

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

AISHA NAMUWONGE, individually, and on)	
behalf of all other similarly situated individuals,)	
)	Case No. 1:19-cv-03239
Plaintiff,)	
)	Judge Sharon Johnson Coleman
v.)	
)	
KRONOS, INC.,)	
)	
Defendant.)	

MEMORANDUM OPINION AND ORDER

Plaintiff Aisha Namuwonge filed a class action complaint against defendant Kronos, Inc. alleging violations of the Illinois Biometric Information Privacy Act (“BIPA”), 740 ILCS 14/1, *et seq.* Kronos moves to dismiss the class action complaint pursuant to Federal Rule of Civil Procedure 12(b)(6). For the reasons stated below, the motion is granted in part and denied in part.

Background

The following facts are summarized from the complaint and taken as true for the purpose of deciding this motion. Defendant Kronos is a leading provider in workforce management software and services. The corporation is best known for its devices that enable employers to process payroll and track employee time. Kronos provides Brookdale Senior Living, Inc. with an employee timekeeping system. Brookdale operates and owns over 1,000 senior living communities in the United States.

Namuwonge began working as a utility worker for a Brookdale facility in Cook County, Illinois on February 11, 2019. Brookdale requires employees to enroll in its database system, supplied by Kronos, that scans their fingerprint as a means of authenticating and monitoring time worked. Namuwonge and other Brookdale employees scanned their fingerprint each time they

clocked in and clocked out for work. Brookdale subsequently stored Namuwonge's fingerprint data in its Krono database. Namuwonge was never provided with nor signed a written release allowing Kronos or Brookdale to collect, store, use, or disseminate her biometric data.

Based on information and belief, Namuwonge alleges that Brookdale failed to inform their employees that they disclose the employees' fingerprint data to third party vendor Kronos. Namuwonge further alleges, also based on information and belief, that Kronos failed to inform Brookdale employees that Kronos disclosed their fingerprints to other third parties, which host data in their data centers. Kronos failed to provide Brookdale employees with a written, publicly available policy explaining their retention schedules and guidelines for permanently destroying biometric data in their possession. Namuwonge further alleges that because Kronos "neither publish[es] a BIPA-mandated data-retention policy nor disclose[s] the purposes for their collection and use of biometric data, Brookdale employees have no idea whether any Defendant sells, discloses, re-discloses, or otherwise disseminates their biometric data." (Dkt. 1-1, Compl. ¶ 41.)

On April 5, 2019, Namuwonge initiated this class action lawsuit against Kronos in the Circuit Court of Cook County, Illinois, alleging three separate violations of BIPA's provisions: 740 ILCS 14/15(a), (b), and (d). Namuwonge, individually, and on behalf of the class, seeks to recover liquidated damages of \$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. Kronos removed this lawsuit to federal court. Now, Kronos moves to dismiss the class action complaint for failure to state a cause of action upon which relief can be granted.

Legal Standard

In ruling on a Rule 12(b)(6) motion to dismiss, the Court accepts all of the plaintiff's allegations as true and views them in the light most favorable to the plaintiff. *Lavalais v. Vill. of Melrose Park*, 734 F.3d 629, 632 (7th Cir. 2013). To survive a motion to dismiss, a complaint must

contain allegations that “state a claim to relief that is plausible on its face.” *Id.* at 632 (internal quotations omitted). The plaintiff does not need to plead particularized facts, but the allegations in the complaint must be sufficient to “raise a right to relief above the speculative level.” *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555, 127 S.Ct. 1955, 167 L.Ed.2d 929 (2007). Threadbare recitals of the elements of a cause of action and allegations that are merely legal conclusions are not sufficient to survive a motion to dismiss. *Ashcroft v. Iqbal*, 556 U.S. 662, 678, 129 S.Ct. 1937, 173 L.Ed.2d 868 (2009).

