

**UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION**

William Naughton, individually and on
behalf of all others similarly situated,

Plaintiff,

v.

Amazon.com, Inc. and Amazon.com,
LLC,

Defendants.

Case No. 20-cv-6485

Judge Mary M. Rowland

MEMORANDUM OPINION AND ORDER

Plaintiff William Naughton claims that, during the COVID-19 pandemic, his employer, Defendant Amazon, required wellness checks as a condition to his entry into the warehouse where he worked. These wellness checks included scans of Naughton's facial geometry—a type of sensitive biometric data. Naughton, on behalf of himself and other putative class members, claims that Amazon has taken this data without his consent and has further disclosed the information to other parties in violation of the Illinois Biometric Information Privacy Act (BIPA). Amazon has moved to dismiss pursuant to Federal Rule of Civil Procedure 12(b)(6). [36]. For the reasons explained below, this Court denies Amazon's motion.

I. Background

Defendants Amazon.com, Inc. and Amazon.com, LLC (collectively, Amazon) operate a leading multinational technology company specializing in e-commerce, cloud-based servicing, streaming, and artificial intelligence. [33] ¶ 1. The named

Plaintiff, William Naughton, worked for Amazon as a “Picker” from September to October 2020 at one of its fulfillment warehouses in Joliet, Illinois. *Id.* ¶ 2.

In approximately June 2020, Amazon began requiring its workers to provide scans of their facial geometry, and possibly other biometric information, as part of a wellness check prior to being allowed to access the facility each day. *Id.* ¶ 4. Naughton alleges, on information and belief, that Amazon uses facial recognition devices and associated software at their fulfillment centers and warehouse locations throughout Illinois. *Id.* ¶ 6. The facial recognition devices and associated software collect and capture biometric identifiers including facial geometry, retinas, and irises. *Id.* ¶ 7. Amazon also scans and records workers’ temperatures. *Id.* Naughton claims that, as a result of Amazon’s conduct, he and the putative class members lost their rights to control the collection, use, and storage of their biometric identifiers and information. *Id.* ¶ 9. Naughton also claims he and the other class members “were exposed to ongoing, serious, and irreversible privacy risks.” *Id.*

Naughton alleges that Amazon never informed him it was collecting, obtaining, or storing his biometric data; never developed or adhered to any publicly available retention schedule and guidelines for permanently destroying Naughton’s biometric data; and never obtained Naughton’s consent for any disclosure or dissemination of his biometric data to third parties. *Id.* ¶ 46. Naughton has never seen, been made aware of, or been able to find any biometric data retention policy, nor does he know of any policies regarding whether Amazon will ever permanently delete his biometric data. *Id.* ¶ 48.

Naughton brings claims on behalf of himself and a class of people defined as: “All employees who entered Defendant’s locations in the State of Illinois who had their facial geometry scans, biometric identifiers, and/or biometric information collected, captured, received, or otherwise obtained, maintained, stored, disclosed, or disseminated by Defendant during the applicable statutory period.” *Id.* ¶ 59. His first amended complaint asserts claims for: failing to institute, maintain, and adhere to publicly available retention schedule and destruction guidelines in violation of 740 Ill. Comp. Stat. § 14/15(a) (Count I); failing to obtain informed written consent and release before collecting or obtaining biometric identifiers or information in violation of 740 Ill. Comp. Stat. § 14/15(b) (Count II); and disclosing or disseminating biometric identifiers and information before obtaining consent in violation of 740 Ill. Comp. Stat. § 14/15(d) (Count III).

Amazon has moved to dismiss the first amended complaint in full. [36].

II. Legal Standard

A motion to dismiss tests the sufficiency of a counterclaim, not the merits of the case. *Gunn v. Cont’l Cas. Co.*, 968 F.3d 802, 806 (7th Cir. 2020). To survive a motion to dismiss under Rule 12(b)(6), the counterclaim “must provide enough factual information to state a claim to relief that is plausible on its face and raise a right to relief above the speculative level.” *Haywood v. Massage Envy Franchising, LLC*, 887 F.3d 329, 333 (7th Cir. 2018) (quoting *Camasta v. Jos. A. Bank Clothiers, Inc.*, 761 F.3d 732, 736 (7th Cir. 2014)); *see also* Fed. R. Civ. P. 8(a)(2) (requiring a complaint to contain a “short and plain statement of the claim showing that the pleader is

entitled to relief”). A court deciding a Rule 12(b)(6) motion accepts the well-pleaded factual allegations as true and draws all permissible inferences in the pleading party’s favor. *Degroot v. Client Servs., Inc.*, 977 F.3d 656, 659 (7th Cir. 2020).

