Blair,* supra at 324 -325.

In this matter, it is undisputed that the plaintiff first began using the timeclock in question in August of 2017. Plaintiff's argument that each time the plaintiff clocked in constituted an independent and separate violation is not well taken. The biometric information is collected the one time, at the beginning of the plaintiff's employment, and thereafter the original print, or coordinates from the print, are used to verify the identity of the individual clocking in. Thus, the offending act is the initial collection of the print and at that time the cause of action accrues. To hold otherwise is contrary to the plain wording of the statute and common sense as to the manner the initially collected biometric information is utilized. Additionally, as a matter of public policy, 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) and had its employees clocking in at the start of the shift, out for lunch, in for the afternoon and out for the end of the shift. Over a period of 50 weeks (assuming a two week vacation) at $1000 for each violation it adds up to $1,000,000 *per employee* in a year's time. This would appear to be contrary to 14/5 (b) and (g) – Legislative findings; intent. It also appears to be contrary to how these time clocks purportedly work.

Given the violation occurs at the first instance of collection of biometric data that does not conform to the requirements set forth, the question becomes what the statute of limitations is given the Act's silence. Defendant argues that because BIPA clearly concerns matters of privacy as well as concerns itself with the dissemination of uniquely personal information and preventing that from occurring, the one year statute of limitations set forth in 13-201 applies, supporting its motion to dismiss.

The parties agree that the Illinois Supreme Court (in *Rosenbach v Six Flags Entm't Corp.* 2019 IL 123186) as well as other cases addressing BIPA have made it clear that BIPA involves an invasion of privacy but they disagree as to what that means. BIPA's structure is designed to prevent compromise of an individual's biometric data. Indeed, the common law right to privacy as it relates to modern technology is at the core of BIPA. The United States Supreme Court has noted that "both the common law and the literal understanding of privacy encompass the individual's control of information concerning his or her person." *U.S. Dep't of Justice v Reporters Comm.for Freedom of the Press*, 489 U.S. 749, 763. Defendant relies heavily on *Blair* and its application of 13-201's one year limitation period and the fact the Right of Publicity Act (765 ILCS 1075) involved in *Blair*, like BIPA, sets forth no statute of limitations period.

However, the Court noted in *Blair* that at common law there was a tort of appropriation of likeness, for which a plaintiff needed to set forth elements of appropriation of a person's name or likeness, without consent, done for another's commercial benefit. The statute of limitations for doing so was the one year statute set forth in 13-201. The Right to Publicity Act went into effect January 1, 1999 and completely replaced the common law tort. The legislature specifically

said it was meant to supplant the common-law. As such, the *Blair* court held the one year statute of limitations would remain applicable for the Act. BIPA is not an act which completely supplants a specific common law cause of action, so is distinguishable from the Right to Publicity Act in this regard. Additionally, *Blair* clearly involved publication as an essential element. That further distinguishes it from BIPA to the extent that publication is not a necessary element of every BIPA claim. Notably, the case at hand contains no allegation of publication.

The Second District's decision and language in *Benitez v KFC Nat. Management Co.*, 305 Ill.App.3d 1027 is informative. There, while the matter involved intrusion upon seclusion and the voyeuristic nature of the affront to privacy which is not present here, the court stated, at page 1034, "The fact that publication is not an element of intrusion upon seclusion is crucial, since the plain language of section 13-201 indicates that the one-year statute of limitations governs only libel, slander and privacy torts involving publication. (see 735 ILCS 5/13-201 (West 1994); *McDonald's Corp. v. Levine,* 108 Ill.App.3d, 737, 64 Ill.Dec. 224, 439 N.E.2d 475(1982) (even if eavesdropping claim was actually a claim for intrusion upon seclusion, the one-year statute of limitations of what is now section 13-201 would not apply...)). Accordingly, since the statute does not refer to a cause of action for intrusion upon seclusion, we decline to read the statute as such." The court went on to note two cases which disagreed with its decision and held that 13-201 applied to intrusion upon seclusion and sexual harassment cases. The court commented, at pages 1007-8, "Nonetheless, we are not persuaded by those cases, since neither case provides any explanation whatsoever of why section 13-201 applies to a cause of action for intrusion upon seclusion. Instead, we find the plain language of the statute controlling."

It is also noteworthy that inclusion upon seclusion is a relatively new, statutorily created violation of the right to privacy and it is an extension of the common law's four distinct types of privacy breaches. While BIPA claims are not claims which can be characterized as intrusion upon seclusion cases, BIPA also is a statutorily created violation of the right to privacy which extends common law privacy protections, as opposed to supplanting a common law right. For those reasons also, as well as the Second District's logic and analysis of 13-201 in *Benitez* (which this court must follow) 13-201 does not apply.

Therefore, for all the foregoing reasons, the court finds that section 5/13-205's Five year limitations period applies to BIPA violations. Given the lack of an express limitations period in the Act, and the finding 13-201 does not apply, BIPA falls into the category of "civil actions not otherwise provided for" and plaintiff has clearly brought her claim prior to August, 2022.

The defendant's motion to dismiss section (b) allegations of BIPA violations is denied.

So ordered:

Date: 3/12/2020

Enter: _____
Hon. Judge Donna Honzel

STATE OF ILLINOIS
IN THE CIRCUIT COURT OF THE 17TH JUDICIAL CIRCUIT
COUNTY OF WINNEBAGO

FILE STAMP

Marcia Smith
Plaintiff

Case No. 2019-L-248

Top Die Casting Co.
Defendant(s)

NOTICE OF FILING

PLEASE TAKE NOTICE that on March 12, 2020, the attached Memorandum of Decision and Order was filed by the Court.

CERTIFICATE OF SERVICE --- SERVICE LIST

Under penalties as provided by 735 ILCS 5/1-109, I state that I served this notice and the document referenced here to the persons listed below by the means specified.

Inean L. Ferris
Representative, Trial Court Administration

Party and address/email address	Method of Service (1st class, email, fax)
David Fish/ dfish@fishlawfirm.com	Email
Jeffrey J. Hoskins/ jhoskins@hinshawlaw.com	Email

17th Circuit Court - Trial Court Administration
Winnebago County Courthouse
400 West State Street, Room 215
Rockford, Illinois 61101

IN THE CIRCUIT COURT OF COOK COUNTY, ILLINOIS
COUNTY DEPARTMENT, CHANCERY DIVISION

THOMAS ROBERTSON, individually, and on behalf of all others similarly situated,	)	
Plaintiff,	)	
v.	)	**Case No. 18-CH-5194**
HOSTMARK HOSPITALITY GROUP, INC., et al,	)	
Defendants,	)	

MEMORANDUM AND ORDER

Plaintiff Thomas Robertson has filed a motion to reconsider this court's January 27, 2020 Memorandum and Order pursuant to 735 ILCS 5/2-1203(a).

I. Background

On April 20, 2018, Plaintiff Thomas Robertson ("Robertson") filed his original complaint alleging Defendants Hostmark Hospitality Group, Inc. ("Hostmark") and Raintree Enterprises Mart Plaza, Inc. ("Raintree") (collectively "Defendants") violated the Biometric Information Privacy Act ("BIPA").

On April 1, 2019, this court granted Robertson's motion for leave to file an amended class action complaint (the "Amended Complaint"). The Amended Complaint now alleges three counts, each alleging a violation of a different subsection of section 15 of BIPA. 740 ILCS 14/15.

Count I alleges a violation of subsection 15(a) based upon Defendants failure to institute, maintain, and adhere to a publicly available retention and deletion schedule for biometric data. 740 ILCS 14/15(a). Count II alleges a violation of subsection 15(b) based upon Defendants failure to obtain written consent prior to collecting and releasing biometric data. 740 ILCS 14/15(b). Count III alleges a violation of subsection 15(d) based upon Defendants failure to obtain consent before disclosing biometric data. 740 ILCS 14/15(d).

On July 31, 2019, this court issued its Memorandum and Order denying Defendants' motion to dismiss Robertson's Amended Complaint. In summary, this court held that: (1) Robertson's claim was not preempted by the Illinois Worker's Compensation Act; (2) the applicable statute of limitations was five years, as provided for in 735 ILCS 5/13-205; and (3) Robertson had adequately pled his claim.

As part of the court's July 31, 2019 ruling, this court addressed the parties' arguments regarding the date Defendants stopped collecting Robertson's biometric information but did not address their arguments regarding when Robertson's claims accrued.

On August 30, 2019, Defendants filed their motion to reconsider and certify questions to the appellate court. In their motion to reconsider, Defendants argued, *inter alia*, that this court erred in applying a five-year statute of limitations to Robertson's claim. On September 4, 2019, this court denied Defendants' motion, in part, but allowed further briefing on the issue of the application of the five-year statute of limitation.

On January 27, 2020, this court issued its Memorandum and Order granting in part and denying in part Defendants' motion to reconsider. The court held that Robertson's claims relating to Defendants' alleged violations of section 15(b) and 15(d) accrued in 2010. The court found that the continuing violation rule did not apply to Robertson's claims because the violations of sections 15(b) and 15(d) represented a single discrete act from which any damages flowed. Thus, it was held that Counts II and III were barred by the five statute of limitations.

Regarding Count I, the court viewed section 15(a) as imposing two distinct requirements: (1) requiring private entities to develop a publicly available retention schedule and deletion guidelines; and (2) requiring the permanent deletion of an individual's biometric data, either in accordance with the deletion guidelines or within 3 years of the individual's last interaction with the private entity, whichever is earlier.

The court held that since it was Defendants' stated position that they ceased collection of biometric data in 2013, the math dictated by section 15(a) results in the conclusion that Robertson's claim could not have started to accrue until, at the earliest, 2016. Accordingly, Robertson's claim was not barred by the five-year statute of limitations.

II. Motion to Reconsider

A. *Application of the Continuing Violation Rule*

"The intended purpose of a motion to reconsider is to bring to the court's attention newly discovered evidence, changes in the law, or errors in the court's previous application of existing law." Chelkova v. Southland Corp., 331 Ill. App. 3d 716, 729-30 (1st Dist. 2002). A party may not raise a new legal or factual argument in a motion to reconsider. North River Ins. Co. v. Grinnell Mut. Reinsurance Co., 369 Ill. App. 3d 563, 572 (1st Dist. 2006).

Robertson's current Motion to Reconsider of this court's January 27, 2020 Memorandum and Order reiterates his previously stated position that his claim is well within the statute of limitations because he was a victim of a continuing violation of his rights under BIPA. Alternatively, he seeks to certify the question to the First District pursuant to Illinois Supreme Court Rule 304(a). [1]

---

[1] Not surprisingly, Defendants argue this court properly applied the law surrounding continuing violations to Robertson's BIPA claims. Alternatively, Defendants suggest that if the question is to be certified it should be pursuant to Illinois Supreme Court Rule 308.

Robertson's most recent request suggests that the proper application of the continuing violation rule is illustrated by Cunningham v. Huffman, 154 Ill. 2d 398, 406 (1993).

Cunningham involved a matter of first impression, namely, "whether the Illinois four-year statute of repose is tolled until the date of last treatment when there is an ongoing patient/physician relationship." Cunningham v. Huffman, 154 Ill. 2d 398, 400 (1993). The trial court found that the plaintiff's claims were time-barred and the continuous course of treatment doctrine was not the law in Illinois. Id. at 401. The Appellate Court affirmed the dismissal stating that "in medical malpractice actions, the statute of repose is triggered only on the last day of treatment, and if the treatment is for the same condition, there is no requirement that the negligence be continuous throughout the treatment. Id. at 403.

The Illinois Supreme Court declined to adopt the continuous course of treatment doctrine. Id. at 403-04. Nonetheless, the court held that statutory scheme did not necessarily preclude the cause of action asserted by the plaintiff. Id. at 404. Specifically, the court held that the medical treatment statue of repose would not bar the plaintiff's action if he could demonstrate: (1) that there was a continuous and unbroken course of *negligent* treatment, and (2) that the treatment was so related as to constitute one continuing wrong." Id. at 406 (emphasis in original). The Illinois Supreme Court emphasized "that there must be a continuous course of *negligent* treatment as opposed to a mere continuous course of treatment." Id. at 407 (emphasis in original).

Robertson's assertion is that Cunningham stands for the proposition that "the continuing violation doctrine applies where a plaintiff demonstrates a continuous and unbroken course of conduct, so related as to constitute one continuous wrong." (Motion at 5).

But the Illinois Supreme Court has explicitly rejected Robertson's argument, stating **"[t]he Cunningham opinion did not adopt a continuing violation rule of general applicability in all tort cases or, as here, cases involving a statutory cause of action.** Rather, the result in Cunningham was based on interpretation of the language contained in the medical malpractice statute of repose." Belleville Toyota v. Toyota Motor Sales, U.S.A., 199 Ill. 2d 325, 347 (2002)(Fitzgerald, J)(emphasis ours).

Robertson ignores Belleville and replies that "[t]here is no binding authority to which the Court may turn for guidance on the exact issue regarding whether the continuing violation doctrine applies." (Reply at 4).

While Justice Fitzgerald's written opinion in Belleville is pretty solid authority to the contrary, as this court previously pointed out, the First District has considered "[w]hether a series of conversions of negotiable instruments over time can constitute a continuing violation under Belleville Toyota, Inc. v. Toyota Motor Sales, U.S.A., Inc., 199 Ill. 2d 325 (2002), for the purpose of determining when the statute of limitations runs." Kidney Cancer Assoc. V. North Shore Com. Bank, 373 Ill.App.3d 396, 397-98 (1st Dist. 2007). The court reasoned that where a complaint alleges a serial conversion of negotiable instruments by a defendant, it cannot be denied that a single unauthorized deposit of a check in an account opened by the defendant gives the plaintiff a right to file a conversion action. Id. at 405. The court rejected the plaintiff's claim

that the defendant's repeated deposits (identical conversions) following the initial deposit served to toll the statute of limitations under the continuing violation rule. Id. Instead, according to the court, each discrete act (deposit) provided a basis for a cause of action and the court need not look to the defendant's conduct as a continuous whole for prescriptive purposes. Id.

In Rosenbach v. Six Flags Entertainment Corp., 2019 IL 123186, ¶ 33, the Illinois Supreme Court held when a private entity fails to comply with one of section 15's requirements, that violation is itself sufficient to support the individual's or customer's **statutory cause of action**. Id. (emphasis ours).

Robertson's Amended Complaint alleges that his statutory rights were invaded in 2010, when Defendants allegedly first collected and disseminated his biometric data without complying with section 15's requirements. (Amended Complaint at ¶42).

In our January 27, 2020 Memorandum and Order, this court explained that under the general rule a cause of action for a statutory violation accrues at the time a plaintiff's interest is invaded. Blair v. Nevada Landing Partnership, 369 Ill. App. 3d 318, 323 (2nd Dist. 2006) (citing Feltmeier v. Feltmeier, 207 Ill. 2d 263, 278-279 (2003)("where there is a single overt act from which subsequent damages may flow, the statute begins to run on the date the defendant invaded the plaintiff's interest and inflicted injury, and this is so despite the continuing nature of the injury." Id, 207 Ill. 2d at 279); see also, Limestone Development Corp. v. Village of Lemont, 520 F.3d 797, 801 (7th Cir. 2008) ("The office of the misnamed doctrine is to allow suit to be delayed until a series of wrongful acts blossoms into an injury on which suit can be brought. [citations]. It is thus a doctrine not about a continuing, but about a cumulative, violation.").