Discussion

BIPA “imposes numerous restriction on how private entities collect, retain, disclose and destroy biometric identifiers ... Under the Act, any person ‘aggrieved’ by a violation of its provisions ‘shall have a right of action against an offending party’ and ‘may recover for each violation.’” *Rosenbach v. Six Flags Entm’t Corp.*, 2019 IL 123186, ¶ 1, 129 N.E.3d 1197 (Ill. 2019); *see also* 740 ILCS 14/1 *et seq.* BIPA imposes distinct sets of obligations on possessors and collectors of biometric data. Entities “in possession” of biometric identifier or biometric information must develop publicly available retention schedules and destruction deadlines. 740 ILCS 14/15(a). These entities also may not disclose or otherwise disseminate the data except under certain circumstances. 740 ILCS 14/15(d). Entities that collect biometric information are subjected to heightened criteria. Namely, these entities must inform the subject in writing that biometric information is being collected and receive an executed written release authorizing the collection. 740 ILCS 14/15(b).

First, Kronos contends that Namuwonge failed to adequately plead that Kronos actually possessed Brookdale employees’ biometric data as required under provisions 15(a) and 15(d). Kronos argues that possession requires the exercise of dominion and control over the biometric data “to the exclusion of others.” (Dkt. 23 at 5.) Namuwonge responds that she sufficiently alleges that

Kronos captured, collected, stored, and used her biometric data and that more than one entity may possess biometric or any electronic data at any given time.

The Court begins its analysis with the Illinois Supreme Court’s recent holding in *Rosenbach v. Six Flags Entertainment Corporation*, 2019 IL 123186, 129 N.E.3d 1197 (Ill. 2019). In *Rosenbach*, the plaintiff alleged that defendant Six Flags collected and stored her son’s fingerprint without informing her son or her of the purpose of data collection or obtaining written consent. *Rosenbach*, 2019 IL 123186 at ¶ 6–9. The Illinois Supreme Court reversed the lower court’s finding that one qualifies as an “aggrieved” person only when he or she has alleged some actual injury beyond a violation of the rights under the statute. In reaching its decision, the court engaged in “basic principles of statutory construction” to examine the plain and ordinary meaning of the statute language to best give effect to the legislature’s intent. *Id.* at ¶ 24 (citing *Acme Markets, Inc. v. Callanan*, 236 Ill. 2d 29, 37–38, 923 N.E.2d 718 (2009)). The Illinois Supreme Court held that when a statute does “not contain its own definition” of what a particular term means, “[the court] assume[s] the legislature intended for it to have its popularly understood meaning.” *Rosenbach*, 2019 IL 123186 at ¶ 29. Similarly, where “a term has a settled legal meaning, the courts will normally infer that the legislature intended to incorporate that established meaning into the law.” *Id.* (citing *People v. Johnson*, 2013 IL 114639, ¶ 9, 995 N.E.2d 986 (Ill. 2013)).

Applying the lessons of *Rosenbach* here, the Court looks first to the statute language. The statute does not define what it means to be “in possession” of biometric information. *See* 740 ILCS 14/10. Following the “ordinarily understood” rule, however, the Illinois Supreme Court held that possession “occurs when a person has or takes control of the subject property or holds the property at his or her disposal.” *People v. Ward*, 215 Ill. 2d 317, 325, 830 N.E.2d 556 (2005). The *Ward* court elaborated that the legislature did not intend for the reader “to delve into the legal intricacies of the word ‘possession’” and rejected Kronos’ argument that “possession” means exclusive control over

property. *Id.* at 325–26. Here, the Court similarly finds no indication that the ordinary meaning of possession does not apply. Thus, the Court finds that Namuwonge’s allegation that Brookdale disclosed their employees’ fingerprint data to Kronos sufficiently alleges that Kronos possessed the fingerprint data collected by Brookdale.

Next, the Court considers whether Namuwonge adequately pleaded that Kronos failed to develop a BIPA-compliant retention schedule, as required by section 15(a). Kronos asserts that because it has a publicly available retention schedule for data, of which Namuwonge’s counsel is aware due to similar litigation, Kronos has not violated section 15(a). Namuwonge contends that Kronos was not in compliance during the entire statutory period and that Kronos’ retention schedule and guidelines were made publicly available shortly before this complaint was filed in April 2019.

