

**IN THE CIRCUIT COURT OF COOK COUNTY, ILLINOIS
CHANCERY DEPARTMENT, FIRST DISTRICT**

ROBIN RAPAI,)
)
 Plaintiff,)
 v.)
)
 HYATT CORPORATION d/b/a THE HYATT)
 LODGE,)
)
 Defendant/Third-Party Plaintiff,)
 v.)
)
 KRONOS INCORPORATED,)
)
)
 Third-Party Defendant.)

Case No. 2017 CH 14483
Judge Anna Helen Demacopoulos

**KRONOS INCORPORATED’S MEMORANDUM IN SUPPORT OF
ITS MOTION TO DISMISS HYATT’S THIRD-PARTY COMPLAINT**

This baseless third-party lawsuit was filed for one reason – Hyatt is seeking to blame Kronos Incorporated (“Kronos”), a timekeeping technology vendor – for Hyatt’s own alleged failure to comply with the Illinois Biometric Information Privacy Act (BIPA), 740 ILCS 14/1 *et seq.* Hyatt’s claims against Kronos are not supported by the parties’ contract and basic principles of contractual interpretation, by BIPA, or by the Court’s prior rulings in this case. Hyatt’s third-party complaint should be dismissed in its entirety for the reasons set forth herein.

In October 2017, former Hyatt employee Robin Rapai brought suit against her employer, Defendant/Counter-Plaintiff Hyatt Corporation (“Hyatt”), for its alleged failure to comply with the Illinois Biometric Information Privacy Act (“BIPA”), 740 ILCS 14/1 *et seq.*, in collecting, storing, and using her biometric data to track her time (the “Rapai Lawsuit”). Rapai alleges that Hyatt required her and other employees “to provide [it] with their fingerprint” through use of finger-scan time clocks. (*Rapai Compl.* ¶ 23.) Hyatt then allegedly stored the finger-scan data “in its employee

FILED DATE: 3/22/2022 4:46 PM 2017CH14483

database” without ever complying with BIPA. (*Id.* ¶¶ 24-27.) She brought claims against Hyatt under BIPA sections 15(a) and 15(b). (*Id.* ¶¶ 39-42.) Section 15(a) requires an entity “in possession” of biometric data to develop and adhere to a publicly available data retention policy. 740 ILCS 14/15(a). Section 15(b) requires an entity to procure informed written consent from the data subject before collecting or capturing their biometric data. § 15(b). “[I]n the employment context,” the duty to procure a written release falls on the employer. § 10.

On January 26, 2022, the Court granted Final Approval to a class-wide settlement agreed to by the Rapai plaintiff and Hyatt. In that settlement, Hyatt settled—without an admission of liability—the claims of “[a]ll individuals who (1) scanned their finger into [Hyatt’s] Timekeeping System during the Class Period, and (2) were not subject to a collective bargaining agreement with [Hyatt] during the Class Period.” (Final Approval Order at 2). The release in the Settlement Agreement explicitly excluded a release of any settlement class members’ claims against Kronos. (Ex. A, Settlement Agmt. at ¶ 43).

Despite the settlement of the claims against it, Hyatt is continuing to pursue its Amended Third-Party Complaint (“Compl.”) against Kronos—the timekeeping and payroll services vendor from whom Hyatt bought the time clocks—on the theory that Kronos agreed, as part of the Sales, Software License and Services Agreement (Ex. 2 to Compl.) (the “Contract”), to indemnify Hyatt against BIPA liability. (Compl. ¶¶ 26-29.) Hyatt claims that Kronos agreed to (1) “process” certain types of personal data on its behalf; (2) do so in compliance with applicable laws; and (3) indemnify Hyatt against any claims brought against Hyatt “arising out of or relating to” any compliance failures. (*Id.*) Hyatt apparently believes that, because Kronos agreed to “process” certain information on its behalf, Hyatt itself “never collected, captured, received, obtained, or transferred the data inputted into the . . . time clock devices” and that, as such, “any liability found

in favor of Plaintiff in the Rapai Lawsuit was caused by and is the responsibility of Kronos.” (*Id.* ¶¶ 29-30.) Hyatt now brings claims for breach of contract (Count I), declaratory judgment (Count II), and implied indemnity (Count III). (*Id.* ¶¶ 34-64.)

The Contract supports none of this. As explained herein, the Contract was a straightforward sales and licensing agreement under which Kronos sold time clocks to Hyatt, who then implemented them in their hotel locations to collect employee data for timekeeping purposes. Hyatt then would store its data on a cloud database hosted by Kronos. At all times and as specified in the Contract, Hyatt retained control over and ownership of its employees’ data. Hyatt also misconstrues the Contract’s indemnification provisions. Read properly, the Rapai Lawsuit does not trigger Kronos’s indemnification duties.