Here, this court respectfully disagrees with Robertson concerning the application of continuing violation rule. It was Defendants' alleged failure to first obtain Robertson's written consent before collecting his biometric data which is the essence of and gave rise to the cause of action, not their continuing failure to do so. Robertson's statutory rights were violated in 2010 when Defendants allegedly first collected and disseminated his biometric data without complying with section 15's requirements.

Per Feltmeier, "where there is a single overt act from which subsequent damages may flow, the statute begins to run on the date the defendant invaded the plaintiff's interest and inflicted injury, and this is so despite the continuing nature of the injury." Id., 207 Ill. 2d at 279. That Defendants lacked the written release to collect and consent to disseminate Robertson's biometric data from 2010 until they ceased collection, does not change the fact Robertson's statutory rights were violated in 2010 nor does it serve to delay or toll the statute of limitations. Id; see also, Bank of Ravenswood v. City of Chicago, 307 Ill. App. 3d 161, 168 (1st Dist. 1999) (holding that the action for trespass began accruing when the defendant invaded plaintiff's interest and the fact that subway was present below the ground was a continual ill effect from the initial violation but not a continual violation.).

The court did not err in holding that the continuing violation rule did not apply to Robertson's claims.

B. *Single vs. Multiple Violations*

Robertson argues that this court erred in holding that his claims for violation of sections 15 (b) and (d) amount to single violations which occurred in 2010. Instead, according to Robertson, each time Defendants collected or disseminated his biometric data without a written release constitutes a single actionable violation.

Robertson's argument is contrary to the unambiguous language of the statute and taken to its logical conclusion would inexorably lead to an absurd result.

* * *

Section 10 of BIPA defines "written release" as: "[. . .] informed written consent or, *in the context of employment, a release executed by an employee as a condition of employment*." 740 ILCS 14/10 (emphasis added).

And, Section 15 (b)(3) of BIPA provides:

> (b) No private entity may collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifier or biometric information, unless it first: *** (3) receives a written release executed by the subject of the biometric identifier or biometric information or the subject's legally authorized representative.

740 ILCS 14/15 (b)(3).

Reading section 10 and 15 of BIPA together makes clear that the "written release" contemplated by section 15 (b)(3) in the context of employment is to be executed as a condition of employment. 740 ILCS 14/10 and 15(b)(3).

As explained by the court in its January 27, 2020 Memorandum and Order, "[t]he most reasonable and practical reading of section 15 (b) requires an employer to obtain a single written release as a condition of employment from an employee or his or her legally authorized representative to allow the collection of his or her biometric data for timekeeping purposes for the duration of his or her employment. Such a release need not be executed before every instance an employee clocks-in and out, rather a single release should suffice to allow the collection of an employee's biometric data." January 27, 2020 Memorandum and Order at 4.

Robertson admits that this is a reasonable reading, (Motion at 7), but argues that Defendants, having failed to obtain a written release or his consent, had to obtain his written release before collecting his biometric data. Since Defendants failed to do, Robertson argues, each time Defendants' collected Robertson's biometric is independently actionable.

But, taken to its logical conclusion Robertson's construction would lead employers to potentially face ruinous liability.

Section 20 of BIPA provides any individual aggrieved by a violation of BIPA with a right of action and further provides that said individual may recover liquidated statutory damages for

each violation in the amount of either $1,000 for negligent violations or $5,000 for intentional or reckless violations. 740 ILCS 14/20.

Robertson alleges that he was required to scan his fingerprints each time he clocked in and out. (Amended Complaint at ¶44). Therefore, at minimum, there exists at least two potentially recoverable violations for *each day* Robertson worked. Extending this to its logical conclusion, a plaintiff like Robertson could potentially seek a total of $500,000 for negligent violations or $2,500,000 for intentional or reckless violations *for each year*[2] Defendants allegedly violated BIPA.

It is a well-settled legal principle that statutes should not be construed to reach absurd or impracticable results, Nowak v. City of Country Club Hills, 2011 IL 111838, ¶ 21, which is where Robertson's argument would take us. This court finds nothing in the statute as it is written or as it was enacted to indicate it was the considered intent of legislature in passing BIPA to impose fines so extreme as to threaten the existence of any business, regardless of its size.

C. *Section 15 (d)(1) – Consent for Dissemination*

Section 15 (d)(1) of BIPA provides:

> (d) No private entity in possession of a biometric identifier or biometric information may disclose, redisclose, or otherwise disseminate a person's or a customer's biometric identifier or biometric information unless:
>
> (1) the subject of the biometric identifier or biometric information or the subject's legally authorized representative consents to the disclosure or redisclosure;
>
> * * * * *

740 ILCS 14/15 (d)(1).

Robertson's main contention here is that: (1) he never alleged when Defendants actually disseminated his biometric data; and (2) a defendant can potentially violate section 15(d) multiple times by disseminating an individual's biometric to additional third-parties.

But this court did not rule that section 15(d)(1) can only be violated a single time by a defendant. Rather, it ruled that based on the allegations as pled, Robertson's claim accrued in 2010.

The court recognizes that "a plaintiff is not required to plead facts with precision when the information needed to plead those facts is within the knowledge and control of defendant rather than plaintiff." Lozman v. Putnam, 328 Ill. App. 3d 761, 769-70 (1st Dist. 2002). However, even under this standard a plaintiff may not simply plead the elements of a claim, Holton v. Resurrection Hospital, 88 Ill. App. 3d 655, 658 (1st Dist. 1980), nor does this rule excuse a plaintiff from alleging sufficient facts. Holton, 88 Ill. App. 3d at 658-59.

[2] Two violations a day multiplied five days multiplied fifty weeks a year multiplied either 1,000 or 5,000.

If Robertson was actually trying to allege that Defendants violated section 15(d)(1) multiple times by disseminating his biometric data to multiple third parties on many occasions between 2010 and whenever Defendants ceased collection, this allegation is not well-pled and Robertson has not stated a claim for this factual scenario. To be sure, Robertson's Amended Complaint plainly alleges that any dissemination occurred systematically and automatically, but Robertson does not allege any underlying facts which support this assertion.

Robertson also argues that it is possible for a private entity to violate section 15(d) multiple times and that therefore the court erred in holding that Defendants violated Robertson's section 15(d)(1) statutory rights only in 2010. ("Defendants, at any point in time, could have disseminated [his] biometric data to any number of other entities, any number of times, over any period of time," (Motion at 13)).

Robertson alleges Defendants "disclose or disclosed [his] fingerprint data to at least one out-of-state third-party vendor, and likely others," (Id. at ¶33), but the allegation relating to "likely others" is not well pled. The Amended Complaint contains no allegations alleging Defendants disseminated Robertson's biometric data to additional third parties at some undetermined point between 2010 and the date Defendants ceased collection.

The Amended Complaint plainly alleges that any disseminations were, on information and belief, done "systematically or automatically." (Id. at ¶¶ 33, 97). "[A]an allegation made on information and belief is not equivalent to an allegation of relevant fact [citation]." Golly v. Eastman (In re Estate of DiMatteo), 2013 IL App (1st) 122948, ¶ 83 (citation omitted).

Without alleging the supporting underlying facts which lead Robertson to believe that his biometric data was being systemically and automatically disseminated, his allegation regarding additional dissemination to additional third parties remains an unsupported conclusion. The same is true for the allegations Robertson pleads on information and belief. Defendants are not required to admit unsupported conclusions on a motion dismiss.

The court did not err.

III. Motions to Certify Questions and/or Motions Leave to Appeal

Robertson seeks leave to immediately appeal this court's orders pursuant to Illinois Supreme Court Rule 304(a). Defendants assert that Illinois Supreme Court Rule 308 is the better procedural vehicle and seeks certification of three questions:

1. Whether exclusivity provisions of the Illinois Worker's Compensation Act bar BIPA claims?

2. Whether BIPA claims are subject to the one-year statute of limitations pursuant to 735 ILCS 5/13-201 or the two-year statute of limitations pursuant to 735 ILCS 5/13-202?

3. Whether a claim for a violation of section 15(a) accrues when a private entity first comes into possession of biometric data?

The questions Defendants seek to certify have been either directly addressed or are closely related to questions other judges have certified.

Judge Raymond W. Mittchell in McDonald v. Symphony Bronzeville Park, LLC, Case No. 17 CH 11311 has already certified a similar question to Defendants' first question in an appeal is pending under Marquita McDonald v. Symphony Bronzeville Park, LLC, No. 1-19-2398.

Similarly, in Juan Cortez v. Headly Manufacturing Co., Case No. 19 CH 4935, Judge Anna H. Demacopoulos has certified the second question concerning of what statute of limitations appropriately applies BIPA claims. This court is informed that the First District has accepted the matter and it is currently being briefed.

The third proposed question – as to whether a violation of section 15(a) begins accruing when a private entity first comes into possession of biometric data – is not yet pending on appeal.

A. Rule 308?

Rule 308(a) provides as follows:

> When the trial court, in making an interlocutory order not otherwise appealable, finds that the order involves a question of law as to which there is substantial ground for difference of opinion and that an immediate appeal from the order may materially advance the ultimate termination of the litigation, the court shall so state in writing, identifying the question of law involved.

ILL. SUP. CT., R. 308(a).

Rule 308(a) "should be strictly construed and sparingly exercised." Kincaid v. Smith, 252 Ill. App. 3d 618, 622 (1st Dist. 1993). "Appeals under this rule should be available only in the exceptional case where there are compelling reasons for rendering an early determination of a critical question of law and where a determination of the issue would materially advance the litigation." Id.

Because Rule 308 should be strictly construed and sparingly exercised, the court will not certify a question already accepted by the Appellate Court. Accordingly, in the interests of efficiency and of not burdening the First District with issue in cases which echo one another, the court declines to certify questions regarding the applicability of the Illinois Worker's Compensation Act, or questions concerning the appropriate statute of limitations under BIPA. Answers to those questions should be forthcoming through the certifications by Judges Mitchell and Demacopoulos.

Regarding the third question concerning the accrual of section 15(a) claims, the court is willing to certify a question regarding section 15(a) but is not willing to certify the question as currently phrased by Defendants.

As explained by the court in its January 27, 2020 Memorandum and Order, section 15(a) contains two distinct requirements: (1) private entities in possession of biometric data must develop a publicly available retention schedule and deletion guidelines; and (2) those guidelines

must provide for the permanent destruction of biometric data when the initial purpose for collecting the biometric data has been satisfied or within 3 years of the individual's last interaction with the private entity, whichever occurs first.

Contrary to Defendants' phrasing of their question regarding section 15(a), the court did not rule that a section 15(a) violation could only accrue once. Rather the court interpreted section 15(a) as imposing two distinct requirements on private entities each with separate accrual dates. The pure legal question is not simply when does the action for a violation of section 15(a) accrue but rather whether the court's interpretation of the statutory language of section 15(a) is correct.

Defendants motion is therefore denied, as written. If they wish, Defendants may resubmit the request to reflect this court's ruling and it will be reconsidered.

B. Rule 304(a)?

Rule 304(a) provides as follows:

> If multiple parties or multiple claims for relief are involved in an action, an appeal may be taken from a final judgment as to one or more but fewer than all of the parties or claims only if the trial court has made an express written finding that there is no just reason for delaying either enforcement or appeal or both.

ILL. SUP. CT., R. 304(a).

Rule 304(a) creates "an exception to [the] general rule of appellate procedural law by permitting appeals from trial court orders that only dispose of a portion of the controversy between parties." Mostardi-Platt Associates, Inc. v. American Toxic Disposal, Inc., 182 Ill. App. 3d 17, 19 (1st Dist. 1989). Rule 304(a)'s exception "arises when a trial judge [. . .] makes an express finding that there is no just reason to delay the enforcement or appeal of the otherwise nonfinal order." Id.

Here, the court did issue a final judgment as to fewer than all of the claims on January 27, 2020 when it granted Defendants' motion to reconsider and dismissed Counts II and III of Robertson's Amended Complaint with prejudice because they were barred by the applicable statute of limitations.

However, as explained many issues Robertson would seek review of under Rule 304(a) will be disposed of by the Appellate Court's answers to Judge Demacopoulos' certified question. Therefore, the court declines to make the necessary finding to allow Robertson to appeal pursuant to Rule 304(a).

III. Conclusion

Robertson's motion for reconsideration is DENIED.

Robertson's request for a Rule 304(a) finding is DENIED.

Defendants' request for to certify questions pursuant to Rule 308(a) is GRANTED IN PART and DENIED IN PART. The court denies Defendants' questions relating to the application of the Illinois Worker's Compensation Act and the two-year statute of limitations.

The court grants Defendants' request in so far as it seeks to certify a question relating to section 15(a) but denies Defendants' question as currently written.

The court orders the parties to confer and to attempt to reach an agreement regarding the phrasing of a question relating to the section 15(a).

The court set the next status date for this matter as June 16, 2020 at 9:30 a.m.

Entered: 5-29-20

Judge Neil H. Cohen #702

IN THE CIRCUIT COURT OF COOK COUNTY, ILLINOIS
COUNTY DEPARTMENT, CHANCERY DIVISION
GENERAL CHANCERY SECTION

BRANDON WATSON, individually and on behalf of all others similarly situated, Plaintiff, v. LEGACY HEALTHCARE FINANCIAL SERVICES, LLC d/b/a Legacy Healthcare; LINCOLN PARK SKILLED NURSING FACILITY, LLC d/b/a Warren Barr Lincoln Park a/k/a The Grove at Lincoln Park; and SOUTH LOOP SKILLED NURSING FACILITY, LLC d/b/a Warren Barr South Loop, Defendants.	CASE NO. 19 CH 3425 CALENDAR 11

ORDER

This matter came before the Court on Defendants' 2-619 motion to dismiss the putative Class Action Complaint of Plaintiff Brandon Watson. For the reasons explained below, the motion is granted.

BACKGROUND

Plaintiff was required to scan his hand to clock in and out of work at Defendants' nursing home facilities in Chicago.[1] Plaintiff worked as a Certified Nursing Assistant for Defendant Legacy Healthcare Financial Services, LLC ("Legacy"), which controls 26 nursing home facilities in Illinois. He worked at Defendant Lincoln Park Skilled Nursing Facility, LLC from December of 2012 through February of 2019, and at Defendant South Loop Skilled Nursing Facility, LLC from May through November of 2017.

Plaintiff filed his one-count Class Action Complaint on March 15, 2019, alleging that Defendants failed to properly disclose and obtain releases related to the collection, storage, and use of his biometric information, in violation of the Illinois Biometric Information Privacy Act ("BIPA"). He asks for statutory damages and an injunction under BIPA, individually and on behalf of a class of similarly-situated employees.

[1] The facts recited here are based upon the allegations of Plaintiff's Complaint, which are taken as true for purposes of this motion.