BIPA states that a “private entity in possession of biometric identifiers or biometric information *must* develop a written policy.” 740 ILCS 14/15(a) (emphasis added). While the statute does not explicitly address the timing for when the written policy should be formulated, the language does not clearly require that it exist before an entity possesses biometric information. In *Rogers v. CSX Intermodal Terminals, Inc.*, the plaintiff sued a rail transportation firm that required him to scan his fingerprint on a biometric device when picking up and dropping off freight loads. No. 1:19-C-2937, 2019 WL 4201570, at *1 (N.D. Ill. Sept. 5, 2019) (Aspen, J.). The court rejected the defendant’s argument that the retention schedule and destruction policy is only required after biometric data is collected because the plaintiff also alleged that defendant “failed to make publicly available any retention or destruction policies.” *Id.* at *4. The court found that the lack of temporal restriction was sufficient to maintain a claim under section 15(a). *Id.*

In contrast, an Illinois Circuit Court dismissed a section 15(a) claim where the plaintiff alleged that the retention schedule and destruction guidelines were not available “‘prior to’

possession of the biometrics information.” *Bernal v. ADP, LLC*, No. 2017-CH-12364, 2019 WL 5028609, at *2 (Ill. Cir. Ct. Aug. 23, 2019). Recognizing that Illinois is a fact-pleading jurisdiction, *id.* at *1, the *Bernal* court reasoned that while it may be true that ADP was not in compliance with section 15(a) before taking possession of biometric information, “such an allegation does not exclude the possibility that [ADP] made available to the public an established schedule and guidelines when, and not before, it was in possession of Plaintiff’s biometric information.” *Id.* at *2.

This Court finds the reasoning of the *Rogers*’ court compelling. Because Namuwonge alleges that Kronos did not publish a data-retention policy and it is unclear from the allegations when any retention policy was formulated relative to when Kronos possessed the Brookdale employees’ biometric information, the Court finds the allegations plausible to state a claim. Namuwonge’s claim is not temporarily restricted. Further, this outcome is consistent with the Illinois Supreme Court’s statements in *Rosenbach* that BIPA’s enforcement mechanism is crucial to ensure compliance by private entities. *See* 2019 IL 12186 at ¶ 34. The Court denies the motion to dismiss Count I brought regarding section 15(a).

Turning to section 15(d), Kronos contends that this claim fails because Namuwonge alleges the transmission of data, which is governed by section 15(e), and not the disclosure of data, which is regulated by 15(d). In addition, Kronos argues that Namuwonge did not allege sufficient facts to support a claim of disclosure to a third party under section 15(d). Namuwonge responds that Kronos has violated section 15(d) because a disclosure occurs when biometric information is transmitted to a third party and that it has alleged that Kronos disclosed her biometric information.

Section 15(d) limits transfers of biometric information while section 15(e) requires that private entities protect biometric information from disclosure. *Miller v. Sw. Airlines Co.*, 926 F.3d 898, 901 (7th Cir. 2019) (citing 740 ILCS 14/15(d)). Again, Kronos points to dictionary definitions to support its arguments for dismissal. BIPA also does not define the terms “transmission” and

“disclosure,” and the Court again does not find Kronos’ argument regarding their meaning compelling. Unlike the word “possession,” Black’s Law Dictionary’s definition for the word “transmit” is simple: “[t]o send or transfer (a thing) from one person or place to another” or “[t]o communicate.” *See Transmit*, Black’s Law Dictionary (11th ed. 2019). The word “disclosure,” however, is broader and more varied. The primary definition is “[t]he act or process of making known something that was previously unknown; a revelation of facts.” *See Disclosure*, Black’s Law Dictionary (11th ed. 2019).

Namuwonge, however, must still provide enough details through her allegations to give Kronos fair notice of what the claim is and “the grounds upon which it rests.” *See Tamayo v. Blagojevich*, 526 F.3d 1074, 1083 (7th Cir. 2008) (internal quotation marks and citations omitted). Here, Namuwonge pleaded on information and belief that Brookdale failed to inform her that they disclosed her fingerprint data to Kronos, which in turn disclosed her fingerprints to other third parties that host the data. (Dkt. 1-1, Compl. ¶¶ 34–35.) Namuwonge further alleged that “Brookdale employees have no idea whether any Defendant sells, discloses, re-discloses, or otherwise disseminates their biometric data.” (*Id.* at ¶ 41.) Namuwonge did not allege other specifics related to any disclosure by Kronos to a third party. Based on her definitive statement, Namuwonge has not pleaded sufficient factual allegations that plausibly suggest that Kronos disclosed or distributed her data to a third party. The Court cannot allow Namuwonge to proceed on such speculative allegations, so the Court grants Kronos’ motion to dismiss Count III brought under section 15(d).