In Illinois, “indemnity contracts . . . will not be construed as indemnifying against a party’s own negligence unless such a construction is required by the clear and explicit language of the contract.” *Pekin Ins. Co. v. Designed Equip. Acquisition Corp.*, 2016 IL App (1st) 151689, ¶ 25. The clear and explicit language of the Contract bars such a construction in this case. Kronos did not agree to undertake compliance on Hyatt’s behalf or otherwise indemnify Hyatt against its own negligent failure to comply with BIPA when using the time clocks. Hyatt alone is responsible for its own duties under BIPA. The Amended Third-Party Complaint must be dismissed.

LEGAL STANDARD

“A section 2-615 motion to dismiss attacks the legal sufficiency of the complaint.” *Kata v. City of Chicago*, 2018 IL App (1st) 162075-U, ¶ 12. Dismissal is proper if the allegations in the complaint do not state a cause of action upon which relief may be granted. *Id.* In ruling on a motion to dismiss, courts consider only well-pled facts and “need not accept conclusions of law or conclusory allegations unsupported by specific facts.” *Id.*

ARGUMENT

I. **COUNT I (BREACH OF CONTRACT) AND COUNT II (DECLARATORY JUDGMENT) SHOULD BE DISMISSED.**

Hyatt's claims for breach of contract (Count I) and declaratory judgment (Count II) ignore BIPA's requirements and rely on a mangled construction of the Contract. Under the Contract, Hyatt purchased Kronos' timekeeping systems to use at its own designated hotel locations. After collecting the data through use of the Kronos time clocks, Hyatt would transfer the data for storage on the Kronos cloud where Hyatt could interact with the data through the software it licensed from Kronos. (*See* Contract §§ 1, 4; Ex. B to Contract.) Importantly, Hyatt retained ownership of and control over the employee data at all times. (*Id.* §§ 25(a)(iii)-(iv).) Kronos did not agree to assume Hyatt's legal obligations under BIPA; Hyatt was and remains responsible for its own BIPA compliance in connection with its handling of the data and cannot pawn off liability for its own compliance failures. For the reasons that follow, both Count I and Count II must be dismissed.

A. **Hyatt is responsible for its own BIPA compliance.**

The sole entity that owes any BIPA duties to Hyatt employees for Hyatt's actions is Hyatt itself. BIPA governs any private entity that collects, captures, obtains, or possesses biometric data. *See* 740 ILCS14/15. The Rapai Lawsuit alleges that Hyatt collected and possessed Rapai's biometric data (*see Rapai* Compl. ¶¶ 8, 23-27, 37) and seeks redress for Hyatt's alleged failure to comply with BIPA sections 15(a) and 15(b) in so doing. (*Id.* ¶¶ 26-27, 41-42.)

BIPA itself and recent case law both make clear that in this context, Hyatt alone is responsible for complying with section 15(a) and section 15(b). Section 15(a) requires "a private entity in possession" of biometric data to develop a publicly available policy establishing guidelines for the retention and destruction of biometric data. 740 ILCS 14/15(a). Section 15(a) also requires that the entity actually comply with its policy. *See id.* Section 15(a) thus is quite

straightforward: when an employer (like Hyatt) possesses its employees' biometric data, it must develop—and actually adhere to—a data retention policy. In *Rogers v. CSX Intermodal Terminals, Inc.*, for example, a truck driver brought BIPA claims against his employer, a rail terminal operator. 2019 WL 4201570, at *1 (N.D. Ill. Sept. 5, 2019). Plaintiff alleged that CSX collected and possessed his data and had failed to publish a section 15(a) policy. *Id.* The court found that plaintiff had adequately pled a claim: his employer possessed his data yet never complied with section 15(a). *Id.* at *3-4. Rapai's allegations against Hyatt are identical. (*See Rapai Compl.* ¶¶ 8, 23-27, 37.) If the allegations are true, Hyatt owed Rapai duties under section 15(a) to publish and adhere to a data retention policy.

The same is true of section 15(b), which bars private entities from collecting, capturing, purchasing, receiving through trade, or otherwise obtaining an individual's biometric data without first obtaining informed written consent from the individual. 740 ILCS 14/15(b). The Rapai Lawsuit alleges that Hyatt did just that: Hyatt "collected, captured, stored, or obtained" Rapai's biometric data by "requir[ing] her to scan her fingerprint before beginning her job functions." (*Rapai Compl.* ¶¶ 25, 42.) If true, Hyatt indeed owed her notice and consent duties under section 15(b). In contrast, the *Rapai* Complaint does not mention Kronos or allege that Kronos owed Rapai any duties under BIPA.