Defendants move to dismiss the Complaint under Section 2-619 of the Illinois Code of Civil Procedure, arguing that (1) Plaintiff's claims are time-barred; (2) Plaintiff's claims are preempted by the Illinois Workers Compensation Act; and (3) Plaintiff's claims are preempted by Section 301 of the Labor Management Relations Act.

APPLICABLE LAW

The purpose of a section 2-619 motion to dismiss is to dispose of issues of law and easily proved issues of fact at the outset of litigation. *Van Meter v. Darien Park Dist.*, 207 Ill. 2d 359, 367 (2003). Section 2-619(a)(5) provides for dismissal of a claim that "was not commenced within the time limited by law." Dismissal of a complaint pursuant to section 2-619(a)(9) is permitted where "the claim asserted against defendant is barred by other affirmative matter avoiding the legal effect of or defeating the claim." *Id.* The affirmative matter must negate the cause of action completely. *Id.* The trial court must interpret all pleadings and supporting documents in the light most favorable to the nonmoving party, and grant the motion only if the plaintiff can prove no set of facts that would support a cause of action. *In re Chicago Flood Litigation*, 176 Ill. 2d 179, 189 (1997).

ANALYSIS

(1) Statute of Limitations

Defendants argue that Plaintiff's claim is barred by the statute of limitations. BIPA does not contain its own statute of limitations, so Defendants contend that the claim should be governed by the one-year statute applicable to what it calls the "most analogous common law claim"—invasion-of-privacy claims. That statute provides:

> Actions for slander, libel or for publication of matter violating the right of privacy, shall be commenced within one year next after the cause of action accrued.

735 ILCS 5/13-201.

This is not the applicable statute of limitations. BIPA's Section 15(d) could be construed to address "publication of matter violating the right of privacy" in prohibiting private entities from "disclos[ing], redisclos[ing], or otherwise disseminat[ing] a person's or a customer's biometric identifier or biometric information . . . ." 740 ILCS 14/15(d). However, in this case Plaintiff did not include a claim under Section 15(d). Rather, he claimed violations only of Sections 15(a) and (b), which require private entities to publicly provide retention schedules and guidelines for permanently destroying biometric information, and to make disclosures and obtain releases before collecting, storing, and using that information. Sections (a) and (b) are violated even if there is no publication. Therefore, the one-year statute does not apply.

Nor does the two-year statute of limitations for a "statutory penalty" (735 ILCS 5/13-202) apply to this case. BIPA's liquidated damages provision is remedial, not penal. In *Rosenbach v. Six Flags Entertainment Corp.*, the Illinois Supreme Court explained that the General Assembly enacted BIPA "to try to head off such problems before they occur," by enacting safeguards and "by subjecting private entities who fail to follow the statute's

requirements to substantial potential liability, including liquidated damages . . . ." 2019 IL 123186, ¶ 36. Like the Telephone Consumer Protection Act at issue in *Standard Mutual Ins. Co. v. Lay*, BIPA was "designed to grant remedies for the protection of rights, introduce regulation conducive to the public good, or cure public evils." 2013 IL 114617, ¶ 31.

The applicable statute of limitations is the five-year "catch-all" provision of 735 ILCS 5/13-205. It begins to run on the date the cause of action accrued. Defendants argue that, even if the five-year statute applies, Plaintiff's claim is time-barred because his cause of action accrued when Defendant scanned Plaintiff's hand on his *first* day of work—December 27, 2012. This suit was filed on March 15, 2019, more than six years later.

Plaintiff argues that each daily scan of his hand violated BIPA, so his *last* day of work—February 21, 2019—is the key date for limitations purposes. He argues that all scans in the five years before he filed the Complaint are actionable.

Generally, a cause of action accrues "when facts exist that authorize one party to maintain an action against another." *Feltmeier v. Feltmeier*, 207 Ill. 2d 263, 278 (2003). Plaintiff argues that his claims are most analogous to wage claims, where each inadequate paycheck gives rise to a separate cause of action. The same cannot be said for each of Plaintiff's hand scans. As the Court in *Feltmeier* stated:

> [W]here there is a single overt act from which subsequent damages may flow, the statute begins to run on the date the defendant invaded the plaintiff's interest and inflicted injury, and this is so despite the continuing nature of the injury.

Id. at 79. (emphasis added).

In wage claims, damages flow from each inadequate paycheck. Additional damages accrue every time a paycheck is short. By contrast, Plaintiff's damages flow from the "single overt act" of the initial collection and storage of his biometric data. According to the Complaint, "From the start of Plaintiff's employment with Defendants in 2012," Defendants required him to have his "fingerprint and/or handprint collected and/or captured so that Defendants could store it and use it moving forward as an authentication method." (Cplt ¶18). The Complaint alleges that, *before* collecting Plaintiff's biometric information, Defendants did not provide Plaintiff with the required written notices and did not get his required consent. (Cplt ¶¶ 22, 23). While the Complaint alleges that Plaintiff had to scan his hand every day he worked, all his damages flowed from that initial act of collecting and storing Plaintiff's handprint in Defendants' computer system without first complying with the statute. Plaintiff's handprint was scanned and stored in Defendants' system on Day 1, allowing for authentication every time he signed in.

Plaintiff's cause of action accrued when his handprint allegedly was collected in violation of BIPA on his first day of work on December 27, 2012. Therefore, because Plaintiff filed his case on March 15, 2019, Plaintiff's claim is time-barred under the five-year statute of limitations.

This holding disposes of the case, but the Court will address Defendants' other arguments for the record.

(2) Preemption by Workers Compensation Act

Defendant argues that Plaintiff's claims are preempted by the exclusive remedy provisions of the Illinois Workers Compensation Act (the "Act"), 820 ILCS 305/5(a) and 11.

The Act "generally provides the exclusive means by which an employee can recover against an employer for a work related injury." *Folta v. Ferro Eng'g*, 2015 IL 118070, ¶ 14. However, the employee can escape the Act's exclusivity provisions by establishing that the injury "(1) was not accidental; (2) did not arise from his [or her] employment; (3) was not received during the course of employment; or (4) was not compensable under the Act." *Id.*

Defendant argues that none of these exceptions apply in this case. In response, Plaintiff argues that exceptions (1) and (4) both apply—that the BIPA violations were not accidental and were not compensable under the Act.

To show that an injury was not accidental, "the employee must establish that his employer or co-employee acted deliberately and with specific intent to injure the employee." *Garland v. Morgan Stanley & Co.*, 2013 IL App (1st) 112121, ¶ 29. Plaintiff has made no such allegation in his Complaint, so he has not established that the injury was not accidental. To put it another way, the Complaint leaves open the possibility that the injury *was* accidental. Plaintiff implicitly acknowledges this when he alleges that he and the members of the class are entitled to recover "anywhere from $1,000 to $5,000 in statutory damages." (Cplt ¶ 57). Statutory damages of $1,000 may be recovered for *negligent* violations of BIPA (740 ILCS 14/20(1)), and caselaw has equated "negligent" with "accidental" under the Act. *See Senesac v. Employer's Vocational Res.*, 324 Ill. App. 3d 380, 392 (1st Dist. 2001).

Plaintiff also argues that exception (4) applies—the injury was not compensable under the Act. In *Folta,* the Illinois Supreme Court addressed how courts should analyze this exception.[2] Rejecting the argument that the plaintiff's mesothelioma was not compensable under the Act because recovery in his situation was barred by a statute of repose, the court focused on the *type of injury* alleged and whether the legislature intended such injuries to be within the scope of the Act. The court stated, "[W]hether an injury is compensable is related to whether the type of injury categorically fits within the purview of the Act." *Id.* at ¶ 23. Because the Act specifically addressed diseases caused by asbestos exposure (such as mesothelioma), the court found that the legislature contemplated that this type of disease would be within the scope of the Act, and it was therefore compensable under the Act. *Id.* at ¶¶ 25, 36.

The same cannot be said for injuries sustained from violations of BIPA. As the court stated in *Liu v. Four Seasons Hotel, Ltd.*, 2019 IL App (1st) 182645, ¶ 30, BIPA "is a privacy rights law that applies inside and outside the workplace." By including in BIPA a provision for a private right of action in state or federal court (740 ILCS 14/20), the legislature showed it did not contemplate that BIPA claims would categorically fit within the purview of the Workers Compensation Act. Moreover, BIPA's definition of "written release" refers specifically to

[2] *Folta* was decided under both the Workers Compensation Act and the Workers' Occupational Diseases Act, 820 ILCS 310/5(a) and 11, which contain analogous exclusivity provisions.

releases executed by an employee as a condition of employment, further evidence that the legislature did not intend the Workers Compensation Act to preempt BIPA actions in the employment context. 740 ILCS 14/10.

The court holds that BIPA claims are not compensable under the Act. Therefore, BIPA claims fall within the fourth exception to the Act's exclusivity provisions. Plaintiff's BIPA claims are not preempted by the Act.

(3) Preemption by § 301 of Labor Management Relations Act

Finally, Defendant argues that this case should be dismissed because Section 301 of the Labor Management Relations Act (29 U.S.C. §185(a)) preempts Plaintiff's BIPA claim. That section provides:

> (a) Venue, amount, and citizenship. Suits for violation of contracts between an employer and a labor organization representing employees in an industry affecting commerce as defined in this Act, or between any such labor organizations, may be brought in any district court of the United States having jurisdiction of the parties, without respect to the amount in controversy or without regard to the citizenship of the parties.

In analyzing this provision, the U.S. Supreme Court stated:

> [I]f the resolution of a state-law claim depends upon the meaning of a collective-bargaining agreement, the application of state law (which might lead to inconsistent results since there could be as many state-law principles as there are States) is pre-empted and federal labor-law principles—necessarily uniform throughout the Nation—must be employed to resolve the dispute.

Lingle v. Norge Div. of Magic Chef, 486 U.S. 399, 405-06 (1988).

In Illinois, the First District Appellate Court explained the analysis as follows:

> Where a matter is purely a question of state law and is entirely independent of any understanding of the terms of a collective bargaining agreement, it may proceed as a state-law claim. By contrast, where the resolution of a state-law claim depends on an interpretation of the collective bargaining agreement, the claim will be preempted. Where claims are predicated on rights addressed by a collective bargaining agreement, and depend on the meaning of, or require interpretation of its terms, an action brought pursuant to state law will be preempted by federal labor laws. Defenses, as well as claims, must be considered in determining whether resolution of a state-law claim requires construing of the relevant collective bargaining agreement.

Gelb v. Air Con Refrigeration & Heating, Inc., 356 Ill. App. 3d 686, 692-93 (1st Dist. 2005) (internal citations omitted).

With their motion, Defendants submitted sworn declarations attaching copies of the collective bargaining agreements ("CBAs") in effect at the Lincoln Park and South Loop nursing facilities where Plaintiff worked. The Lincoln Park CBA with SEIU provided, in relevant part:[3]

> Management of the Home, the control of the premises and the direction of the working force are vested exclusively in the Employer subject to the provisions of this Agreement. The right to manage includes . . . to determine and change starting times, quitting times and shifts, and the number of hours to be worked . . . to determine or change the methods and means by which its operations ought to be carried on; to set reasonable work standards . . . .

(Dfts' Mot., Choi Dec., Exh. A, p. 7).

The South Loop CBA with Local 743 in effect when Plaintiff worked at the South Loop facility in 2017 provided, in relevant part:

> [South Loop] has, retains, and shall continue to possess and exercise all management rights, functions, powers, privileges and authority inherent in the right to manage includ[ing] . . . the right to determine and change schedules, starting times, quitting times, and shifts, and the number of hours to be worked . . . to determine, modify, and enforce reasonable work standards, rules of conduct and regulation (including reasonable rules regarding . . . attendance, and employee honesty and integrity) . . . .

(Dfts' Mot., James Dec., Exh. A, p. 5).

Under *Lingle* and *Gelb*, the question is whether resolution of the BIPA claim in this case depends on an interpretation of the CBAs quoted above. Defendants argue that Plaintiff's claim "cannot possibly be resolved" without interpreting the governing CBAs. The Court disagrees. Resolution of this case is purely a question of state law—whether or not Defendants complied with BIPA by making the required written disclosures and getting the required written release before collecting, storing, and using Plaintiff's biometric information. Even if the CBAs allowed Defendants to set a rule requiring Plaintiff to clock in with his handprint—as part of "determining reasonable work standards"—the Court does not need to interpret the CBAs to decide if Defendants complied with BIPA's requirements. This is so even though the unions may be Plaintiff's "legally authorized representatives" under Section 15(b)(3) for purposes of signing the required release. The Court does not need to interpret the CBA to determine if the release was signed or not.

The CBAs are only tangentially related to this dispute, if at all. As the U.S. Supreme Court stated in *Allis-Chalmers Corp. v. Lueck*, 471 U.S. 202, 211 (1985), "[N]ot every dispute

[3] Defendants attached the CBA in effect between May 1, 2017 and April 30, 2020. The relevant CBA would be the one in effect when Plaintiff began work at Lincoln Park on December 27, 2012. Even if Defendants had attached the correct CBA, though, Defendants' preemption argument fails for the other reasons described herein.

concerning employment, or *tangentially involving* a provision of a collective-bargaining agreement, is pre-empted by § 301 or other provisions of the federal labor law." (emphasis added). Preemption promotes uniformity of federal labor law, but preemption is required only if resolution of the dispute is "substantially dependent" on analysis of the terms of the CBA. *Id.* at 220.

As the court in *Gelb* directed, this Court has considered the defenses as well as the claims in this case. The Court notes that Defendants have raised no defenses that require an interpretation of the CBAs. Defendants do not assert that the unions received the required BIPA disclosures or signed BIPA releases on behalf of employees. Instead, they only point out that the broad management rights provisions of the CBAs allow them to set work standards. Deciding this case does not require the Court to interpret the CBAs.

In making our holding, the Court respectfully declines to follow the nonbinding Seventh Circuit case of *Miller v. Southwest Airlines*, 926 F. 3d 898 (7th Cir. 2019) and the Northern District of Illinois cases that followed it, *Gray v. Univ. of Chi. Med. Ctr., Inc.*, No. 19-cv-04229, 2019 U.S. Dist. LEXIS 229536 (N.D. Ill. Mar. 26, 2019) and *Peatry v. Bimbo Bakeries USA, Inc.*, No. 19 C 2942, 2020 U.S. Dist. LEXIS 32577 (N.D. Ill. Feb. 26, 2020). Our case involves a motion to dismiss under Section 2-619 of the Illinois Rules of Civil Procedure, which should be granted "only if the plaintiff can prove no set of facts that would support a cause of action." *In re Chicago Flood Litigation,* 176 Ill. 2d 179, 189 (1997). Here, Plaintiff *could* prove a set of facts under which his claim was not preempted. Defendants did not meet their burden of proof on their 2-619 motion to dismiss argument based on Section 301 preemption.

CONCLUSION

Defendants' Motion to Dismiss is granted under 2-619(a)(5) and Plaintiff's Complaint is dismissed with prejudice for failure to bring suit within five years after the cause of action accrued. This is a final order disposing of all matters.

