

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

**NATASHA R. JONES,**

**Plaintiff,**

v.

**MICROSOFT CORPORATION,**

**Defendant.**

)  
)  
)  
)  
)  
)  
)  
)  
)  
)  
)

**No. 22-cv-3437**

**Judge Jorge L. Alonso**

**Memorandum Opinion and Order**

Plaintiff Natasha Jones filed a complaint alleging that Defendant Microsoft Corp. violated the Illinois Biometric Information Privacy Act (“BIPA”). Jones initially filed her lawsuit in the Circuit Court of Cook County, Illinois, but Microsoft removed it based on diversity jurisdiction and the Class Action Fairness Act, 28 U.S.C. § 1332(d). *See* [1]. Microsoft now moves to dismiss counts II and IV of Jones’s complaint under Federal Rule of Civil Procedure 12(b)(6). Jones also filed a motion to remand counts I and III back to the Circuit Court of Cook County. For the reasons below, the Court grants Jones’s motion [13] and remands Counts I and III to the Circuit Court of Cook County. The Court also grants Microsoft’s motion to dismiss [15] counts II and IV.

**Background**

The Court recounts the following facts from Jones’s complaint. Microsoft provides a service called Azure, a cloud computing and storage platform. Cloud computing services, like Azure, allow users to store and access data through the internet rather than storing it locally.

Jones began working for Chicago Marriott Suites in October of 2015 and worked there for six years. During her employment, Chicago Marriott required its employees to register and scan their fingerprint for timekeeping purposes each time they clocked-in and out at work. To accomplish this, Chicago Marriott hired Paychex, a prominent biometric timekeeping provider in Illinois, to collect and store its employee's biometric data. Paychex hosts a variety of cloud-based apps supported by and stored on Microsoft's Azure platform.

Plaintiff alleges that even though Paychex uploaded her and others' biometric information onto the Azure platform, Microsoft never provided her with, nor did she ever sign, a release acknowledging that it could collect, store, use, or disseminate her biometric data. Nor did Microsoft publish any policies addressing retention or destruction schedules for this data.

### **Discussion**

BIPA imposes certain restrictions on how "private entit[ies]" may collect, retain, use, disclose, and destroy "biometric identifiers" and "biometric information." *See* 740 ILCS 14/15. "Biometric identifier" generally means "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry," apart from various exclusions. 740 ILCS 14/10. "Biometric information" refers to "any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual," except for information derived from "items or procedures excluded under the definition of biometric identifiers." *Id.*

BIPA requires that, before collecting or obtaining an individual's biometric identifiers or information, a private entity must inform the individual in writing that it is collecting his data, 740 ILCS 14/15(b)(1); state the specific purpose of collecting or using the data, 740 ILCS 14/15(b)(2); and state the length of time for which it will collect, store, and use the data, *id.* The

entity must also get a signed “written release” from the individual before collecting their biometric data. 740 ILCS 14/15(b)(3). In addition, the entity must make publicly available the “retention schedule and guidelines” it uses for permanently destroying the biometric identifiers and information it collects. 740 ILCS 14/15(a).

BIPA further prohibits private entities from selling, leasing, trading, or otherwise profiting from a person’s or customer’s biometric identifier or information. 740 ILC 14/15(c). Lastly, BIPA prevents private entities from disclosing, redisclosing, or otherwise disseminating a person’s or customer’s biometric identifiers or information absent consent, a requirement by federal, state, or local law, or in accordance with a valid subpoena. 740 ILCS 14/15(d).

Here, Jones alleges violation of four BIPA provisions: 740 ILCS 14/15(a), (b), (c), and (d). After Microsoft removed this case to federal court, Jones filed a motion to remand her §15(a) and (c) claims. Microsoft stipulated to the remand of those claims but seeks to dismiss the other claims. The Court addresses each motion in turn.

