UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

MARIEL RONQUILLO, individually and on Behalf of all others similarly situated,	)	
Plaintiff,	)	
	)	No. 21 C 4903
v.	)	
	)	Judge Sara L. Ellis
DOCTOR’S ASSOCIATES, LLC, and HP INC.,	)	
Defendants.	)	

OPINION AND ORDER

Plaintiff Mariel Ronquillo worked at a Subway restaurant in Illinois that used a point-of-sale (“POS”) system, comprised of hardware owned by Defendant HP Inc. (“HP”) and POS software licensed by Defendant Doctor’s Associates, LLC (“DAL”). Ronquillo used the POS system to clock in and out of her shifts and breaks, as well as to unlock the registers. She filed this putative class action lawsuit alleging that HP and DAL violated § 15(b) of the Illinois Biometric Information Privacy Act (“BIPA”), 740 Ill. Comp. Stat. 14/15(b), because they collected and obtained her biometric information without providing her with the required notice and obtaining her written consent. HP and DAL have separately moved to dismiss Ronquillo’s claims pursuant to Federal Rule of Civil Procedure 12(b)(6). Because Ronquillo has sufficiently alleged a violation of § 15(b) by HP and DAL and need not plead her request for enhanced statutory damages with particularity, the Court denies the motions to dismiss.

BACKGROUND[1]

DAL is the American franchisor for Subway restaurants. DAL requires its franchisees to use its Restaurant Technology as a Service ("RTaaS") POS system. The RTaaS system includes a proprietary POS software system, SubwayPOS, that DAL licenses to its franchisees. HP, which manufactures and sells personal computers, printers, and other hardware, including restaurant POS equipment, provides the hardware, including an integrated biometric scanner, for the RTaaS POS system. Subway franchisees pay monthly fees to lease the POS equipment from HP, with HP retaining ownership of the POS equipment. SubwayPOS integrates with the HP biometric scanner, with the software and hardware (collectively, the "Biometric System") allowing employees to unlock registers, as well as clock in and out of shifts and breaks, with their fingerprints. Upon first use of the Biometric System, DAL uses the SubwayPOS to capture a worker's fingerprint and create a reference template, or algorithmic representation of the fingerprint's features. SubwayPOS stores the reference templates and other information identifying the workers in a database on the POS hardware. Every subsequent time a worker uses the Biometric System, DAL uses the SubwayPOS to capture the fingerprint and compare it to the stored reference templates to identify the worker.

Ronquillo worked at a Subway restaurant at 6559 N. Sheridan Road in Chicago, Illinois. The Subway restaurant at which Ronquillo worked used the Biometric System, including the hardware owned by HP and the SubwayPOS software licensed by DAL. Ronquillo used the Biometric System to clock in and out of her shifts and breaks, as well as to unlock the POS system, with her reference template and identifying information stored on that system. DAL and HP did not explain the Biometric System, how they use the data collected through the Biometric

[1] The Court takes the facts in the background section from Ronquillo's complaint and presumes them to be true for the purpose of resolving Defendants' motions to dismiss. *See Phillips v. Prudential Ins. Co. of Am.*, 714 F.3d 1017, 1019–20 (7th Cir. 2013).

System, or how long they keep the collected data to Ronquillo or other Subway employees. Ronquillo did not consent to the capture, collection, use, or retention of her biometric information.

LEGAL STANDARD

A motion to dismiss under Rule 12(b)(6) challenges the sufficiency of the complaint, not its merits. Fed. R. Civ. P. 12(b)(6); *Gibson v. City of Chicago*, 910 F.2d 1510, 1520 (7th Cir. 1990). In considering a Rule 12(b)(6) motion, the Court accepts as true all well-pleaded facts in the plaintiff's complaint and draws all reasonable inferences from those facts in the plaintiff's favor. *Kubiak v. City of Chicago*, 810 F.3d 476, 480–81 (7th Cir. 2016). To survive a Rule 12(b)(6) motion, the complaint must assert a facially plausible claim and provide fair notice to the defendant of the claim's basis. *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009); *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555 (2007); *Adams v. City of Indianapolis*, 742 F.3d 720, 728–29 (7th Cir. 2014). A claim is facially plausible "when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Iqbal*, 556 U.S. at 678.