ENTERED:

Judge Pamela McLean Meyerson

Judge Pamela McLean Meyerson

JUN 10 2020

Circuit Court – 2097

477 F.Supp.3d 723
United States District Court,
N.D. Illinois, Eastern Division.

Latrina COTHRON, Individually and on behalf of similarly situated individuals, Plaintiff,
v.
WHITE CASTLE SYSTEM, INC. d/b/a White Castle, Defendant.

No. 19 CV 00382
|
Signed 08/07/2020

Synopsis

Background: Employee brought putative class action in state court against employer, alleging violations of various provisions of Illinois' Biometric Information Privacy Act (BIPA) in connection with implementation of a system that involved capturing employee's fingerprint data and disclosing it to third parties without employee's consent. Employer removed to federal court and moved for judgment on the pleadings.

Holdings: The District Court, John J. Tharp, J., held that:

[1] employer did not waive its right to assert a statute of limitations defense in motion for judgment on the pleadings;

[2] continuing violation doctrine did not apply;

[3] BIPA claims accrued, and statute of limitations period began to run, at the time of each scan of employee's fingerprint post-BIPA and each time employer disclosed employee's biometric information to a third party over that same period without consent.

Motion denied.

Procedural Posture(s): Motion for Judgment on the Pleadings.

West Headnotes (22)

[1] **Federal Civil Procedure** Matters deemed admitted

170A Federal Civil Procedure
170AVII Pleadings
170AVII(L) Judgment on the Pleadings
170AVII(L)1 In General
170Ak1053 Determination of Motion
170Ak1055 Matters deemed admitted

On a motion for judgment on the pleadings, the Court must accept all well-pleaded facts in the second amended complaint as true and draw all permissible inferences in favor of the plaintiffs. Fed. R. Civ. P. 12(c).

[2] **Federal Civil Procedure** Insufficiency of claim or defense

Federal Civil Procedure Insufficiency in general

170A Federal Civil Procedure
170AVII Pleadings
170AVII(L) Judgment on the Pleadings
170AVII(L)1 In General
170Ak1049 Insufficiency of claim or defense
170A Federal Civil Procedure
170AXI Dismissal
170AXI(B) Involuntary Dismissal
170AXI(B)3 Pleading, Defects In, in General
170Ak1772 Insufficiency in general

A motion for judgment on the pleadings is evaluated using the same standard as a motion to dismiss for failure to state a claim: to survive the motion, a complaint must state a claim to relief that is plausible on its face. Fed. R. Civ. P. 12(b)(6), 12(c).

[3] **Federal Civil Procedure** Insufficiency of claim or defense

170A Federal Civil Procedure
170AVII Pleadings
170AVII(L) Judgment on the Pleadings
170AVII(L)1 In General
170Ak1049 Insufficiency of claim or defense

In deciding a motion for judgment on the pleadings, a claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged. Fed. R. Civ. P. 12(c).

[4] **Federal Civil Procedure** 🔑 Determination of Motion

Federal Civil Procedure 🔑 Matters deemed admitted

170A Federal Civil Procedure
170AVII Pleadings
170AVII(L) Judgment on the Pleadings
170AVII(L)1 In General
170Ak1053 Determination of Motion
170Ak1053.1 In general
170A Federal Civil Procedure
170AVII Pleadings
170AVII(L) Judgment on the Pleadings
170AVII(L)1 In General
170Ak1053 Determination of Motion
170Ak1055 Matters deemed admitted

In assessing a motion for judgment on the pleadings, the Court draws all reasonable inferences and facts in favor of the nonmovant, but need not accept as true any legal assertions. Fed. R. Civ. P. 12(c).

[5] **Federal Civil Procedure** 🔑 Limitations and laches

170A Federal Civil Procedure
170AVII Pleadings
170AVII(C) Answer
170AVII(C)2 Affirmative Defense or Avoidance
170Ak755 Limitations and laches

Affirmative defenses, such as the defense of statute of limitations, are external to the complaint.

1 Cases that cite this headnote

[6] **Federal Civil Procedure** 🔑 Limitations and laches

170A Federal Civil Procedure
170AVII Pleadings
170AVII(C) Answer
170AVII(C)2 Affirmative Defense or Avoidance
170Ak755 Limitations and laches

Employer did not waive its right to assert a statute of limitations defense in motion for judgment on the pleadings in employee's action alleging violations of various provisions of Illinois' Biometric Information Privacy Act (BIPA) in connection with implementation of a system that involved capturing employee's fingerprint data and disclosing it to third parties without employee's consent; employer filed an answer after court had denied employer's motion to dismiss employee's second amended complaint in which employer raised a statute of limitations defense and subsequently moved for judgment on the pleadings on that basis. 740 Ill. Comp. Stat. Ann. 14/15(b), 14/15(d); Fed. R. Civ. P. 12(g)(2), 12(h)(2), 12(h)(2)(B).

1 Cases that cite this headnote

[7] **Limitation of Actions** 🔑 Nature of statutory limitation

Limitation of Actions 🔑 Causes of action in general

241 Limitation of Actions
241I Statutes of Limitation
241I(A) Nature, Validity, and Construction in General
241k1 Nature of statutory limitation
241 Limitation of Actions
241II Computation of Period of Limitation
241II(A) Accrual of Right of Action or Defense
241k43 Causes of action in general

A statute of limitations defense is an argument about the timeliness of a claim, and timeliness is a function of both the accrual date of a cause of action and the applicable statute of limitations.

[8] **Limitation of Actions** 🔑 Causes of action in general

241 Limitation of Actions
241II Computation of Period of Limitation
241II(A) Accrual of Right of Action or Defense
241k43 Causes of action in general

Under Illinois law, a cause of action generally accrues and the limitations period begins to run

when facts exist that authorize one party to maintain an action against another.

[9] **Limitation of Actions** Causes of action in general

Limitation of Actions Continuing injury in general

241 Limitation of Actions
241II Computation of Period of Limitation
241II(A) Accrual of Right of Action or Defense
241k43 Causes of action in general
241 Limitation of Actions
241II Computation of Period of Limitation
241II(A) Accrual of Right of Action or Defense
241k55 Torts
241k55(6) Continuing injury in general

Under the continuing tort or continuing violation rule as an exception to the general rule governing accrual, where a tort involves a continuing or repeated injury, the limitations period does not begin to run until the date of the last injury or the date the tortious acts cease.

1 Cases that cite this headnote

[10] **Limitation of Actions** Continuing injury in general

Limitation of Actions Liabilities Created by Statute

241 Limitation of Actions
241II Computation of Period of Limitation
241II(A) Accrual of Right of Action or Defense
241k55 Torts
241k55(6) Continuing injury in general
241 Limitation of Actions
241II Computation of Period of Limitation
241II(A) Accrual of Right of Action or Defense
241k58 Liabilities Created by Statute
241k58(1) In general

Under the "continuing violation doctrine," a continuing violation or tort is occasioned by continuing unlawful acts and conduct, not by continual ill effects from an initial violation.

1 Cases that cite this headnote

[11] **Limitation of Actions** Continuing violation in general

241 Limitation of Actions
241II Computation of Period of Limitation
241II(A) Accrual of Right of Action or Defense
241k58 Liabilities Created by Statute
241k58(1.5) Continuing violation in general

The purpose of the continuing violation doctrine is to allow suit to be delayed until a series of wrongful acts blossoms into an injury on which suit can be brought.

[12] **Limitation of Actions** Continuing violation in general

241 Limitation of Actions
241II Computation of Period of Limitation
241II(A) Accrual of Right of Action or Defense
241k58 Liabilities Created by Statute
241k58(1.5) Continuing violation in general

The continuing violation doctrine, as exception to the general accrual rule for limitations purposes, is misnamed; it is a doctrine not about a continuing, but about a cumulative, violation.

[13] **Limitation of Actions** Continuing violation in general

241 Limitation of Actions
241II Computation of Period of Limitation
241II(A) Accrual of Right of Action or Defense
241k58 Liabilities Created by Statute
241k58(1.5) Continuing violation in general

The continuing violation rule does not apply to a series of discrete acts, each of which is independently actionable, even if those acts form an overall pattern of wrongdoing.

1 Cases that cite this headnote

[14] **Limitation of Actions** Privacy; disclosure of confidential information

241 Limitation of Actions
241II Computation of Period of Limitation
241II(A) Accrual of Right of Action or Defense
241k58 Liabilities Created by Statute
241k58(17) Privacy; disclosure of confidential information

Continuing violation doctrine did not apply to employee's action under Illinois' Biometric Information Privacy Act (BIPA) in connection with employer's implementation of a system

that involved capturing employee's fingerprint data and disclosing it to third parties without employee's consent, even if employer repeatedly violated BIPA's terms; BIPA violations occurred through discrete individual acts, not accumulated courses of conduct, requirement of informed consent was violated fully and immediately when employer scanned employee's fingerprint without consent, employer violated obligation to obtain informed consent before disclosing biometric data when employer disclosed data to third parties without consent, and injuries resulting from violations did not need time to blossom or accumulate. 740 Ill. Comp. Stat. Ann. 14/15(b), 14/15(d).

[15] **Limitation of Actions** Privacy; disclosure of confidential information

241 Limitation of Actions
241II Computation of Period of Limitation
241II(A) Accrual of Right of Action or Defense
241k58 Liabilities Created by Statute
241k58(17) Privacy; disclosure of confidential information

Employee's Illinois' Biometric Information Privacy Act (BIPA) claims accrued, and statute of limitations period began to run, at the time of each scan of employee's fingerprint post-BIPA and each time employer disclosed employee's biometric information to a third party over that same period without consent; employer would have ample opportunity to explain why it was absurd to suppose that the legislature sought to impose harsh sanctions on Illinois businesses that ignored BIPA requirements for more than a decade. 740 Ill. Comp. Stat. Ann. 14/15(b), 14/15(d), 14/20.

1 Cases that cite this headnote

[16] **Statutes** Plain Language; Plain, Ordinary, or Common Meaning

Statutes Plain language; plain, ordinary, common, or literal meaning

361 Statutes
361III Construction
361III(B) Plain Language; Plain, Ordinary, or Common Meaning
361k1091 In general
361 Statutes
361III Construction
361III(C) Clarity and Ambiguity; Multiple Meanings
361k1107 Absence of Ambiguity; Application of Clear or Unambiguous Statute or Language
361k1111 Plain language; plain, ordinary, common, or literal meaning

Under Illinois law, the statutory language must be given its plain and ordinary meaning, and, where the language is clear and unambiguous, courts must apply the statute without resort to further aids of statutory construction.

[17] **Records** Biometric information

326 Records
326V Examination, Inspection, and Disclosure; Public Access
326V(B) Access to and Disclosure of Particular Records
326V(B)2 Records Concerning Individuals; Privacy and Confidentiality
326k320 Particular Subjects of Records Concerning Individuals
326k325 Biometric information
(Formerly 326k31)

A party violates Illinois' Biometric Information Privacy Act (BIPA) when it collects, captures, or otherwise obtains a person's biometric information without prior informed consent; this is true the first time an entity scans a fingerprint or otherwise collects biometric information, but it is no less true with each subsequent scan or collection. 740 Ill. Comp. Stat. Ann. 14/15(b).

[18] **Records** Biometric information

326 Records
326V Examination, Inspection, and Disclosure; Public Access
326V(B) Access to and Disclosure of Particular Records
326V(B)2 Records Concerning Individuals; Privacy and Confidentiality
326k320 Particular Subjects of Records Concerning Individuals
326k325 Biometric information
(Formerly 326k31)

Each time an entity discloses or otherwise disseminates biometric information without consent, it violates Illinois' Biometric Information Privacy Act (BIPA). 740 Ill. Comp. Stat. Ann. 14/15(d).

[19] **Records** Biometric information

326 Records
326V Examination, Inspection, and Disclosure; Public Access
326V(B) Access to and Disclosure of Particular Records
326V(B)2 Records Concerning Individuals; Privacy and Confidentiality
326k320 Particular Subjects of Records Concerning Individuals
326k325 Biometric information
(Formerly 326k31)

Even where an entity transmits the biometric information to a third party to which it has previously transmitted that same information, the redisclosure requires consent under the Illinois' Biometric Information Privacy Act (BIPA). 740 Ill. Comp. Stat. Ann. 14/15(d).

[20] **Records** Particular cases

326 Records
326V Examination, Inspection, and Disclosure; Public Access
326V(H) Penalties and Sanctions
326k602 Particular cases
(Formerly 326k31)

Subjecting private entities who fail to follow Illinois' Biometric Information Privacy Act's (BIPA) requirements to substantial potential liability, including liquidated damages, injunctions, attorney fees, and litigation expenses for each violation of the law is one of the principal means that the Illinois legislature adopted to achieve BIPA's objectives of protecting biometric information. 740 Ill. Comp. Stat. Ann. 14/15(b), 14/15(d).

[21] **Constitutional Law** Wisdom

Constitutional Law Justice

Statutes Giving effect to statute or language; construction as written

Statutes Relation to plain, literal, or clear meaning; ambiguity

92 Constitutional Law
92XX Separation of Powers
92XX(C) Judicial Powers and Functions
92XX(C)2 Encroachment on Legislature
92k2485 Inquiry into Legislative Judgment
92k2489 Wisdom
92 Constitutional Law
92XX Separation of Powers
92XX(C) Judicial Powers and Functions
92XX(C)2 Encroachment on Legislature
92k2485 Inquiry into Legislative Judgment
92k2490 Justice
361 Statutes
361III Construction
361III(C) Clarity and Ambiguity; Multiple Meanings
361k1107 Absence of Ambiguity; Application of Clear or Unambiguous Statute or Language
361k1110 Giving effect to statute or language; construction as written
361 Statutes
361IV Operation and Effect
361k1402 Construction in View of Effects, Consequences, or Results
361k1405 Relation to plain, literal, or clear meaning; ambiguity

Under Illinois law, where the words employed in a legislative enactment are free from ambiguity or doubt, they must be given effect by the courts even though the consequences may be harsh, unjust, absurd or unwise; such consequences can be avoided only by a change of the law, not by judicial construction.

[22] **Constitutional Law** Judicial rewriting or revision

92 Constitutional Law
92XX Separation of Powers
92XX(C) Judicial Powers and Functions
92XX(C)2 Encroachment on Legislature
92k2472 Making, Interpretation, and Application of Statutes
92k2474 Judicial rewriting or revision

It is not the role of a court, particularly a federal court, to rewrite a state statute to avoid

a construction that may penalize violations severely.

Attorneys and Law Firms

***726** Andrew C. Ficzko, James B. Zouras, Ryan F. Stephan, Stephan Zouras, LLP, Chicago, IL, for Plaintiff.

Alexander M. Misakian, Kenneth Daniel Walsh, Lewis Brisbois Bisgaard & Smith LLP, Benjamin Sedrish, Kathleen Mary Ryan, Erin Bolan Hines, Melissa Anne Siebert, William Francis Northrip, Shook, Hardy & Bacon L.L.P., Mary A. Smigielski, Lewis Brisbois, Chicago, IL, Melissa Dunlap Palmisciano, White Castle System, Inc., Columbus, OH, for Defendant.