In the employment context, moreover, the employer owes notice and consent duties. Section 15(b) mandates that an entity receive a "written release" from the individual before collecting their biometric data. 740 ILCS 14/15(b). In turn, section 10 clarifies that "in the context of employment," the term "'written release' means . . . a release executed by an employee as a condition of employment." 740 ILCS 14/10 (emphasis added). As multiple Illinois state courts have held, this language clearly delegates notice and consent duties exclusively to the employer

where, as here, biometric data is collected in the context of employment. *See Cameron v. Polar Tech Indus., Inc.*, No. 2019-CH-000013 (Cook Cty. Ill. Cir. Ct., dismissed Aug. 23, 2019), at 33 (Ex. B) (dismissing section 15(b) claim against time clock vendor with prejudice because, in the employment context, section 15(b) “only applies to an employer and not a third party”); *Bernal v. ADP, LLC*, No. 2017-CH-12364 (Ill. Cir. Ct., dismissed Aug. 23, 2019), at 2 n.3 (Ex. C) (dismissing section 15(b) claim against time clock vendor because vendor was “not Plaintiff’s employer,” and “BIPA’s definition of ‘written release’ clearly limits its applicability, in the context of employment, to the relationship that exists between employer and employee”). Likewise, in *Namuwonge v. Kronos, Inc.*, a federal district court recently confirmed that when an employer uses a finger-scan time clock in the employment context, **only** the employer—not the time clock vendor—owes section 15(b) duties. 2019 WL 6253807, at *5 (N.D. Ill. Nov. 22, 2019). The *Namuwonge* court found that in this scenario—the same one alleged in the Rapai Lawsuit—only the employer is “collecting biometric information” and thereby accruing notice and consent duties under section 15(b). *Id.*

Even in the cases where courts have departed from this reasoning and acknowledged that a third-party technology provider may owe BIPA duties to its customers’ employees, those courts have made clear that the alleged collection, use, or disclosure of biometric data by the technology provider (like Kronos) is *separate and distinct* from the collection, use, or disclosure of biometric data by the employers/customers (like Hyatt). For example, in *Gutierrez v. Senior Lifestyle Corp.*, Case No. 2017-CH-11314 (Cir. Ct. Cook Cty.), a BIPA defendant brought a third-party claim for contribution against Kronos as the vendors of the technology at issue in the underlying BIPA lawsuit. Judge Reilly dismissed the third-party claims against Kronos because the underlying complaint “[did] not allege that Kronos [] ‘collected, captured, purchased, received through trade,

or otherwise obtained' the biometric data at issue in the underlying Complaint.” (Ex. D, *Gutierrez*, July 10, 2020 Order at 4). Therefore, Judge Reilly found the injury from the underlying allegations stemmed from the underlying defendant’s alleged collection of biometric information without proper notice or consent.

Like *Gutierrez*, the Rapai Lawsuit does not allege that Kronos collected, captured, purchased, received through trade, or otherwise obtained the underlying Plaintiff’s biometric data in violation of BIPA. Instead, the claims that the Rapai plaintiff brought, and that the underlying parties settled, were claims about Hyatt’s improper collection and use of biometric data. As such, even if Kronos did collect or obtain the Rapai plaintiff’s biometric data in violation of BIPA—it did not—the injuries claimed by the Rapai plaintiff would not stem from such conduct. *See Figueroa v. Kronos*, 454 F. Supp. 3d 772, 787 (N.D. Ill. 2020) (“Plaintiffs’ allegations that Kronos *itself* obtained and disseminated their biometric information reflect a course of conduct distinct from any BIPA violations in which their employers may have engaged, even if such violations occurred simultaneously or through use of the same equipment.”). Accordingly, Hyatt’s payments to the settlement class in the Rapai Lawsuit are for Hyatt’s separate and distinct alleged improper collection and use biometric data—not for any actions or activities of Kronos.

Thus BIPA’s text and the case law interpreting it are unequivocal: any BIPA duties that apply to *Hyatt’s* collection and possession of the Rapai plaintiff’s biometric data under section 15(a) and section 15(b) belong to *Hyatt* alone. The Rapai Lawsuit clearly seeks redress for Hyatt’s failure to comply with those duties—not any alleged duties of Kronos. (*See Rapai Compl.* ¶¶ 8, 23-27, 37.) Hyatt cannot pass off the consequences for its own failure to comply with BIPA to Kronos or to any other party.