Dismissal for failure to state a claim is proper “when the allegations in a complaint, however true, could not raise a claim of entitlement to relief.” *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 558 (2007). Deciding the plausibility of the claim is “a context-specific task that requires the reviewing court to draw on its judicial experience and common sense.” *Bilek v. Fed. Ins. Co.*, 8 F.4th 581, 586–87 (7th Cir. 2021) (quoting *W. Bend Mut. Ins. Co. v. Schumacher*, 844 F.3d 670, 676 (7th Cir. 2016)).

III. Analysis

A. BIPA

The Illinois General Assembly adopted the Biometric Information Privacy Act in 2008 in response to increased commercial use of biometric data. *Cothron v. White Castle Sys., Inc.*, No. 20-3202, --- F.4th ---, 2021 WL 5998537, at *1 (7th Cir. Dec. 20, 2021). The Act protects a person’s privacy interests in his or her biometric identifiers, including fingerprints, retina and iris scans, hand scans, and facial geometry; it does so by regulating the collection use, retention, disclosure, and dissemination of biometric identifiers, providing a cause of action for persons “aggrieved” by a statutory violation. *Fox v. Dakkota Integrated Sys., LLC*, 980 F.3d 1146, 1148 (7th Cir. 2020); *see also Bryant v. Compass Grp. USA, Inc.*, 958 F.3d 617, 620 (7th Cir. 2020), *as amended on denial of reh’g and reh’g en banc* (June 30, 2020). A successful

plaintiff recovers the greater of actual damages or statutory damages of \$1,000 for each negligent violation and \$5,000 for each reckless or willful violation. *Cothron*, 2021 WL 5998537, at *1.

Naughton's first amended complaint implicates three BIPA sections. Section 15(a) requires private entities "in possession of biometric identifiers or biometric information" to "develop a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information." 740 Ill. Comp. Stat. 14/15(a). 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). And section 15(d) provides that a private entity may not "disclose, redisclose, or otherwise disseminate" biometric data without consent. *Id.* § 14/15(d).

B. Sufficiency of Allegations

Amazon attacks the sufficiency of Naughton's allegations on a variety of grounds, but ultimately, none are persuasive under the Rule 12(b)(6) standard.¹

First, Amazon argues that the FAC fails to plausibly state that Amazon purposely collected any data that could qualify as biometric data, thus dooming Naughton's section 15(b) claim. As discussed, section 15(b) makes it unlawful to "collect, capture, purchase, receive through trade, or otherwise obtain" a

¹ Amazon disputes that it collected Biometric Data in the "wellness checks" it conducted on employees via "thermal cameras". (Dkt. 32 at 9). At this stage, the Court is obligated to accept the facts as pled in the complaint as true. Ultimately Plaintiff will have the burden of proving this fact.

person's biometric data without his or her written consent. *Cothron*, 2021 WL 5998537, at *4 (quoting 740 Ill. Comp. Stat. 14/15(b)). Amazon emphasizes that courts in this district have interpreted section 15(b) to impose liability only if an entity takes, at a minimum, "an *active step* to collect, capture, purchase or otherwise obtain biometric data." *Jacobs v. Hanwha Techwin Am., Inc.*, No. 21 C 866, 2021 WL 3172967, at *2 (N.D. Ill. July 27, 2021) (emphasis added); *see also Heard v. Becton, Dickinson & Co.*, 440 F. Supp. 3d 960, 966 (N.D. Ill. 2020) (*Heard I*). Amazon insists that Naughton has not plausibly alleged that is has taken any "active step" to collect his biometric data, citing two cases from this district dismissing section 15(b) claims for omitting such allegations. [37] at 8.