MEMORANDUM OPINION AND ORDER

John J. Tharp, Jr., United States District Judge

Despite numerous recent suits concerning Illinois' Biometric Information Privacy Act (BIPA), important questions of statutory interpretation remain unresolved. This case presents two such questions: what acts violate BIPA Section 15(b) and Section 15(d) and when do claims premised on such violations accrue? Plaintiff Latrina Cothron alleges that, in 2007, her employer, White Castle System, Inc. ("White Castle"), implemented a system that involved capturing her fingerprint data and disclosing it to third parties. After BIPA's enactment in mid-2008, White Castle continued to operate its system but did not obtain the newly required consent of its employees, thereby violating BIPA Section 15(b) ***727** and Section 15(d).[1] White Castle has moved for judgment on the pleadings pursuant to Federal Rule of Civil Procedure 12(c), arguing that Ms. Cothron's claims accrued in 2008 and are therefore barred by the statute of limitations. Because the Court finds that Ms. Cothron's claims under both Section 15(b) and Section 15(d) are timely, White Castle's motion is denied.

BACKGROUND[2]

[1] The facts set forth below are largely the same as those described in the Court's prior opinion in this case. *See* Mem. Op. Order 2-3, ECF No. 117. Latrina Cothron began working for White Castle in 2004 and is still employed by the restaurant-chain as a manager. Sec. Am. Compl. ¶ 39, ECF No. 44. Roughly three years after Ms. Cothron was hired, White Castle introduced a fingerprint-based computer system that required Ms. Cothron, as a condition of continued employment, to scan and register her fingerprint in order "to access the computer as a manager and access her paystubs as an hourly employee." *Id.* ¶ 40. According to Ms. Cothron, White Castle's system involved transferring the fingerprints to two third-party vendors—Cross Match and Digital Persona—as well as storing the fingerprints at other separately owned and operated data-storage facilities. *Id.* ¶¶ 28-31. Perhaps unsurprisingly—given that the Illinois Biometric Information Privacy Act ("BIPA") did not exist yet—White Castle did not receive a written release from Ms. Cothron to collect her fingerprints or to transfer them to third parties before implementing the system. *Id.* ¶ 41.

When the Illinois legislature enacted BIPA in mid-2008, the legal landscape changed but White Castle's practices did not—at least not for roughly ten years. *Id.* ¶¶ 27-28. White Castle continued to use its fingerprint system in the years following BIPA's passage and continued to disseminate that data to the same third parties. *Id.* ¶¶ 28-31. It was not until October 2018 that White Castle provided Ms. Cothron with the required disclosures or a consent form. *Id.* ¶¶ 45, 48-49. On December 6, 2018, Ms. Cothron filed her class action complaint in the Circuit Court of Cook County, Illinois and the case was subsequently removed to this Court by Cross Match Technologies, Inc. (since dismissed from the case). Mot. J. Pleadings 2, ECF No. 120. After the Court denied White Castle's motion to dismiss Ms. Cothron's second amended complaint, White Castle filed an answer. *Id.* In the answer, White Castle raised a statute of limitations defense and subsequently moved for judgment on the pleadings on that basis. *Id.*

DISCUSSION

[2] **[3]** **[4]** A motion for judgment on the pleadings under Rule 12(c) is evaluated using the same standard as a motion to dismiss under Rule 12(b)(6): to survive the motion, "a complaint must state a claim to relief that is plausible on its face." *Bishop v. Air Line Pilots Ass'n, Int'l*, 900 F.3d 388, 397 (7th Cir. 2018) (citations omitted). A claim has "facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference ***728** that the defendant is liable for the misconduct alleged." *Wagner*

v. Teva Pharm. USA, Inc., 840 F.3d 355, 358 (7th Cir. 2016) (quoting *Ashcroft v. Iqbal*, 556 U.S. 662, 678, 129 S.Ct. 1937, 173 L.Ed.2d 868 (2009)). In assessing a motion for judgment on the pleadings, the Court draws "all reasonable inferences and facts in favor of the nonmovant, but need not accept as true any legal assertions." *Id.* Ms. Cothron provides two arguments for rejecting White Castle's statute of limitations defense: first, that White Castle waived its statute of limitations defense by not asserting it in its previously filed motion to dismiss; second, that her claims are timely.

I. Waiver

[5] **[6]** In making her waiver argument, Ms. Cothron ignores the basic framework provided by the Federal Rules of Civil Procedure as well as the language of Rule 12(g)(2), on which she relies. The Rules provide that a defendant may respond to a complaint by filing a responsive pleading or, alternatively, by filing a motion to dismiss under Rule 12(b). Fed. R. Civ. P. 12(a). A Rule 12(b) motion, which must be made before a responsive pleading, is the proper vehicle for challenging the sufficiency of the complaint. Fed. R. Civ. P. 12(b). And White Castle, in its previously filed motion to dismiss, properly raised arguments under Rule 12(b)(6) that targeted the sufficiency of the complaint. Affirmative defenses (such as the defense of statute of limitations), on the other hand, are "external" to the complaint. *Brownmark Films, LLC v. Comedy Partners*, 682 F.3d 687, 690 n.1 (7th Cir. 2012). Per Rule 8(c), the proper time to identify affirmative defenses is in a defendant's responsive pleading. Fed. R. Civ. P. 8(c). Then, "[a]fter pleadings are closed," a party may subsequently file a motion for judgment on the pleadings and seek judgment based on the previously raised affirmative defense. Fed. R. Civ. P. 12(c). In keeping with these rules, the Seventh Circuit has "repeatedly cautioned that the proper heading for such motions is Rule 12(c)." *Brownmark Films LLC*, 682 F.3d at 690 n.1; *see also Burton v. Ghosh*, 961 F.3d 960, 964-965 (7th Cir. 2020) ("The proper way to seek a dismissal based on an affirmative defense under most circumstances is not to move to dismiss under Rule 12(b)(6) for failure to state a claim. Rather, the defendant should answer and then move under Rule 12(c) for judgment on the pleadings." (citation omitted)). Contrary to Ms. Cothron's argument, White Castle did not waive its right to assert a statute of limitations defense in a motion for judgment on the pleadings; Rule 12(g)(2) expressly states that its limitation on further motions is applicable "***except as provided in Rule 12(h)(2)***." And Rule 12(h)(2)(B), in turn, expressly provides that failure to state a claim may be raised "by a motion under Rule 12(c)"—a motion which, again, may only be made "after the pleadings are closed."[3] Far from having waived its statute of limitations defense, ***729** White Castle has raised the affirmative defense at precisely the procedural posture envisioned by the Rules. Ms. Cothron's argument to the contrary is entirely off-base.

II. Timeliness

[7] Ms. Cothron's second argument for denying the motion —that, considered on the merits, White Castle's statute of limitations defense fails—is substantially stronger; indeed, the Court concludes that it is correct. A statute of limitations defense is an argument about the timeliness of a claim, and timeliness is a function of both the accrual date of a cause of action and the applicable statute of limitations. Nonetheless, in asserting its defense, White Castle limits itself to the issue of accrual and the Court does the same. *See* Reply Br. 5 n.2, ECF No. 124 ("White Castle has argued that Plaintiff's claims are untimely no matter what statute of limitations applies. Should the Court wish to determine the applicable limitations period, White Castle requests additional briefing on the issue.").[4]

[8] **[9]** As a general matter, under Illinois law, a cause of action accrues and the "limitations period begins to run when facts exist that authorize one party to maintain an action against another." *Feltmeier v. Feltmeier*, 207 Ill. 2d 263, 278, 278 Ill.Dec. 228, 798 N.E.2d 75, 85 (2003). On the same facts, however, the parties put forth accrual dates that differ by roughly 10 years: White Castle argues that the claims accrued in mid-2008, while Ms. Cothron contends that at least a portion of her claims accrued in 2018. How so far apart? The ten-year delay stems from accepting either of Ms. Cothron's two theories of accrual. First, Ms. Cothron contends that the alleged BIPA violations can be understood as falling under an exception to the general rule governing accrual, the continuing violation exception. "[U]nder the 'continuing tort' or 'continuing violation' rule, 'where a tort involves a continuing or repeated injury, the limitations period does not begin to run until the date of the last injury or the date the tortious acts cease.' " *Id.* (quoting *Belleville Toyota, Inc. v. Toyota Motor Sales, U.S.A., Inc.*, 199 Ill.2d 325, 345, 264 Ill.Dec. 283, 770 N.E.2d 177 (2002)).

Applying this doctrine, Ms. Cothron argues that the statute of limitations did not begin to run on any portion of her claim until the final violation (the last time White Castle collected and disseminated her fingerprint before she received BIPA notice and provided her consent). In the alternative, Ms.

Cothron contends that each post-BIPA scan of her fingerprint constituted a separate violation of Section 15(b) and each disclosure to a third-party over that same period a separate violation of Section 15(d), with each violation accruing at the time of occurrence. Under this theory, at least a portion of Ms. Cothron's claims did not accrue until 2018 and would therefore be timely under any statute of limitations. White Castle rejects both theories, arguing instead that the complaint describes a single violation of Section 15(b) and a single violation of Section 15(d), both of which occurred and accrued "in 2008, during the first post-BIPA finger-scan that she alleges violated BIPA." Mot. J. Pleadings 10, ***730** ECF No. 120. The Court considers each argument in turn.

A. Continuing Violation Exception

At the outset, it is worth noting that Ms. Cothron's invocation of the continuing violation exception is ambiguous: it is unclear whether, in her view, White Castle's alleged course of conduct amounts to a single ongoing violation of each of the two BIPA provisions at issue or whether her argument is that White Castle violated the statute's terms repeatedly but the violations should be viewed as a continuous whole for prescriptive purposes only. Under either interpretation, however, the argument fails.

[10] **[11]** **[12]** **[13]** The continuing violation doctrine is a well-established, but limited exception to the general rule of accrual. In *Feltmeier*, the Illinois Supreme Court limned the doctrine's scope: "A continuing violation or tort is occasioned by continuing unlawful acts and conduct, not by continual ill effects from an initial violation." 207 Ill. 2d at 278, 278 Ill.Dec. 228, 798 N.E.2d at 85. And those unlawful acts must produce a certain sort of injury for the doctrine to apply: the purpose of the doctrine is "to allow suit to be delayed until a series of wrongful acts blossoms into an injury on which suit can be brought." *Limestone Dev. Corp. v. Vill. of Lemont, Ill.*, 520 F.3d 797, 801 (7th Cir. 2008). Thus, the continuing violation doctrine is "misnamed"—"it is [ ] a doctrine not about a continuing, but about a cumulative, violation." *Id.* *See also Rodrigue v. Olin Employees Credit Union*, 406 F.3d 434, 442 (7th Cir. 2005) ("Where a cause of action arises not from individually identifiable wrongs but rather from a series of acts considered collectively, the Illinois Supreme Court has deemed application of the continuing violation rule appropriate."). By contrast, "the continuing violation rule does not apply to a series of discrete acts, each of which is independently actionable, even if those acts form an overall pattern of wrongdoing." *Id.* at 443. *Compare Cunningham v. Huffman*, 154 Ill. 2d 398, 406, 182 Ill.Dec. 18, 609 N.E.2d 321, 324-325 (Ill. 1993) ("When the cumulative results of continued negligence is the cause of the injury, the statute of repose cannot start to run until the last date of negligent treatment."), *with Belleville Toyota*, 199 Ill. 2d at 349, 264 Ill.Dec. 283, 770 N.E.2d at 192 ("Rather, each allocation constituted a separate violation of section 4 of the Act, each violation supporting a separate cause of action. Based on the foregoing, we agree with defendants that the appellate court erred in affirming the trial court's application of the so-called continuing violation rule.").

[14] BIPA claims do not fall within the limited purview of this exception. The Illinois Supreme Court has held that a person is " 'aggrieved within the meaning of Section 20 of the [BIPA] and entitled to seek recovery under that provision' " whenever "a private entity fails to comply with one of section 15's requirements." *Rosenbach v. Six Flags Entm't Corp.*, 432 Ill. Dec. 654, 663, 129 N.E.3d 1197, 1206 (Ill. 2019). And, as relevant here, Sections 15(b) and 15(d) impose obligations that are violated through discrete individual acts, not accumulated courses of conduct. Section 15(b) provides that no private entity "may collect, capture, purchase, receive through trade, or otherwise obtain" a person's biometric information unless it first receives that person's informed consent. 740 ILCS 14/15(b). This requirement is violated—fully and immediately—when a party collects biometric information without the necessary disclosure and consent. Similarly, Section 15(d) states that entities in possession of biometric data may only disclose or "otherwise disseminate" a person's ***731** data upon obtaining the person's consent or in limited other circumstances inapplicable here. 740 ILCS 14/15(d). Like Section 15(b), an entity violates this obligation the moment that, absent consent, it discloses or otherwise disseminates a person's biometric information to a third party. The injuries resulting from these violations do not need time to blossom or accumulate. Time may exacerbate them, but an injury occurs immediately upon violation.[5] *Cf. Bryant v. Compass Grp. USA, Inc.*, 958 F.3d 617, 627 (7th Cir. 2020), as amended on denial of reh'g and reh'g en banc (June 30, 2020) (by failing to obtain informed consent, defendant "inflicted the concrete injury BIPA intended to protect against, *i.e.* a consumer's loss of the power and ability to make informed decisions about the collection, storage, and use of her biometric information.").

On the facts set forth in the pleadings, White Castle violated Section 15(b) when it first scanned Ms. Cothron's fingerprint and violated Section 15(d) when it first disclosed her biometric information to a third party. At that point,

Ms. Cothron's injuries stemming from those actions were immediately and independently actionable. Even if White Castle repeatedly violated BIPA's terms—a possibility discussed below—that would not transform the violations into a continuing violation. *See Belleville Toyota*, 199 Ill. 2d at 348-49, 264 Ill.Dec. 283, 770 N.E.2d at 192 ("Although we recognize that the allocations were repeated, we cannot conclude that defendants' conduct somehow constituted one, continuing, unbroken, decade-long violation of the Act."). This case presents a substantially similar question to the one confronted in *Belleville Toyota* and the Court views it as a good "indicator of how the [Illinois Supreme] Court would decide this case." *Rodrigue*, 406 F.3d at 444.

In sum, the Court finds that the continuing violation doctrine does not apply to BIPA violations—at least not to those at issue here—and, as a result, Ms. Cothron's right to sue for those violations accrued when the violations occurred. The next question is: when did the alleged violations occur?

III. BIPA Violations Alleged in the Second Amended Complaint

[15] As an alternative argument, Ms. Cothron contends that each post-BIPA scan of her fingerprint constituted an independent violation of Section 15(b) and each disclosure to a third party over that same period violated Section 15(d). Because Ms. Cothron has alleged scans and disclosures occurring within a year of filing suit, this alternative theory would also render at least some of her claims timely. [6]

[16] The question of what constitutes a violation of BIPA's terms is a pure question of statutory interpretation, and the Illinois Supreme Court has counseled that the "most reliable indicator" of legislative intent is "the language of the statute." *Michigan Ave. Nat. Bank v. Cty. of Cook*, 191 Ill. 2d 493, 504, 247 Ill.Dec. 473, 732 N.E.2d 528, 535 (Ill. 2000). "The statutory language must be given its plain and ordinary meaning, and, where the language is clear and unambiguous, we must apply the statute without resort to further aids of ***732** statutory construction." *Id.* Therefore, the analysis must begin with the text of Sections 15(b) and 15(d).