## **I. Motion to Remand**

Jones argues she lacks Article III standing to pursue her §15(a) or §15(c) BIPA claims in federal court. The party invoking federal jurisdiction, which in this case is Microsoft as the removing party, bears the burden of establishing Article III standing. *Collier v. SP Plus Corp.*, 889 F.3d 894, 896 (7th Cir. 2018). To establish Article III standing, the complaint must allege three things: (1) the plaintiff suffered a concrete and particularized injury-in-fact; (2) a causal connection between the plaintiff’s injury and the defendant’s conduct; and (3) a favorable judicial decision is likely to redress the injury. *Fox v. Dakkota Integrated Systems, LLC*, 980 F.3d 1146, 1153 (7th Cir. 2020).

Microsoft, rather than respond to Jones’s substantive arguments, stipulates to severance and remand of the §15(a) and (c) claims. The Court agrees with the parties that Jones’s allegations do not satisfy the requirements of the standing doctrine for those claims, *see Bryant v. Compass Group, USA, Inc.*, 958 F.3d 617, 626 (7th Cir. 2020), *Thornley v. Clearview AI, Inc.*, 984 F.3d 1241, 1247 (7th Cir. 2021), and, in the absence of any argument to the contrary, the Court grants the motion to remand. The Court severs counts I and III of the complaint and remands those counts to the Circuit Court of Cook County.

## **II. Motion to Dismiss**

“A motion under Rule 12(b)(6) tests whether the complaint states a claim on which relief may be granted.” *Richards v. Mitcheff*, 696 F.3d 635, 637 (7th Cir. 2012). Under Rule 8(a)(2), a complaint must include “a short and plain statement of the claim showing that the pleader is entitled to relief.” Fed. R. Civ. P. 8(a)(2). This short and plain statement must “give the defendant fair notice of what the claim is and the grounds upon which it rests.” *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555 (2007) (internal quotation marks and alteration marks omitted). Under federal notice-pleading standards, “a complaint must contain sufficient factual matter, accepted as true, to ‘state a claim to relief that is plausible on its face.’” *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Twombly*, 550 U.S. at 570). “In reviewing the sufficiency of a complaint under the plausibility standard, [courts must] accept the well-pleaded facts in the complaint as true, but [they] ‘need[] not accept as true legal conclusions, or threadbare recitals of the elements of a cause of action, supported by mere conclusory statements.’” *Alam v. Miller Brewing Co.*, 709 F.3d 662, 665-66 (7th Cir. 2013) (quoting *Brooks v. Ross*, 578 F.3d 574, 581 (7th Cir. 2009)).

**A. §15(b)**

Microsoft argues that the Court should dismiss Jones’s §15(b) claim because she does not allege that it took an “active step” to collect or obtain her biometric data and that, in any event, it had no practical way to obtain her consent because it did not have a direct relationship with her. Jones responds that BIPA contains no “active step” requirement, nor must a private entity have a direct relationship with the individual under the statute.

The Court begins its analysis by noting that the Illinois legislature used the term “possession” in certain BIPA sections but not in §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, 227 Ill. Dec. 179, 687 N.E.2d 102 (1st Dist. 1997). Thus, §15(b) does not penalize merely possessing biometric identifiers or information, unlike other BIPA sections. *Compare* 740 ILCS 14/15(b) *with* 740 ILCS 14/15(a), (c), (d). The Court is persuaded of this principle both by the statute’s plain language as well as the fact that many other judges, including those within in this district, have reached the same conclusion. *See Stauffer v. Innovative Heights Fairview Heights, LLC*, Case No. 20-cv-046, 2022 WL 3139507, at \*3-4 (S.D. Ill. Aug. 5, 2022); *Ronquillo v. Doctor’s Assoc., LLC*, Case No. 21-cv-4903, 2022 WL 1016600, at \*2 (N.D. Ill. April 4, 2022); *Patterson v. Respondus, Inc.*, 593 F. Supp. 3d 783, 824 (N.D. Ill. 2022); *King v. PeopleNet Corp.*, 21-cv-2774, 2021 WL 5006692, at \*8 n.11 (N.D. Ill. Oct 28, 2021); *Jacobs v. Hanwha Techwin Am., Inc.*, Case No. 21-cv-866, 2021 WL 3172967, at \*2 (N.D. Ill. July 27, 2021); *Heard v. Becton, Dickinson & Co.*, 440 F. Supp. 3d 960, 965 (N.D. Ill. 2020) (“*Heard P*”); *Namuwonge v. Kronos, Inc.*, 418 F. Supp. 3d 279, 286 (N.D. Ill. 2019).