ANALYSIS

I. Sufficiency of the Allegations

Ronquillo claims that DAL and HP violated § 15(b) of BIPA, which requires private entities that "collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifier or biometric information" to first obtain the individual's informed, written consent. 740 Ill. Comp. Stat. 14/15(b). Ronquillo alleges that DAL and HP violated § 15(b) by (1) failing to inform her that they collected, stored, and used her biometric information; (2) failing to inform her of the specific purpose for the collection, storage, and use, as well as the length of time they would retain her biometric information; and (3) failing to obtain a written release authorizing the collection, receipt through trade, or other obtainment of her biometric information. DAL and HP argue, however, that § 15(b) does not apply to them because Ronquillo has not alleged that they *actively* collected, received through trade, or otherwise obtained her biometric information, with the complaint instead suggesting that her employer, an unnamed Subway franchisee, collected and stored that information instead. At most, DAL and HP maintain that the complaint indicates that they possessed her biometric information, which does not suffice to support a § 15(b) violation.

Indeed, as DAL and HP point out, courts have recognized that possession of biometric data alone does not subject an entity to § 15(b)'s requirements. *See King v. PeopleNet Corp.*, No. 21 CV 2774, 2021 WL 5006692, at *8 (N.D. Ill. Oct. 28, 2021) ("§ 15(b) doesn't penalize mere possession of biometric information."); *Heard v. Becton, Dickinson & Co.* ("*Heard I*"), 440 F. Supp. 3d 960, 965–66 (N.D. Ill. 2020) ("Unlike Sections 15(a), (c), (d), and (e) of the BIPA—all of which apply to entities 'in possession of' biometric data—Section 15(b) applies to entities that 'collect, capture, purchase, receive through trade, or otherwise obtain' biometric data. Recognizing this distinction, the parties agree that mere possession of biometric data is insufficient to trigger Section 15(b)'s requirements." (citations omitted)); *Namuwonge v. Kronos, Inc.*, 418 F. Supp. 3d 279, 286 (N.D. Ill. 2019) ("[T]here is a difference between *possessing* and *collecting* biometric information."). Thus, a number of courts have concluded that, for § 15(b) to apply, the defendant must take active steps to collect, capture, or otherwise obtain the plaintiff's biometric information. *See, e.g.*, *Jacobs v. Hanwha Techwin Am., Inc.*, No. 21 C 866, 2021 WL 3172967, at *2 (N.D. Ill. July 27, 2021) ("[P]laintiff agrees that Section 15(b) requires something more than mere possession, but is unable to articulate what that 'something more' is, if not an affirmative act of collection. . . . Following other courts in this district, this court concludes that for Section 15(b)'s requirements to apply, an entity must, at a minimum, take an active step to collect, capture, purchase, or otherwise obtain biometric data."); *Heard I*, 440 F. Supp. 3d at 966 ("[F]or Section 15(b)'s requirements to apply, an entity must, at a minimum, take an active step to 'collect, capture, purchase, receive through trade, or otherwise obtain' biometric data." (citation omitted)).

Although Ronquillo disagrees that § 15(b) requires an active step, the Court need not resolve the question here. Even assuming that Ronquillo must plead that DAL and HP took an active step to collect, capture, or otherwise obtain her biometric information, Ronquillo's complaint adequately sets forth how DAL and HP did so. Specifically, Ronquillo alleges that DAL uses the SubwayPOS system, which it exclusively controls, to capture workers' fingerprints and create the reference templates. Doc. 1 ¶¶ 19, 33, 63–66. And Ronquillo further alleges that HP stores the reference templates on its hardware, which DAL then compares to scanned fingerprints to identify the workers. *Id.* ¶¶ 20, 34, 35, 54, 55. These allegations allow for the inference that DAL and HP took active steps to obtain Ronquillo's biometric information. *See Smith v. Signature Sys., Inc.*, No. 2021-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 v. Becton, Dickinson & Co.* ("*Heard II*"), 524 F. Supp. 3d 831, 841 (N.D. Ill. 2021) (plaintiff sufficiently alleged active steps by alleging that "when a user enrolls in the Pyxis system, the device scans the user's fingerprint, extracts the unique features of that fingerprint to create a user template, and then stores users' biometric information both on the device *and* in [defendant's] servers"); *Figueroa v. Kronos Inc.*, 454 F. Supp. 3d 772, 783–84

(N.D. Ill. 2020) (allegations that the defendant stored data sufficed for § 15(b) liability because in order to store data, the defendant "necessarily first had to 'obtain' the data").