[17] In full, Section 15(b) provides:

> No private entity may collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifier or biometric information, unless it first:
>
> (1) informs the subject or the subject's legally authorized representative in writing that a biometric identifier or biometric information is being collected or stored;
>
> (2) informs the subject or the subject's legally authorized representative in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; and
>
> (3) receives a written release executed by the subject of the biometric identifier or biometric information or the subject's legally authorized representative.

740 ILCS 14/15(b). In the Court's view, this text is unambiguous and therefore dispositive. A party violates Section 15(b) when it collects, captures, or otherwise obtains a person's biometric information without prior informed consent. This is true the first time an entity scans a fingerprint or otherwise collects biometric information, but it is no less true with each subsequent scan or collection. Consider a fingerprint-based system like the one described in Ms. Cothron's complaint. Each time an employee scans her fingerprint to access the system, the system must capture her biometric information and compare that newly captured information to the original scan (stored in an off-site database by one of the third-parties with which White Castle contracted). [7] In other words, the biometric information acts like an account password—upon each use, the information must be provided to the system so that the system can verify the user's identity.

In its only text-based argument to the contrary, White Castle points to the statute's language requiring that informed consent be acquired before collection. That means, White Castle urges, that it is the failure to provide notice that is the violation, not the collection of the data. But that reading simply ignores the required element of collection. There is no violation of Section 15(b) without collection; unlike Section 15(a), a failure to disclose information is not itself a violation. Section 15(b) is violated only where there is both a failure to provide specific information about collection of biometric data and collection of that data. A statutory requirement indicating ***when*** certain information must be provided, moreover, is different than a requirement indicating for ***which*** collections that provision of information is required. The text of Section 15(b) does indicate when consent must be acquired, but it does not differentiate between the first collection and subsequent collections: for any and

all collections, consent must be obtained "first." 740 ILCS 14/15(b).

***733** This understanding of the consent requirement is entirely consistent with the possibility of consent covering multiple future scans (*e.g.*, all scans in the context of employment). Section 15(b) provides for consent through "written release," which is defined elsewhere in the statute as "informed written consent or, in the context of employment, a release executed by an employee as a condition of employment." 740 ILCS 14/10. To comply with Section 15(b), White Castle could have provided Ms. Cothron with a release informing her of "the specific purpose and length of term" for which her information was being used and requiring her consent to all future scans consistent with those uses as a condition of employment. 740 ILCS 14/15(b). On the facts alleged, however, it did not do so until 2018 at the earliest; as for the intervening years, the only possible conclusion is that White Castle violated Section 15(b) repeatedly when it collected her biometric data without first having obtained her informed consent.

[18] **[19]** The language of Section 15(d) requires the same result. In relevant part, Section 15(d) provides:

> No private entity in possession of a biometric identifier or biometric information may disclose, redisclose, or otherwise disseminate a person's or a customer's biometric identifier or biometric information unless:
>
> (1) the subject of the biometric identifier or biometric information or the subject's legally authorized representative consents to the disclosure or redisclosure

740 ILCS 14/15(d). Again, each time an entity discloses or otherwise disseminates biometric information without consent, it violates the statute. This conclusion is especially unavoidable where, as here, the statute includes "redisclose" in the list of actions that cannot be taken without consent. As a result, even where an entity transmits the biometric information to a third party to which it has previously transmitted that same information, the redisclosure requires consent. Here, White Castle does not provide a single text-based argument to the contrary. And again, the Court notes that, as with Section 15(b), it is consistent with the statutory language to obtain consent for multiple future disclosures through a single written release. But it is also once again true that White Castle failed to do so until 2018 at the earliest. Therefore, each time that White Castle disclosed Ms. Cothron's biometric information to a third party without consent, it violated Section 15(d).

[20] **[21]** **[22]** Instead of providing a plausible alternative reading of the statutory text, White Castle maintains that reading Section 15(b) and Section 15(d) this way would lead to absurd results because the statutory damages for each violation—if defined as every unauthorized scan or disclosure of Ms. Cothron's fingerprint—would be crippling. And the Court fully acknowledges the large damage awards that may result from this reading of the statute. But, as an initial matter, such results are not necessarily "absurd," as White Castle insists; as the Illinois Supreme Court explained in *Rosenbach*, "subjecting 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" is one of the principal means that the Illinois legislature adopted to achieve BIPA's objectives of protecting biometric information. *Rosenbach*, 432 Ill. Dec. at 663, 129 N.E.3d at 1207. And absurd or not, the Illinois Supreme Court has repeatedly held that, where statutory language is clear, it must be given effect:

> ***734** Where the words employed in a legislative enactment are free from ambiguity or doubt, they must be given effect by the courts ***even though the consequences may be harsh, unjust, absurd or unwise***. Such consequences can be avoided only by a change of the law, not by judicial construction.

Petersen v. Wallach, 198 Ill. 2d 439, 447, 261 Ill.Dec. 728, 764 N.E.2d 19, 24 (Ill. 2002) (cleaned up) (emphasis added). As a result, the Court is bound by the clear text of the statute. If the Illinois legislature agrees that this reading of BIPA is absurd, it is of course free to modify the statute to make its intention pellucid. But it is not the role of a court—particularly a federal court—to rewrite a state statute to avoid a construction that may penalize violations severely. In any event, this Court's ruling is unlikely to be the last word on this subject. On appeal—and possibly upon certification to the Illinois Supreme Court[8]—White Castle will have ample opportunity to explain why it is absurd to suppose that the legislature sought to impose harsh sanctions on Illinois

businesses that ignored the requirements of BIPA for more than a decade.

In sum, the Court concludes that Ms. Cothron has alleged multiple timely violations of both Section 15(b) and Section 15(d). According to BIPA Section 20, she can recover "for each violation." 740 ILCS 14/20. The number of those timely violations will be resolved at a future point when, in accordance with White Castle's request, further briefing is devoted to the issue of the applicable statute of limitations. For the present, however, it is clear that at least some of her claims survive under this reading of the statute and, therefore, White Castle's motion for judgment on the pleadings is denied.

All Citations

477 F.Supp.3d 723, 2020 IER Cases 298,219

Footnotes

1 Ms. Cothron's second amended complaint included alleged violations of Section 15(a), but the Court dismissed her claims under that provision for lack of Article III standing. *See* Mem. Op. Order 5-6, ECF No. 117.

2 On a motion for judgment on the pleadings, the Court must accept all well-pleaded facts in the second amended complaint as true and draw all permissible inferences in favor of the plaintiffs. *Pisciotta v. Old Nat. Bancorp*, 499 F.3d 629, 633 (7th Cir. 2007).

3 *See* 5C FED. PRAC. & PROC. CIV. § 1392 (3d ed.):

> The operation of Rule 12(h)(2) is relatively simple. The three defenses protected by the rule may be asserted by motion before serving a responsive pleading. Unlike the Rule 12(h)(1) defenses, however, if a party makes a preliminary motion under Rule 12 and fails to include one of the Rule 12(h)(2) objections, she has not waived it, even though, under Rule 12(g), the party may not assert the defense by a second pre-answer motion. As the rule explicitly provides, a defending litigant also may interpose any of the Rule 12(h)(2) defenses in the responsive pleading or in any pleading permitted or ordered by the court under Rule 7(a). Moreover, even if these defenses are not interposed in any pleading, they may be the subject of a motion under Rule 12(c) for judgment on the pleadings or of a motion to dismiss at trial.

4 As noted, the Court accepts, for present purposes, White Castle's position that the statute of limitations for BIPA claims has not been definitively resolved and that such claims are potentially subject to a "one-, two-, or five-year statute of limitations." Mot. J. Pleadings 1, ECF No. 120. Nonetheless, the Court also acknowledges Ms. Cothron's argument that "[e]very trial court that has decided the issue has unanimously held the five-year 'catch-all' limitations period applies." Pl.'s Resp. 8, ECF No. 123.

5 The Court notes that BIPA provides for either liquidated or actual damages, whichever is greater. 740 ILCS 14/20. While actual damages might not be immediately obvious and could emerge at any point after an unlawful scan or disclosure, there is nothing cumulative about the damages that would require treating a series of violations as a continuous whole.

6 As noted *supra* note 4, the shortest potentially applicable statute of limitations is one year.

7 One fact question that may be of particular significance to liability under Section 15(d) is where the comparison takes place. Must White Castle send the newly collected fingerprint scan to one of the third parties in order for the comparison to be made at an off-site location or does White Castle retrieve the information from the off-site location such that the comparison takes place at the White Castle location? It is entirely unclear, however, why the statute is designed such that this distinction should matter to the question of liability; the privacy concerns are implicated equally whether the new data is sent off-site for comparison or the old data is retrieved from an off-site location so that the comparison can take place on-site.

8 The Illinois Supreme Court accepts certified questions from federal courts of appeals but not from federal district courts. *See* Ill. S. Ct. Rule 20.

2020 IER Cases 298,219

End of Document

20 F.4th 1156
United States Court of Appeals, Seventh Circuit.

Latrina COTHRON, individually and on behalf of all others similarly situated, Plaintiff-Appellee,
v.
WHITE CASTLE SYSTEM, INC., Defendant-Appellant.

No. 20-3202
|
Argued September 14, 2021
|
Decided December 20, 2021

Synopsis

Background: Employee brought putative class action in state court against employer, alleging that its fingerprint-scanning and verification system violated the Illinois Biometric Information Privacy Act (BIPA). Following removal, employer moved for judgment on the pleadings based on the statute of limitations. The United States District Court for the Northern District of Illinois, John J. Tharp, J., 477 F.Supp.3d 723, denied the motion. Employer appealed.

Holdings: The Court of Appeals, Sykes, Chief Judge, held that:

[1] employee suffered a concrete and particularized injury which conferred standing, and

[2] Court of Appeals would certify to the Illinois Supreme Court the question as to whether a BIPA claim accrues each time a person's biometric identifier is scanned and each time it is transmitted, or only upon the first scan and first transmission.

Question certified.

Procedural Posture(s): On Appeal; Motion for Judgment on the Pleadings; Motion to Certify Question.

West Headnotes (11)

[1] **Federal Courts** Necessity of Objection; Power and Duty of Court

170B Federal Courts
170BII Jurisdiction, Powers, and Authority in General
170BII(C) Objections, Proceedings, and Determination in General
170Bk2072 Necessity of Objection; Power and Duty of Court
170Bk2073 In general

Subject-matter jurisdiction is the first issue in any case, and the district court has an independent duty to ensure that a case is properly in federal court.

1 Cases that cite this headnote

[2] **Federal Civil Procedure** In general; injury or interest

Federal Courts Case or Controversy Requirement

170A Federal Civil Procedure
170AII Parties
170AII(A) In General
170Ak103.1 Standing in General
170Ak103.2 In general; injury or interest
170B Federal Courts
170BIII Case or Controversy Requirement
170BIII(A) In General
170Bk2101 In general

Essential to "cases and controversies" limitation on jurisdictional reach of the federal courts is the requirement that a plaintiff have standing to sue in federal court. U.S. Const. art. 3, § 2, cl. 1.

[3] **Federal Civil Procedure** In general; injury or interest

Federal Civil Procedure Causation; redressability

170A Federal Civil Procedure
170AII Parties
170AII(A) In General
170Ak103.1 Standing in General
170Ak103.2 In general; injury or interest

170A Federal Civil Procedure
170AII Parties
170AII(A) In General
170Ak103.1 Standing in General
170Ak103.3 Causation; redressability

At the pleading stage, Article III standing requires allegations of a concrete and particularized injury in fact that is traceable to the defendant's conduct and redressable by judicial relief. U.S. Const. art. 3, § 2, cl. 1.

2 Cases that cite this headnote

[4] **Federal Civil Procedure** In general; injury or interest

170A Federal Civil Procedure
170AII Parties
170AII(A) In General
170Ak103.1 Standing in General
170Ak103.2 In general; injury or interest

"Concrete injuries," for purposes of Article III standing, encompass harms that are real, and not abstract. U.S. Const. art. 3, § 2, cl. 1.

[5] **Federal Civil Procedure** In general; injury or interest

170A Federal Civil Procedure
170AII Parties
170AII(A) In General
170Ak103.1 Standing in General
170Ak103.2 In general; injury or interest

"Particularized injuries," for purposes of Article III standing, are those that affect the plaintiff in a personal and individual way. U.S. Const. art. 3, § 2, cl. 1.

[6] **Federal Civil Procedure** In general; injury or interest

Federal Civil Procedure Rights of third parties or public

170A Federal Civil Procedure
170AII Parties
170AII(A) In General
170Ak103.1 Standing in General
170Ak103.2 In general; injury or interest
170A Federal Civil Procedure
170AII Parties
170AII(A) In General
170Ak103.1 Standing in General
170Ak103.4 Rights of third parties or public

Particularized injuries, which are required for Article III standing, must be distinguished from generalized grievances that affect the public generally and for which an individual cannot seek relief in federal court. U.S. Const. art. 3, § 2, cl. 1.

[7] **Records** Persons entitled to pursue proceedings; standing

326 Records
326V Examination, Inspection, and Disclosure; Public Access
326V(G) Judicial Proceedings Concerning Access or Disclosure
326k541 Parties
326k543 Persons entitled to pursue proceedings; standing

Employer's alleged failure to obtain employee's written consent before implementing a fingerprint-scanning system, in violation of the Illinois Biometric Information Privacy Act (BIPA), inflicted a "concrete" and "particularized" injury which conferred standing on employee to pursue claim in federal court; disclosure or dissemination of an employee's biometric data without consent was an act that invaded her private domain and deprived her of her of the opportunity to consider who might possess her biometric data and under what circumstances, given the attendant risks. U.S. Const. art. 3, § 2, cl. 1; 740 Ill. Comp. Stat. Ann. 14/15(d).

1 Cases that cite this headnote

[8] **Limitation of Actions** Torts

241 Limitation of Actions
241II Computation of Period of Limitation
241II(A) Accrual of Right of Action or Defense
241k55 Torts
241k55(1) In general

Under Illinois' single-publication rule, a tort claim based on a defamatory statement contained in a widely circulated publication accrues, for limitations purposes, only upon initial publication, not with each subsequent publication of the same statement.

[9] **Federal Courts** Withholding Decision; Certifying Questions

170B Federal Courts
170BXV State or Federal Laws as Rules of Decision; Erie Doctrine
170BXV(C) Unsettled or Undecided Questions
170Bk3105 Withholding Decision; Certifying Questions
170Bk3106 In general

For a federal court to certify a state law question for resolution by state's highest court, it must first and foremost find itself genuinely uncertain about the answer to the state-law question before considering certification.

[10] **Federal Courts** Withholding Decision; Certifying Questions

170B Federal Courts
170BXV State or Federal Laws as Rules of Decision; Erie Doctrine
170BXV(C) Unsettled or Undecided Questions
170Bk3105 Withholding Decision; Certifying Questions
170Bk3106 In general

For a federal court deciding whether to certify a state law question for resolution by state's highest court, it is important that the dispositive legal question is general and likely to recur rather than unique and fact bound.