Having determined that §15(b) requires something beyond possession, the inquiry turns to what that is. Section 15(b) states 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” absent consent. 740 ILCS § 14/15(b). Under a commonsense reading, this means that the private entity must undertake some effort to collect or obtain biometric identifiers or information. Courts sometimes refer to this as an “active step” requirement. *See Heard I*, 440 F. Supp. 3d at 966; *Jacobs*, 2021 WL 3172967, at \*2. Although BIPA does not say the words “active step,” this concept simply describes the unifying characteristic among the verbs in the statute.

Indeed, even the catch-all phrase “otherwise obtain” contemplates some type of affirmative effort. *See Obtain*, BLACK’S LAW DICTIONARY (11th ed. 2019) (“defining “obtain” as “[t]o bring into one’s own possession; to procure, *esp. through effort.*”) (emphasis added). What’s more, the Court agrees with Microsoft that when a statutory clause specifically describes several classes of things and then includes “other persons or things,”—or in this case, the analogous phrase “otherwise obtain”—the word “other” should be interpreted to mean “other such like.” *See Pooh-Bah Enterprises, Inc., v. County of Cook*, 232 Ill. 2d 463, 492 (2009). Thus, the Court interprets the phrase “otherwise obtained” in line with “collect,” “capture,” “purchase,” and “receive through trade”—all of which denote some affirmative act taken in furtherance of collection.

Jones argues that the Court should reject the “active step” idea and cites to *Heard v. Becton, Dickinson & Co.*, 524 F. Supp. 3d 831 (N.D. Ill. 2021) (“*Heard II*”), *Figueroa v. Kronos, Inc.*, 454 F. Supp. 3d 772 (N.D. Ill. 2020), and *Rogers v. BNSF Railway Co.*, 19-cv-3083, 2022 WL 4465737 (N.D. Ill. Sept. 26, 2022). But these cases do not support her position.

In *Heard II*, rather than reject the idea of an active step, the court ruled that the amended complaint established that the defendant played an active role in collecting and obtaining users' biometric information. 524 F. Supp. 3d at 841. Similarly, in *Figueroa*, the court acknowledged that the defendant made the necessary active step by providing biometric timekeeping devices and storing the scanned data on its databases. 454 F. Supp. 3d at 779. And lastly, in *Rogers*, the judge acknowledged that one must "do something" to violate §15(b). [27-1] at pg. 5 ("You have to have done something. 'Collecting' is doing something. 'Capturing' is doing something. 'Purchasing' is doing something. 'Receiving through trade' is doing something. 'Otherwise obtained' is doing something."). None of these cases say anything in conflict with the idea that a defendant must take some affirmative step in furtherance of collecting, capturing, purchasing, receiving through trade, or obtaining biometric identifiers or information.

But the Court's analysis does not end here because Jones also argues, in the alternative, that even if §15(b) requires an active step, Microsoft's conduct satisfies that requirement. She argues that Microsoft "received through trade" and/or "otherwise obtained" her biometric identifiers and information. The Court disagrees. The complaint makes clear that Paychex provided the biometric timekeeping services to Jones's employer, [1-1] at ¶40; Paychex registered and scanned Jones's fingerprint, *Id.*; and Paychex utilized and sent the data to Microsoft's Azure platform, [1-1] at ¶¶28, 39-41.

To be sure, Microsoft contracted with Paychex to provide access to its cloud computing storage platform. But this act, unlike like those in the cases cited by the parties, does not constitute an active step or affirmative act on Microsoft's part to get, acquire, or obtain Jones's biometric data. For contrast, consider *Heard II*. There, the plaintiff alleged that when a user enrolled in the defendant's system, the user's fingerprints were scanned and extracted to create a

template that was stored on both on the device and defendant's servers. *Heard II*, 524 F. Supp. at 841. Thus, the biometric collection technology, supplied by the defendant, not only collected but automatically uploaded that data to defendant's servers. And in *Figueroa*, the defendant also supplied the biometric timekeeping devices, which stored the collected data on its servers. 454 F. Supp. 3d at 779.