DAL and HP nonetheless argue that only Ronquillo's actual employer, the unnamed Subway franchisee, captured and obtained her biometric information. But in doing so, they attempt to rewrite the complaint to avoid its actual allegations, which allow for the reasonable inference that DAL and HP played more than a passive role in the process. *See King*, 2021 WL 5006692, at *8 ("[I]t's reasonable to infer that PeopleNet, not its client-employers, was doing the capturing and obtaining of King's biometric information."); *cf. Jacobs*, 2021 WL 3172967, at *3 & n.2 (no active step where "a complete reading of the complaint makes clear that defendant is merely a third-party technology provider (that is, merely provided the cameras), and that the active collector and processor of the data is T.J. Maxx" and does not suggest that the third party itself "collected, obtained, or stored the biometric data"); *Bernal v. ADP, LLC*, No. 2017-CH-12364, 2019 WL 5028609, at *2 (Ill. Cir. Ct. Aug. 23, 2019) ("Plaintiff has failed to allege facts sufficient enough for the Court to properly assess Defendant's actual involvement, relative to the biometric scanning technology, beyond the fact that Defendant supplied Rockit with the technology. In order for the Court to determine whether or not § 15(b) is applicable here, Plaintiff's Complaint must include factual allegations of what Defendant's role relative to Plaintiff's biometric information is."). That suffices at this stage to plead that § 15(b) applies to DAL and HP. The Court leaves the question of whether Ronquillo will actually be able to prove DAL and HP's role in collecting and obtaining her biometric information for another day on a more developed record. *See Smith*, 2022 WL 595707, at *5 ("While a defendant 'may ultimately prevail' through discovery or trial on the point that it is the employer, not the defendant, that stores users' biometric information on their own systems and servers, the plaintiff 'is not required to prove the merits of his claims at the pleading stage.'" (quoting *Heard II*, 524 F. Supp. 3d at 841)).

II. Section 15(b)'s Applicability to Third-Party Vendors

Alternatively, DAL and HP argue that § 15(b) does not apply to third-party vendors of technology an employer uses to obtain its employees' biometric information, contending that extending § 15(b)'s reach to such parties does not further BIPA's purpose and instead creates absurd results. *See Bernal*, 2019 WL 5028609, at *1 ("While Plaintiff correctly contends that BIPA can be applied outside of an employment situation, there is nothing to suggest that BIPA was intended to apply to situations wherein the parties are without any direct relationship. . . . [T]o read BIPA as requiring that a third party provider of the biometric timeclock technology, without any direct relationship with its customers' employees, obtain written releases from said employees would be unquestionably not only inconvenient but arguably absurd."). But *Bernal* appears to be an outlier, with the language on which DAL and HP rely appearing only in *dicta*. *See Heard II*, 524 F. Supp. 3d at 843 ("The *Bernal* court's decision rested not on the inapplicability of Section 15(b) to third-party vendors, but on the insufficiency of the plaintiff's complaint on that count."). More importantly, DAL and HP cannot point to anything in BIPA's text that supports limiting § 15(b)'s reach only to employers. *See Neals v. PAR Tech. Corp.*, 419 F. Supp. 3d 1088, 1092 (N.D. Ill. 2019) ("no textual support whatsoever" exists for "the proposition that the BIPA exempts a third-party non-employer collector of biometric information when an action arises in the employment context"). True, BIPA does define "written release," used in § 15(b)(3), as "informed written consent or, in the context of employment, a release executed by an employee as a condition of employment." 740 Ill. Comp. Stat. 14/10. But this more specific definition of what constitutes a written release in the employment context does not negate the broader definition or otherwise restrict § 15(b)'s reach. *Neals*, 419 F. Supp. 3d at 1092; *see also Flores v. Motorola Sols., Inc.*, No. 1:20-cv-01128, 2021 WL 232627, at *3 (N.D. Ill. Jan. 8, 2021) (rejecting argument that Section 15(b)'s written consent requirement "only applies where an information collector has some relationship with the individual and has an opportunity to perform the written exchange of notice"). Nor does imposing § 15(b)'s written consent requirement on third-party vendors create absurd results. Contrary to DAL and HP's arguments of impossibility, they "could have complied by, for example, requiring [Ronquillo's] employer[ ], as a contractual precondition of using [DAL and HP's] biometric timekeeping device, to agree to obtain [its] employees' written consent to [DAL and HP] obtaining their data." *Figueroa*, 454 F. Supp. 3d at 783; *see also King*, 2021 WL 5006692, at *9 ("It's not absurd to read § 15(b) as applicable to vendors as well as employers. A waiver imposes a minor compliance cost and does not threaten BIPA's underlying purposes." (citations omitted)). Further, even if the written release requirement only applied to employers, "[s]ince the release is just one of the requirements imposed by § 15(b), the employment context of [Ronquillo's] case doesn't excuse [DAL and HP] from informing [Ronquillo] that it was collecting her biometrics, explaining why it was using her information, and for how long." *King*, 2021 WL 5006692, at *9; *Heard II*, 524 F. Supp. 3d at 842 ("[E]ven if [a third-party vendor] is not required to obtain a written release from end users, it is still subject to Section 15(b)(1) and (2)."). Thus, the Court cannot conclude that DAL and HP may escape liability under § 15(b) because they do not have a direct employment relationship with Ronquillo.