[11] **Federal Courts** Particular questions

170B Federal Courts
170BXV State or Federal Laws as Rules of Decision; Erie Doctrine
170BXV(C) Unsettled or Undecided Questions
170Bk3105 Withholding Decision; Certifying Questions
170Bk3107 Particular questions

In employee's action alleging that employer's fingerprint scanning and verification system violated the Illinois Biometric Information Privacy Act (BIPA), the Court of Appeals would certify to the Illinois Supreme Court the question of whether claims alleging BIPA violations for the collection and dissemination of biometric data without prior written consent 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; whether a claim accrued only once or repeatedly was important and recurring question of Illinois law implicating state accrual principles as applied to a novel statute and required authoritative guidance only the state's highest court could provide. 740 Ill. Comp. Stat. Ann. 14/15(b), 14/15(d).

3 Cases that cite this headnote

***1158** Appeal from the United States District Court for the Northern District of Illinois, Eastern Division. No. 19 CV 00382 — **John J. Tharp, Jr.**, *Judge*.

Attorneys and Law Firms

Teresa M. Becvar, Andrew C. Ficzko, Ryan F. Stephan, James B. Zouras, Attorneys, Stephan Zouras, LLP, Chicago, IL, for Plaintiff-Appellee.

Melissa A. Siebert, Erin Bolan Hines, William F. Northrip, Attorneys, Shook, Hardy & Bacon LLP, Chicago, IL, for Defendant-Appellant.

Meredith C. Slawe, Attorney, Cozen O'Connor, Philadelphia, PA, for Amici Curiae Retail Litigation Center, Inc., Restaurant Law Center.

Debra Rae Bernard, Attorney, Perkins Coie LLP, Chicago, IL, Sopen B. Shah, Attorney, Perkins Coie LLP, Madison, WI, for Amicus Curiae LeadingAge Illinois.

Jed Wolf Glickstein, Attorney, Mayer Brown LLP, Chicago, IL, for Amicus Curiae Internet Association.

Randall D. Schmidt, Attorney, Mandel Legal Aid Clinic, Chicago, IL, for Amicus Curiae American Association for Justice.

Catherine Simmons-Gill, Attorney, Office of Catherine Simmons-Gill, LLC, Chicago, IL, for Amicus Curiae NELA/Illinois.

Alan Butler, Attorney, Alan Butler, Washington, DC, for Amicus Curiae Electronic Privacy Information Center.

Before Sykes, Chief Judge, and Easterbrook and Brennan, Circuit Judges.

Opinion

Sykes, Chief Judge.

Latrina Cothron works as a manager at an Illinois White Castle hamburger restaurant where she must scan her fingerprint to access the restaurant's computer system. With each scan her fingerprint is collected and transmitted to a third-party vendor for authentication. Cothron alleges that White Castle did not obtain her written consent before implementing the fingerprint-scanning system, violating the Illinois Biometric Information Privacy Act. She brought this proposed class-action lawsuit on behalf of all Illinois White Castle employees.

White Castle moved for judgment on the pleadings based on the statute of limitations. The restaurant argued that a claim accrued under the Act the first time Cothron scanned her fingerprint into the system after the law took effect in 2008. That was more than a decade before she sued, making her suit untimely under the longest possible limitations period. Cothron responded that every unauthorized fingerprint ***1159** scan amounted to a separate violation of the statute, so a new claim accrued with each scan. That would make her suit timely for the scans within the limitations period.

The district judge rejected White Castle's "one time only" theory of claim accrual and denied the motion. But he found the question close enough to warrant an interlocutory appeal under 28 U.S.C. § 1292(b). Cothron now asks us to certify the question to the Illinois Supreme Court.

We agree that this issue is best decided by the Illinois Supreme Court. Whether a claim accrues only once or repeatedly is an important and recurring question of Illinois law implicating state accrual principles as applied to this novel state statute. It requires authoritative guidance that only the state's highest court can provide.

I. Background

Cothron has worked for White Castle since 2004. She alleges that not long after she began, White Castle introduced a system that requires its employees to scan their finger-prints to access pay stubs and work computers. Each scan is sent to a third-party vendor that authenticates it and gives her access to the restaurant's computer system. Cothron contends that White Castle implemented this system without properly obtaining her consent in violation of the Illinois Biometric Information Privacy Act ("BIPA" or "the Act"), 740 ILL. COMP. STAT. 14/1 *et seq.*

The Illinois General Assembly adopted the Act in 2008 in response to increased commercial use of biometric data. Biometrics are "biologically unique" personal identifiers, *id.* § 14/5(c), and include iris scans, face geometry, and, relevant here, fingerprints, *id.* § 14/10. Unlike other sensitive personal information, like social security numbers, once compromised biometrics cannot be changed. § 14/5(c). The legislative findings note growing concern among members of the public about the use and collection of biometrics. *See id.* § 14/5(d)–(e).

To address these concerns, the Act 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. *Id.* § 14/20. 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. *Id.*

Two of the Act's provisions are relevant here. Section 15(b) provides that a private entity may not "collect, capture, purchase, receive through trade, or otherwise obtain" a person's biometric data without first providing notice to and receiving consent from the person. *Id.* § 14/15(b). Section 15(d) provides that a private entity may not "disclose, redisclose, or otherwise disseminate" biometric data without consent. *Id.* § 14/15(d).

Cothron alleges that White Castle did not attempt to obtain her consent until 2018—a decade after the Act took effect—and therefore unlawfully collected her fingerprints and unlawfully disclosed them to its third-party vendor in violation of sections 15(b) and 15(d), respectively. She sued White Castle and Cross Match Technologies, Inc., the third-party vendor, in Illinois state court seeking to represent White Castle employees whose rights were violated. Cross Match removed the case to federal court under the Class Action Fairness Act of 2005. *See* 28 U.S.C. §§ 1332(d), 1453. (Cothron later voluntarily dismissed Cross Match from the suit, so we mention it no further.)

The district judge sua sponte addressed subject-matter jurisdiction, examining whether Cothron alleged a concrete and particularized injury as required for Article III standing. ***1160** *Cothron v. White Castle Sys., Inc.*, 467 F. Supp. 3d 604 (N.D. Ill. 2020). Based on our reasoning in *Bryant v. Compass Group USA, Inc.*, 958 F.3d 617 (7th Cir. 2020), the judge determined that jurisdiction is secure. *Cothron*, 467 F. Supp. 3d at 611–13.

White Castle then moved for judgment on the pleadings, *see* FED. R. CIV. P. 12(c), arguing that the suit is untimely. (The duration of the limitations period is disputed, but all agree that it is no longer than five years.) White Castle maintained that Cothron filed suit too late because her claim accrued in 2008 with her first fingerprint scan after the Act's effective date. Cothron countered that a new claim accrued each time she scanned her fingerprint and White Castle sent it to the third-party authenticator—not just the first time—so her suit is timely with respect to the unlawful scans and transmissions that occurred within the limitations period.

The judge agreed with Cothron and denied White Castle's motion. *Cothron v. White Castle Sys., Inc.*, 477 F. Supp. 3d 723, 734 (N.D. Ill. 2020). Because the decision involved a controlling question of law on which there is substantial ground for disagreement, the judge certified his order for immediate appeal, *see* § 1292(b), and we accepted the certification. Cothron in turn asks us to certify the question to the Illinois Supreme Court.

II. Discussion

[1] Though no one challenges the judge's jurisdictional ruling, "[s]ubject-matter jurisdiction is the first issue in any case," *Miller v. Sw. Airlines Co.*, 926 F.3d 898, 902 (7th Cir. 2019), so we begin with our "independent duty to ensure" that this case is properly in federal court, *Dexia Crédit Loc. v. Rogan*, 602 F.3d 879, 883 (7th Cir. 2010). After confirming Cothron's standing, we turn to the controlling legal question —whether section 15(b) and 15(d) claims accrue just once or repeatedly—as well as Cothron's request to certify the question to the Illinois Supreme Court.

A. Article III Standing and Section 15(d)

[2] **[3]** Article III of the Constitution limits the jurisdictional reach of the federal courts to "Cases" and "Controversies." U.S. CONST. art. III, § 2. Essential to this limitation is the requirement that a plaintiff have standing to sue in federal court. *DaimlerChrysler Corp. v. Cuno*, 547 U.S. 332, 342, 126 S.Ct. 1854, 164 L.Ed.2d 589 (2006). At the pleading stage, standing requires allegations of a concrete and particularized injury in fact that is traceable to the defendant's conduct and redressable by judicial relief. *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 560–61, 112 S.Ct. 2130, 119 L.Ed.2d 351 (1992); *Bryant*, 958 F.3d at 620–21.

Our decision in *Bryant* resolved the standing question for claims under section 15(b) of the Act, *see* 958 F.3d at 624, but we have yet to decide whether a violation of section 15(d) inflicts a concrete and particularized Article III injury. We do so here.

[4] Concrete injuries encompass harms that are "real, and not abstract." *Spokeo, Inc. v. Robins*, 578 U.S. 330, 340, 136 S.Ct. 1540, 194 L.Ed.2d 635 (2016) (quotation marks omitted). Tangible harms like physical and monetary injuries are the most obvious, but certain intangible harms, most particularly those closely related to harms "traditionally recognized as providing a basis for lawsuits in American courts," also qualify. *TransUnion LLC v. Ramirez*, —— U.S. ——, 141 S. Ct. 2190, 2204, 210 L.Ed.2d 568 (2021); *see also Spokeo*, 578 U.S. at 340–41, 136 S.Ct. 1540. These include, for example, "reputational harms, disclosure of private information, and intrusion upon seclusion." *TransUnion*, 141 S. Ct. at 2204.

***1161** **[5]** **[6]** Particularized injuries are those that "affect the plaintiff in a personal and individual way." *Lujan*, 504 U.S. at 560 n.1, 112 S.Ct. 2130. They must be distinguished from "generalized grievances" that affect the public generally and for which an individual cannot seek relief in federal court. *DaimlerChrysler*, 547 U.S. at 348, 126 S.Ct. 1854.

Our application of these principles to section 15(d) is streamlined by the reasoning in *Bryant* and related circuit precedent regarding other sections of the Act. In *Bryant* we addressed whether the collection of biometric data without complying with section 15(b)'s informed-consent procedures inflicts an Article III injury. 958 F.3d at 620. We noted that the informed-consent duties prescribed by section 15(b) protect a person's privacy interests in his unique biometric data, so a noncompliant collection of biometric data amounts to an invasion of an individual's "private domain, much like an act of trespass." *Id.* at 624.

We explained that the duties imposed by section 15(b) reflect the General Assembly's judgment that people must have

"the opportunity to make informed choices about to whom and for what purpose they will relinquish control" over their biometric data. *Id.* at 626. Failure to comply with these requirements deprives a person of "the opportunity to consider whether the terms of ... collection and usage [are] acceptable given the attendant risks." *Id.* That deprivation, we held, is a concrete and particularized harm, so a violation of section 15(b) inflicts an Article III injury. *Id.*

In *Fox v. Dakkota Integrated Systems, LLC*, 980 F.3d 1146 (7th Cir. 2020), we extended *Bryant*'s reasoning to a provision in section 15(a) of the Act, 740 ILL. COMP. STAT. 14/15(a). The relevant provision conditions the retention of biometric data on compliance with the purposes of its collection as set out in a data-retention schedule. *Fox*, 980 F.3d at 1154–55. We explained that the duty to comply with a data-retention schedule protects a person's biometric privacy just as surely as section 15(b)'s informed-consent requirements. *See id.* at 1155. We thus concluded that the unlawful *retention* of biometric data, just like its unlawful *collection*, works a concrete and particularized Article III injury. *Id.*

[7] The same reasoning applies to section 15(d), which prohibits the disclosure, redisclosure, or dissemination of a person's biometric data without consent, an act that invades his private domain just as surely as an unconsented collection or retention does. Section 15(d) is therefore unlike other sections of the Act that impose duties owed only to the public generally—the violation of which does not, without more, confer standing. *See, e.g., Thornley v. Clearview AI, Inc.*, 984 F.3d 1241, 1247 (7th Cir. 2021) (holding that a violation of section 15(c)'s general prohibition on the sale of biometric data does not inflict an Article III injury); *Bryant*, 958 F.3d at 626 (holding that a violation of section 15(a)'s duty to provide a data-retention schedule to the public does not inflict an Article III injury). And just as with section 15(b), the failure to obtain consent for a disclosure or dissemination deprives a person of the opportunity to consider who may possess his biometric data and under what circumstances, "given the attendant risks." *Bryant*, 958 F.3d at 626. It follows that a violation of section 15(d) inflicts a concrete and particularized Article III injury. Cothron's suit is properly in federal court.

B. BIPA Claim Accrual

The timeliness of the suit depends on whether a claim under the Act accrued each time Cothron scanned her fingerprint to access a work computer or just the first time. Cothron maintains that each scan amounted to a distinct and separately actionable ***1162** section 15(b) violation and that each transmission of her fingerprint likewise amounted to a distinct and separately actionable section 15(d) violation. White Castle says only the first scan and transmission matter for accrual purposes.

The disagreement, framed differently, is whether the Act should be treated like a junk-fax statute for which a claim accrues for each unsolicited fax, *Reliable Money Ord., Inc. v. McKnight Sales Co.*, 704 F.3d 489, 491 (7th Cir. 2013), or instead like certain privacy and reputational torts that accrue only at the initial publication of defamatory material, *Pippen v. NBCUniversal Media, LLC*, 734 F.3d 610, 614–15 (7th Cir. 2013). In the district court, the judge sided with Cothron and denied White Castle's motion for judgment on the pleadings. We review that ruling de novo. *Moss v. Martin*, 473 F.3d 694, 698 (7th Cir. 2007).

1. Illinois Claim-Accrual Principles

This appeal requires us to apply Illinois claim-accrual principles to this unique statute. As a general matter, the Illinois Supreme Court has explained that a claim accrues and "a limitations period begins to run when facts exist that authorize one party to maintain an action against another." *Feltmeier v. Feltmeier*, 207 Ill.2d 263, 278 Ill.Dec. 228, 798 N.E.2d 75, 85 (2003); *see also Khan v. Deutsche Bank AG*, 365 Ill.Dec. 517, 978 N.E.2d 1020, 1028 (Ill. 2012) ("A cause of action 'accrues' when facts exist that authorize the bringing of a cause of action.").

The elements of the statutory cause of action are found in sections 15 and 20 of the Act. Again, as relevant here, section 15(b) makes it unlawful to "collect, capture, purchase, receive through trade, or otherwise obtain" a person's biometric data without his written consent. And section 15(d) makes it unlawful to "disclose, redisclose, or otherwise disseminate" biometric data without the subject's consent. Section 20 sets out the private cause of action, authorizing "[a]ny person aggrieved by a violation" of the Act to sue and "recover for each violation."

The key inquiry for claim-accrual purposes is identifying when these statutory elements were satisfied, thus authorizing suit. *See Khan*, 365 Ill.Dec. 517, 978 N.E.2d at 1028. More to the point here, we must determine whether suit was authorized on only one occasion or instead repeatedly.