The cases upon which Amazon relies are distinguishable. In *Namuwonge v. Kronos, Inc.*, the district held that the plaintiff failed to allege a plausible section 15(b) claim against a third-party vendor (a timekeeping tracking company) that collected information based on plaintiff clocking in via her fingerprints as required by her employer. 418 F. Supp. 3d 279, 286 (N.D. Ill. 2019). The court reasoned that the complaint's allegations made clear that it was the employer, not the vendor itself, that collected the biometric data. *Id.* To the contrary, in *Heard v. Becton, Dickinson & Co.*, the court originally dismissed a section 15(b) claim against a supplier of fingerprint equipment because the complaint did not explain how the supplier, as opposed to the employer, actively collected the biometric data. 440 F. Supp. 3d 960, 967 (N.D. Ill. 2020) (*Heard I*). The plaintiff in *Heard* filed an amended complaint that the court subsequently found stated a claim under section 15(b) by alleging that the

supplier of the fingerprint equipment “extracts the unique features of that fingerprint to create a user template, and then stores users’ biometric information both on the device *and* in [its] servers.” *See Heard v. Becton, Dickinson & Co.*, 524 F. Supp. 3d 831, 841 (N.D. Ill. 2021) (*Heard II*).

In contrast to *Namuwonge* and consistent with the reasoning of *Heard II*, the first amended complaint here asserts that Amazon collects the data for its own use. The allegations also state that Amazon has imposed this requirement on warehouse workers like Plaintiff as a condition of their employment. By asserting that Amazon itself implemented the facial scans and required workers to submit to these scans as a condition of work, Naughton plausibly alleges Amazon took an “active step” in collecting his biometric data. *See, e.g., King v. PeopleNet Corp.*, No. 21 CV 2774, 2021 WL 5006692, at *8 (N.D. Ill. Oct. 28, 2021) (finding that a complaint adequately alleged a section 15(b) violation by asserting that the plaintiff did not know of or consent to her employer’s collection of her fingerprints during a mandatory onboarding process).

Second, Amazon argues that Naughton insufficiently pleads Amazon’s “possession” of biometric data, thus failing to meet a central element of his section 15(a) and (d) claims. [37] at 10. As Amazon correctly recognizes, these BIPA sections apply only to a private entity “*in possession* of biometric identifiers or biometric information.” 740 Ill. Comp. Stat. 14/15(a), (d) (emphasis added). Amazon contends that Naughton has not adequately alleged that Amazon collected his biometric data and that this failure also necessarily means that Amazon could not have possessed

his biometric data. [37] at 10. Again, this Court disagrees. As explained above, by requiring that Naughton submit to scans disclosing his facial geometry, Amazon has taken the requisite “active step” in collecting, and thus also possessing, the data. Beyond that, Naughton also specifically asserts that Amazon stores his biometric data in a database. [33] ¶ 44. This plainly satisfies the “possession” requirement at the pleadings stage.

Finally, Amazon argues that because Naughton has failed to allege “collection” and “possession” of data, he has also failed to allege that Amazon disclosed any biometric data in violation of section 15(d). [37] at 10–11. For the same reasons as explained above, this Court rejects the notion that Naughton’s allegations fail to satisfy the “collection” and “possession” requirements under the statute. Amazon also contends that Naughton’s section 15(d) falls short because although he claims that Amazon disclosed his biometric data to third parties, he does not more fulsomely allege what data Amazon disclosed, when or where the disclosure occurred, or to whom the disclosure occurred. [37] at 11. But Amazon seeks to impose a heightened standard where there is none; all Naughton must plead is “plausible dissemination.” *Cothron v. White Castle Sys., Inc.*, 467 F. Supp. 3d 604, 618 (N.D. Ill. 2020). He has done so here by indicating that Amazon has collected his facial geometry, disclosed that data to “other Amazon entities” and to “third-party biometric device and software vendor(s)” and other possible third parties. [33] ¶¶ 4, 34. The law does not demand more at the pleadings stage.

IV. Conclusion

For the reasons explained above, this Court denies Amazon's motion to dismiss [36]. Naughton's motion for leave to file a second amended complaint to substitute named plaintiff [48] remains under advisement. The Court will not require Amazon to answer the first amended complaint until after ruling on the pending motion to substitute.

Dated: January 3, 2022

E N T E R:



MARY M. ROWLAND
United States District Judge