Microsoft's situation is different. It was merely a vendor to the third-party that provided the biometric timekeeping technology and services to Jones's employer. Although several courts have extended BIPA to apply to third-party providers that supply biometric collection technology and services, no case has extended BIPA to vendors for such third-party providers. *See, e.g., Smith v. Signature Sys., Inc.*, Case No. 21-cv-02025, 2022 WL 595707, at \*4 (N.D. Ill. Feb. 28, 2022)) (complaint alleged active steps of collection by alleging that the POS system vendor scanned and collected copies of its client's employees' fingerprints and then compared them to those stored in the database); *Heard II*, 524 F. Supp. 3d at 841; *Figueroa*, 454 F. Supp. 3d at 783–84 (N.D. Ill. 2020); *Ronquillo* 597 F. Supp. at 1230 (alleging that defendant required franchisees to use its proprietary biometric scanning hardware and software).

Microsoft stands a step removed from those companies providing biometric collection software and hardware. Instead, Microsoft provided Paychex with one component (storage) that it used as part of its system for collecting and storing biometric data. But the allegations make clear that Paychex put these various pieces together to create the system necessary to collect and store Jones's biometric data. Nor does the Court see how the transaction between Paychex and Microsoft demonstrates that Microsoft received Jones's biometric data "through trade." Microsoft received money in exchange for access to its product, not biometric data.



Jones further argues that Microsoft made the requisite active step because to possess her biometric information it necessarily had to obtain it first. This logic seems circular. And in any event, the allegations explain how Microsoft came to possess Jones's biometric data without collecting or obtaining it. More specifically, Paychex sent the data to Microsoft's cloud storage platform. As a result, because Microsoft did not obtain or receive Jones's biometric data through trade, the Court dismisses count II.

**B. §15(d)**

The Court also dismisses Jones's §15(d) claim. All her allegations regarding disclosure, redisclosure, or dissemination parrot BIPA's language. *See* [1-1] at ¶90 ("As alleged herein, after Plaintiff's and other Class members' biometric identifiers were obtained by Defendant through its clients' platforms, Defendant disclosed or otherwise disseminated their biometrics"); *Id.* at ¶91 ("Defendant never obtained Plaintiff's or other Class members' consent to disclose or disseminate their biometrics."). Without more factual support, this claim must fail. *See Namuwonge*, 418 F. Supp. 3d at 285 (dismissing §15(d) claim when plaintiff "pleaded on information and belief that [the defendant]...disclosed her fingerprints to other third parties that host the data").

Jones argues that her allegations mirror those in *Heard II* and *Figueroa*, which survived the initial pleading stage. But these cases are distinguishable. In *Heard II*, the plaintiff affirmatively alleged that the defendant disclosed the biometric information it possessed to third-party data centers. 524 F. Supp. 3d at 843. Likewise, in *Figueroa*, the plaintiff alleged that the defendant disseminated her biometric data to other firms that hosted the information in their data centers. 454 F. Supp. 3d at 785. Here, however, Jones makes no such allegations. Unlike *Heard*

*II* and *Figueroa*, Jones does not allege that Microsoft disseminated her biometric data to any third-party data centers or any tangible third parties whatsoever. This claim, therefore, fails.

### **Conclusion**

For the reasons above, the Court grants Microsoft's motion to dismiss [15]. The Court grants Jones' motion to remand [13] and remands Counts I and III to the Circuit Court of Cook County. Civil case terminated.

**SO ORDERED.**

**ENTERED: January 9, 2023**

A handwritten signature in black ink, consisting of a large, stylized 'J' and 'A' with a horizontal line through them, enclosed within a large, loopy oval shape.

---

**HON. JORGE ALONSO**  
**United States District Judge**