2. The Parties' Arguments

Cothron contends that the plain language of section 15(b) points to only one conclusion: each unlawful "collection" of her fingerprint is a separate violation. She further argues that the language of section 15(d) is similarly plain and means that each unlawful "disclosure" or "dissemination" is a separate violation. Finally, she maintains that she was "aggrieved" afresh with each statutory violation. For support she relies on the Illinois Supreme Court's decision in *Rosenbach v. Six Flags Entertainment Corp.*, 432 Ill.Dec. 654, 129 N.E.3d 1197, 1206 (Ill. 2019), which explained that a violation of section 15 itself "aggrieves" a plaintiff within the meaning of section 20. Putting these pieces together, Cothron argues that she has a claim for each fingerprint scan within the limitations period.

White Castle argues that the answer to the accrual question is not quite so straightforward, offering two reasons for its proposed one-time-only rule. First, White Castle invokes a special accrual principle applicable in cases involving defamation and other privacy torts: the single-publication rule. Second, the restaurant argues that the Illinois Supreme Court's reasoning in *Rosenbach* actually points to the opposite conclusion: that a plaintiff is "aggrieved" ***1163** only by the initial violations of sections 15(b) and 15(d).

[8] Under the single-publication rule, a tort claim based on a defamatory statement contained in a widely circulated publication accrues only upon initial publication, not with each subsequent publication of the same statement. *See Ciolino v. Simon*, No. 126024, —— Ill.Dec. ——, ——, —— N.E.3d ——, 2021 WL 1031371, at *6 (Ill. Mar. 18, 2021); *see also Founding Church of Scientology of Wash., D.C. v. Am. Med. Ass'n*, 60 Ill.App.3d 586, 18 Ill.Dec. 5, 377 N.E.2d 158, 160 (1978) ("[T]he cause of action for libel is complete at the time of the first publication, and any subsequent appearances or distributions of copies of the original publication are of no consequence to the creation or existence of a cause of action ...."). The purpose and effect of this rule is to "protect[ ] speakers and writers from repeated litigation arising from a single, but mass-produced, defamatory publication." *Pippen*, 734 F.3d at 615.

Though originally adopted judicially in Illinois, *see Winrod v. Time, Inc.*, 334 Ill.App. 59, 78 N.E.2d 708, 714 (1948), the single-publication rule is now codified in the Uniform Single Publication Act, which Illinois has adopted. The statute provides in relevant part:

> No person shall have more than one cause of action for damages for libel or slander or invasion of privacy or any other tort founded upon any single publication or exhibition or utterance, such as any one edition of a newspaper or book or magazine or any one presentation to an audience or any one broadcast over radio or television or any one exhibition of a motion picture.

740 ILL. COMP. STAT. 165/1.

White Castle argues that an unlawful disclosure of a person's biometric data is a privacy-invading "publication" to which the single-publication rule should apply, drawing on the reasoning in the Illinois Supreme Court's decision in *West Bend Mutual Insurance Co. v. Krishna Schaumburg Tan, Inc.*, No. 125978, —— Ill.Dec. ——, —— N.E.3d ——, 2021 WL 2005464 (Ill. May 20, 2021). There the court held that a disclosure of a fingerprint scan in violation of the Act was a "publication" within the meaning of a commercial insurance policy. *Id.* at ——, —— N.E.3d ——, 2021 WL 2005464 at *7. If White Castle is right, Cothron's section 15(d) claim is untimely.

As Cothron points out, however, there are reasons to doubt the application of the single-publication rule in this context. By its terms the Uniform Single Publication Act covers defamation and other traditional privacy torts, and its illustrative list of publication media—newspapers, books, movies, and television and radio broadcasts—suggests that it may not be a comfortable fit with the Act. Nor is *West Bend Mutual* the slam dunk that White Castle thinks it is. That case concerned whether a section 15(d) disclosure was a publication within the meaning of an insurance contract, not within the meaning of the Uniform Single Publication Act. *Id.* at ——, —— N.E.3d ——, 2021 WL 2005464 at *6.

Even if the single-publication rule does not apply, the language of section 15(d) is arguably consistent with White Castle's proposed first-time-only accrual rule. The ordinary meaning of "disclose" connotes a new revelation. *Disclose*, BLACK'S LAW DICTIONARY (11th ed. 2019) ("To make (something) known or public; to show (something) after a period of inaccessibility or of being unknown; to reveal.").

Repeated transmissions of the same biometric identifier to the same third party are not new revelations. White Castle argues, not unreasonably, that an actionable disclosure occurred only the first time Cothron's fingerprint was transmitted.

***1164** Cothron counters that the Act's ban on "redisclos[ure]" of biometric data forecloses White Castle's proposed accrual rule. She reads the term "redisclose" as used in section 15(d) to include repeated disclosures of the same biometric data to the same third party. For its part, White Castle offers a different interpretation of the term: a downstream disclosure carried out by a third party to whom information was originally disclosed. That reading is consistent with the term "redisclose" as used in other Illinois statutes.[1] Countering again, Cothron argues that this usage would make "redisclose" meaningless surplusage. Section 15(d) applies to any "private entity in possession of a biometric identifier or biometric information." As such, a violation by a down-stream entity can just be called a "disclosure," making "redisclose" redundant under White Castle's reading. Maybe so; or maybe "redisclose" serves to make certain that down-stream entities are subject to section 15(d). *See Reid Hosp. & Health Care Servs., Inc. v. Conifer Revenue Cycle Sols., LLC*, 8 F.4th 642, 652 (7th Cir. 2021) (noting the tension between the anti-surplusage canon and the belt-and-suspenders drafting approach).

Finally, the catchall language in section 15(d)—recall that the statute makes it unlawful to "disclose, redisclose, or *otherwise disseminate*" a person's biometric identifier—does not clearly preclude a single-time accrual rule. The phrase following the terms "disclose" and "redisclose" may simply be a way to ensure that all disclosure-like acts are covered. *See People v. Davis*, 199 Ill.2d 130, 262 Ill.Dec. 721, 766 N.E.2d 641, 645 (2002) ("[W]hen a statutory clause specifically describes several classes of persons or things and then includes 'other persons or things,' the word 'other' is interpreted as meaning 'other such like.' "). The upshot is that although section 15(d) does not clearly say that a claim accrues only once, that is a plausible reading of the statutory language.

White Castle's second argument is based on the Illinois Supreme Court's reasoning in *Rosenbach*, which concerned section 15(b) of the Act. There, a Six Flags amusement park collected a patron's fingerprint to facilitate his entry to the park as a season pass holder. *Rosenbach*, 432 Ill.Dec. 654, 129 N.E.3d at 1200. He sued for the unlawful collection of his biometric data in violation of section 15(b). *Id.*, 432 Ill.Dec. 654, 129 N.E.3d at 1201. The question was whether the alleged statutory violation by itself "aggrieved" the plaintiff within the meaning of section 20, giving him the right to sue. *Id.*, 432 Ill.Dec. 654, 129 N.E.3d at 1202.

To answer the question, the Illinois Supreme Court explained that the Act generally protects a person's "right to privacy in and control over" his biometric data and that the provisions in section 15 define the contours of that right. *Id.*, 432 Ill.Dec. 654, 129 N.E.3d at 1206. It follows, the court held, that a violation of one of those provisions aggrieves a plaintiff within the meaning of section 20. *Id.* The court was clear that "[n]o additional consequences need be pleaded or proved." *Id.* Accordingly, a plaintiff can sue without "show[ing] some injury beyond [a] violation of [his] statutory ***1165** rights." *Id.*, 432 Ill.Dec. 654, 129 N.E.3d at 1207.

Rosenbach's expansive language can be read to favor Cothron's position. A section 15 violation, without more, aggrieves a plaintiff within the meaning of section 20. And it may follow that an "aggrievement" occurs at each violation, with a claim accruing each time as well.

At bottom, however, the issue in *Rosenbach* was not claim accrual, let alone the repeated accrual issue we consider here. Seizing this opening, White Castle focuses on *Rosenbach*'s reasoning, with special emphasis on the court's explanation that the Act protects a person's right of "privacy in and control over" his biometric data. White Castle theorizes that this right is fully invaded by an initial violation of section 15(b) or 15(d) and that repeated violations by the same person do no further harm to the person's privacy or control rights.

White Castle's one-and-done theory makes sense if we accept that subsequent collections or disclosures of biometric data do not work a harm that the Act seeks to prevent. And more importantly, focusing on what it means to be "aggrieved" by a violation of the statute gives this theory a plausible hook in the statutory text. But the theory also has some notable weak spots. The premise—two violations aren't worse than one—may simply be wrong. Repeated collections or disclosures of biometric data, even if by or to the same entity, might increase the risk of misuse or mishandling of biometric data. If so, each violation would seem to independently aggrieve a plaintiff. And the theory is hard to square with the broad language in *Rosenbach* that "[n]o additional consequences need be pleaded or proved" other than a violation of the plaintiff's statutory rights. *Id.*, 432 Ill.Dec. 654, 129 N.E.3d at 1206.

Beyond their arguments from text and precedent, both Cothron and White Castle maintain that the other's position would produce untenable consequences that the General Assembly could not possibly have intended. *See People v. Collins*, 214 Ill.2d 206, 291 Ill.Dec. 686, 824 N.E.2d 262, 266 (2005) ("[I]n construing a statute, we presume that the legislature did not intend an absurd result."). White Castle reminds us that the Act provides for statutory damages of $1,000 or $5,000 for "each violation" of the statute. § 14/20. Because White Castle's employees scan their fingerprints frequently, perhaps even multiple times per shift, Cothron's interpretation could yield staggering damages awards in this case and others like it. If a new claim accrues with each scan, as Cothron argues, violators face potentially crippling financial liability.

Cothron responds that the calculation of damages is separate from the question of claim accrual. True, but she does not explain how alternative theories of calculating damages might be reconciled with the text of section 20. Her better point is that White Castle's first-time-only reading would itself lead to an odd result. Once a private entity has violated the Act, it would have little incentive to course correct and comply if subsequent violations carry no legal consequences. All told, the practical implications of either side's interpretation, to the extent that Illinois courts would weigh them, do not decisively tilt one way or the other.

C. Certification

In light of the novelty and uncertainty of the claim-accrual question, Cothron asks us to certify it to the Illinois Supreme Court. Our rules permit us to certify state-law questions to a state supreme court when the answer will control the outcome of a case and the state court accepts such certifications. 7TH CIR. R. 52(a). The Illinois Supreme Court accepts certified questions from this court when none of its precedents ***1166** control and the answer to the certified question will determine the outcome of the case. ILL. S. CT. R. 20(a). Those threshold requirements are met here. The Illinois Supreme Court has not yet decided whether section 15(b) and 15(d) claims accrue repeatedly. If they do, Cothron's action can continue; otherwise, it fails.

[9] These are necessary but not sufficient conditions for certification. We are mindful of our obligation not to burden a state's highest court with unwarranted certification requests, so additional factors weigh in the balance. *See State Farm Mut. Auto. Ins. Co. v. Pate*, 275 F.3d 666, 671 (7th Cir. 2001). First and foremost, we must find ourselves "genuinely uncertain" about the answer to the state-law question before considering certification. *In re Hernandez*, 918 F.3d 563, 570 (7th Cir. 2019). That criterion is satisfied here. As discussed, there are reasons to think that the Illinois Supreme Court might side with *either* Cothron or White Castle. A wrong answer may also transcend the Act and implicate fundamental Illinois accrual principles on which only the state's highest court can provide authoritative guidance. [2]

[10] It's also important that the dispositive legal question is general and likely to recur rather than unique and fact bound. *Zahn v. N. Am. Power & Gas, LLC*, 815 F.3d 1082, 1085 (7th Cir. 2016). The question here is a purely legal one that has already shown itself to frequently arise. It drew significant interest from amici on both sides. Several federal district courts have recently stayed their proceedings awaiting our judgment in this case. *E.g., Callender v. Quality Packaging Specialists Int'l, LLC*, No. 21-cv-505-SMY, 2021 WL 4169967, at *2 (S.D. Ill. Aug. 27, 2021); *Johns v. Paycor, Inc.*, No. 20-cv-00264-DWD, 2021 WL 2627974, at *2 (S.D. Ill. May 11, 2021).

Finally, it matters that the Act is a unique Illinois statute regularly applied by the federal courts, *see Nagy v. Riblet Prods. Corp.*, 79 F.3d 572, 577 (7th Cir. 1996), and one that the Illinois Supreme Court has shown an interest in interpreting, *see Stephan v. Rocky Mountain Chocolate Factory, Inc.*, 129 F.3d 414, 418 (7th Cir. 1997). In addition to deciding *Rosenbach* in 2019 and *West Bend Mutual* in 2021, the court recently accepted review of *McDonald v. Symphony Bronzeville Park, LLC*, 444 Ill.Dec. 183, 163 N.E.3d 746 (Table) (Ill. 2021), which asks whether the state's Workers' Compensation Act precludes an employee's claims for statutory damages under the Act.

[11] Accordingly, the relevant criteria favor certification. We therefore respectfully ask the Illinois Supreme Court, in its discretion, to answer the following certified question:

> ***1167** 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?

Nothing in this certification should be read to limit the scope of the Illinois Supreme Court's inquiry, and the justices are invited to reformulate the certified question. Further proceedings in this court are stayed while this matter is under consideration by the Illinois Supreme Court.

QUESTION CERTIFIED

All Citations

20 F.4th 1156

Footnotes

1 *See, e.g.*, 740 ILL. COMP. STAT. 110/5(d) ("No person or agency to whom any information is disclosed under this [s]ection may redisclose such information unless the person who consented to the disclosure specifically consents to such redisclosure."); *id.* § 110/9 ("A person to whom disclosure is made under this [s]ection shall not redisclose any information except as provided in this Act."); 20 ILL. COMP. STAT. 505/35.3(b) ("A person to whom disclosure of a foster parent's name, address, or telephone number is made under this [s]ection shall not redisclose that information except as provided in this Act or the Juvenile Court Act of 1987.").

2 Just a few days ago, the First District of the Illinois Appellate Court decided *Watson v. Legacy Healthcare Financial Services, LLC*, No. 1-21-0279, —— Ill.Dec. ——, —— N.E.3d ——, 2021 WL 5917935 (Ill. App. Ct. Dec. 15, 2021). There the court held that a section 15(b) claim accrues with "each and every capture and use of [a] plaintiff's fingerprint or hand scan." *Id.* at ——, —— N.E.3d ——, 2021 WL 5917935 at *5. Generally speaking, certification to a state supreme court is not appropriate when the state's intermediate appellate courts have addressed the question and agree on the answer. *See Liberty Mut. Fire Ins. Co. v. Statewide Ins. Co.*, 352 F.3d 1098, 1100 (7th Cir. 2003) (declining to certify a question to the Illinois Supreme Court because the "Illinois appellate courts have spoken, and they are not in conflict"). The recent decision in *Watson* does not weigh against certification. It is the only appellate decision to address the repeated accrual of claims under the Act, and it did not address section 15(d), which we consider alongside section 15(b) here. Furthermore, as we explain, the issue of claim accrual under the Act is a close, recurring, and hotly disputed question of great legal and practical consequence that requires authoritative guidance from the Illinois Supreme Court.