B. Kronos did not agree to indemnify Hyatt against Hyatt’s own failure to comply with BIPA.

In an attempt to avoid the consequences of its own alleged negligent failure to comply with BIPA, Hyatt alleges that Kronos agreed to assume all of Hyatt’s BIPA obligations in connection with Hyatt’s use of the time clocks and the data they collect. “It is well settled,” however, “that indemnity contracts . . . will not be construed as indemnifying against a party’s own negligence unless such a construction is required by the clear and explicit language of the contract.” *Pekin Ins. Co.*, 2016 IL App (1st) 151689, ¶ 25. Here, the “clear and explicit language of the contract” compels the opposite conclusion—that Kronos did **not** agree to indemnify Hyatt against BIPA liability:

For clarity, Kronos will have no responsibility for any use Customer makes of any Products or Services that itself does not comply with applicable Laws.

(*See* Contract § 17(a).) Indeed, Hyatt agreed that, “[w]hen using and applying the information generated by [the] Products, **Customer is responsible for ensuring that Customer complies with the applicable requirements of applicable Laws.**” (*Id.* § 16(c) (emphasis added).) And as if to dispel any remaining ambiguity, Hyatt expressly “acknowledge[d] and agree[d] that **Kronos is not providing legal compliance Services hereunder.**” (*Id.* § 17(b) (emphasis added).)

“[W]hen interpreting an indemnification agreement, a court must give effect to the intention of the parties as determined from the language of the agreement.” *Smith v. West Suburban Med. Ctr.*, 391 Ill. App. 3d 995, 1000 (1st Dist. 2010). Other portions of the Contract make clear that Hyatt agreed to control the time clocks at its locations and retain full ownership of its employees’ data at all times, even after it was stored on the cloud. This was a sales and licensing agreement: the purpose of the Contract was to allow Hyatt and its affiliates “use of the Products and Services” subject to the terms and conditions set forth therein in exchange for agreed-upon fees. (*See* Contract §§ 1, 4.) This is notable because Kronos has “no responsibility or liability for

any use Customer makes of any Products or Services that itself does not comply with applicable Laws.” (*Id.* § 17(a).) After using the clocks to collect its employees’ data, Hyatt was to transfer that data to Kronos for simultaneous storage in the Kronos cloud environment.¹ Hyatt agreed to “ensure that the transfer of any Personal Information to Kronos and Kronos’ storage thereof in the Hosting Environment complies with applicable Data Protection Laws, including, if applicable, **any such laws requiring Customer to obtain consent from individuals for such transfer and storage.**” (Ex. B to Contract §12.3 (emphasis added).) The parties agreed, further, that Hyatt would at all times retain ownership of and control over the data: “all such Personal Information shall be deemed to be . . . owned by the Customer,” and Kronos could “process” it “only on the prior written instructions of Customer and only to the extent reasonably necessary for performance of this Agreement.” (Contract § 25(a)(iii)-(iv).) The Contract is not ambiguous as to these points: Hyatt used the time clocks to collect employee data and retained ownership and control over the data at all times. Kronos certainly did not agree to assume responsibility for Hyatt’s duties under BIPA or any other applicable law.

Hyatt’s apparent theory is that by agreeing to “Process” certain types of personal information on behalf of Hyatt, Kronos agreed to indemnify Hyatt against any liability Hyatt might incur with respect to that information. (*See* Compl. ¶¶ 42-48.) To support its theory, Hyatt cobbles together bits and pieces of the Contract, presents them out of order, and omits relevant language that forecloses such a broad reading. (*Id.* ¶¶ 22-26.) Read properly, the Contract lends no support for Hyatt’s theory.

¹ Indeed, as alleged in the *Rapai* Lawsuit, it was Hyatt that operated the time clocks that allegedly collected *Rapai* and the putative class’ biometric data. (*Rapai* Compl. ¶ 23).

As Hyatt admits (*see* Compl. ¶ 42), Kronos’s obligation to “Process” certain types of personal information on behalf of Hyatt—and to comply with certain privacy and security requirements in so doing—comes from Section 25 of the Contract (“Data Privacy and Protection Requirements”), which does not include an indemnification clause for any and all claims related to Kronos’ “processing.” (*See* Contract § 25(a).) Crucially, in Section 18(c), the Contract’s “Indemnification” Section limits Kronos’s indemnification duties for a purported breach of Section 25. Kronos agreed to indemnify Hyatt only against **claims involving a security breach** “arising out of or relating to” a “breach . . . of its obligations in Section 25 (Data Privacy Protection Requirements).” (*See* Contract § 18(c)(i)-(v) (limiting indemnification to various costs and liabilities incurred by Hyatt associated with “the security breach”).)