III. Extraterritoriality Doctrine

HP also argues that the extraterritoriality doctrine bars Ronquillo's claim against it because she seeks to apply BIPA to a non-Illinois resident. Under Illinois law, "a statute is without extraterritorial effect unless a clear intent in this respect appears from the express provisions of the statute." *Avery v. State Farm Mut. Auto. Ins. Co.*, 216 Ill. 2d 100, 184–85 (2005). Because "none of BIPA's express provisions indicates that the statute was intended to have extraterritorial effect . . . . BIPA does not apply extraterritorially." *Monroy v. Shutterfly, Inc.*, No. 16 C 10984, 2017 WL 4099846, at *5 (N.D. Ill. Sept. 15, 2017). To avoid the extraterritoriality doctrine, "the circumstances that relate to the disputed transaction [must have] occur[red] primarily and substantially in Illinois." *Avery*, 216 Ill. 2d at 187. Here, although HP is a non-resident defendant, Ronquillo alleges that she scanned her fingerprints at a Subway restaurant in Illinois, which leased HP's hardware, and that this hardware, located on site in Illinois, stored her fingerprints. These allegations suffice to suggest that the alleged BIPA violations took place "primarily and substantially in Illinois." *See Smith*, 2022 WL 595707, at *3 (extraterritoriality doctrine did not bar claim where complaint alleged that BIPA violations occurred in Illinois); *Patel v. Facebook, Inc.*, 932 F.3d 1264, 1276 (9th Cir. 2019) ("[I]t is reasonable to infer that the General Assembly contemplated BIPA's application to individuals who are located in Illinois, even if some relevant activities occur outside the state."); *cf. Neals*, 419 F. Supp. 3d at 1091 ("[I]n light of the fact that Neals does not specify the location of the Charley's Philly Steaks at which she worked, the Court is unable to reasonably infer from the complaint that her fingerprint was collected in Illinois. If plaintiff were able to so allege, then she would sufficiently allege facts indicating that the circumstances relating to the alleged transaction occurred primarily and substantially in Illinois; the transaction would allegedly involve an Illinois resident having her biometric information collected in Illinois by a private entity, without the entity's having provided the requisite disclosures and obtained the requisite consent there.").

IV. Enhanced Statutory Damages

Finally, DAL and HP argue that the Court should strike Ronquillo's request for enhanced statutory damages under BIPA because she has not sufficiently pleaded that DAL and HP acted intentionally or recklessly. BIPA provides that a plaintiff may recover statutory damages of $1,000 for negligent violations and $5,000 for intentional or reckless violations. 740 Ill. Comp. Stat. 14/20(1)–(2). But the need to demonstrate negligence, intentional action, or recklessness impacts a plaintiff's recovery, not the underlying substantive BIPA violation. *See Rosenbach v. Six Flags Entm't Corp.*, 2019 IL 123186, ¶¶ 33, 36 ("[W]hen a private entity fails to comply with one of section 15's requirements, that violation 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 breach. . . . The violation, in itself, is sufficient to support the individual's or customer's statutory cause of action."); *see also Smith*, 2022 WL 595707, at *5 ("[A]llegations of scienter or no, [the] complaint states a plausible claim for relief under sections 15(b) and 15(d); Rule 12(b)(6) does not require her to plead the facts that will determine the amount of actual damages she may be entitled to recover." (second alteration in original) (quoting *Cothron v. White Castle Sys., Inc.*, 467 F. Supp. 3d 604,615 (N.D. Ill. 2020))); Fed. R. Civ. P. 8(a)(3) (requiring a plaintiff to plead only "a demand for the relief sought"). Thus, the Court defers the question of whether Ronquillo has the right to recover enhanced damages based on DAL and HP's allegedly reckless and intentional conduct to a later date.

CONCLUSION

For the foregoing reasons, the Court denies DAL and HP's motions to dismiss [15], [20].

Dated: April 4, 2022

SARA L. ELLIS
United States District Judge