Next, Kronos asserts that Namuwonge fails to allege a section 15(b) claim because she fails to plead facts placing Kronos within any category of collectors of biometric data under BIPA. Namuwonge responds that any private entity that collected biometric data must receive informed consent, which encompasses Kronos.

Section 15(b) requires private entities that collect, capture, or otherwise obtain a person’s biometric information to inform the subject in writing that the private entity is collecting or otherwise has obtained a person’s data and secured the person’s written consent. 740 ILCS 14/15(b). Namuwonge alleges that Brookdale used a Kronos system to collect her and other Brookdale employees’ fingerprints. (Dkt. 1-1, Compl. ¶ 33.) The Illinois legislature used the term possession in certain sections of BIPA (*i.e.*, sections 15(a) and 15(d)), but chose not to include possession in section 15(b). “Where the legislature uses certain words in one instance and different words in another, it intended different results.” *Dana Tank Container, Inc. v. Human Rights Comm’n*, 292 Ill. App. 3d 1022, 1026, 687 N.E.2d 102 (1st Dist. 1997).

Here, there is a difference between *possessing* and *collecting* biometric information. Although Namuwonge asserts that “[e]ach Defendant systematically and automatically collected, used, stored and disseminated [her] ... biometric identifiers” (Dkt. 1-1, Compl. ¶ 89) and that she “had [her] ‘biometric identifiers’ collected by Defendants ..., as explained in detail in Sections II and III,” (*id.* at ¶ 77), the more precise allegation referred to in Section II makes clear that Brookdale collected the fingerprints using a system that Kronos supplied to Brookdale. (*Id.* at ¶ 33.) Together, these allegations do not plausibly allege that Kronos collected, captured, or otherwise obtained Namuwonge’s biometric information. Without more, Namuwonge does not plausibly allege a violation of section 15(b). In light of this, the Court does not address the parties’ arguments regarding whether section 15(b) requires a private entity other than an employer to secure an executed written release, and the Court grants Kronos’ motion to dismiss the section 15(b) claim.

Finally, Kronos asserts that Namuwonge failed to plead negligence, recklessness, or intent, which are additional grounds for dismissal. Kronos argues in the alternative that the Court should strike Namuwonge’s prayer for the \$5,000 statutory reward based on a reckless or intentional violation. Namuwonge has alleged that Kronos failed to maintain a satisfactory biometric data

retention policy, despite BIPA taking effect more than ten years ago. The Court may “draw on its judicial experience and common sense,” *Iqbal*, 556 U.S. at 679, and thus may plausibly infer from Namuwonge’s allegations that Kronos acted negligently. However, she does not allege any substantive details regarding whether the allegations were reckless or intentional. “States of mind may be pleaded generally, but a plaintiff still must point to details sufficient to render a claim plausible.” *Pippen v. NBCUniversal Media, LLC*, 734 F.3d 610, 614 (7th Cir. 2013) (citing *Twombly*, 550 U.S. at 570). Namuwonge’s abstract statements regarding damages are insufficient for the Court to infer that Kronos acted recklessly or intentionally. *Huri v. Office of the Chief Judge of the Circuit Court of Cook Cty.*, 804 F.3d 826, 832 (7th Cir. 2015). Thus, Namuwonge’s claim for damages based on intentional and reckless conduct is dismissed.

Conclusion

Based on the foregoing, Kronos’ Motion to Dismiss [22] is granted as Counts II and III without prejudice and damages for intentional and reckless conduct are stricken without prejudice. The Court denies the motion as to Count I. If Namuwonge believes that she can cure the deficiencies in her complaint, she may file amended papers with the Court within 30 days of the date of this Order.

IT IS SO ORDERED.

Date: 11/22/2019

Entered: 
SHARON JOHNSON COLEMAN
United States District Court Judge