Hyatt has alleged that Kronos violated Section 25 by failing to “Process” certain types of information in compliance with certain laws and requirements. (Compl. ¶¶ 42-48.) But neither Hyatt nor Rapai has alleged in their complaints, nor stated in their settlement agreement, that this purported compliance breach (i.e. notice and consent) was tantamount to the sort of data security breach that might trigger Kronos’s indemnification duties under Section 18(c).² Nor does the Rapai Lawsuit “aris[e] out of or relat[e] to” any purported breach by Kronos. (Contract § 18(c).) It clearly seeks redress against Hyatt for **Hyatt’s** failures. (*See Rapai* Compl. ¶¶ 8, 23-27, 37.). Put simply, whether Kronos complies with BIPA is not relevant to whether **Hyatt** complied with BIPA (the subject of the Rapai Lawsuit). Thus even if Hyatt’s allegations were true, Kronos would owe no indemnification duties under the Contract.

² Further, neither Rapai nor Hyatt alleges that there was ever even a failure to protect the data at question in the *Rapai* Lawsuit under the standards set forth in BIPA Section 15(e).

C. Kronos could not have executed BIPA compliance for Hyatt in any event.

It is not surprising that Kronos did not agree to undertake BIPA compliance for Hyatt. Such would have been highly complicated—if not outright impossible—and the parties clearly never intended as much. *See Smith*, 391 Ill. App. 3d at 1000 (courts must give effect to the intention of the parties “when interpreting an indemnification agreement”). Section 15(a) requires that the entity **develop** a data retention policy, **publish** it, and thereafter **comply** with it in handling individual biometric data. *See* 740 ILCS 14/15(a). It is unclear how Kronos would have accomplished all of this for Hyatt. Such would have required that Hyatt: (1) delegate significant policymaking authority to Kronos so that Kronos could craft the policy; (2) grant Kronos access to its website and internal systems sufficient for Kronos to publish the policy; and (3) agree to allow Kronos significant authority to ensure Hyatt’s subsequent compliance with the policy, including through periodic audits. It is no wonder why the parties expressly agreed that Kronos would not provide legal compliance services to Hyatt in connection with the time clocks. (*See* Contract § 17(b) (“Customer acknowledges and agrees that Kronos is not providing legal compliance Services hereunder.”))

The same is true with respect to section 15(b). Hyatt’s apparent view is that Kronos was contractually obligated to procure informed written consent from its employees on its behalf. (*See* Compl. ¶¶ 42-48.) But Kronos has no relationship at all with Hyatt’s employees, and as the *Bernal* court noted, “requiring that a third party provider of the biometric time clock technology, without any direct relationship with its customers’ employees, obtain written releases from said employees would be unquestionably not only inconvenient but arguably absurd.” (*Bernal*, Ex. C at 2-3.) As the Illinois Supreme Court noted, “[c]ompliance [with BIPA] should not be difficult.” *Rosenbach v. Six Flags Entm’t Corp.*, 2019 IL 123186, ¶ 37. Left unexplained is why either party—Kronos

or Hyatt—would have agreed to such a complicated arrangement. Notably, Hyatt does not allege that it ever asked or required Kronos to undertake any sort of compliance efforts on its behalf.

This Court must construe the Contract “as a whole,” and “the construction should be a natural and easy one.” *Smith*, 397 Ill. App. 3d at 100. Hyatt’s construction of the Contract simply does not hold up against the wording and plain meaning of its Contract.

* * *

In sum, Hyatt’s claim for breach of contract (Count I) fails because it woefully misconstrues both BIPA’s requirements and the express terms and structure of the Contract. Kronos did not agree to assume Hyatt’s responsibilities under BIPA; Hyatt is responsible for its own compliance and cannot now pawn off liability for any failures to comply. Because Hyatt’s claim for declaratory judgment (Count II) simply duplicates Count I by asking the Court to declare that its breach of contract theory is correct, (*See* Compl. ¶¶ 52-63.) Count II therefore is flawed for the same reasons stated herein and likewise must be dismissed.

II. COUNT III (IMPLIED INDEMNITY) SHOULD BE DISMISSED.

Hyatt’s claim for implied indemnity (Count III) again simply restates the breach of contract claim by seeking redress for Kronos’s purported breach of Section 25(a) of the Contract (*See* Compl. ¶ 70.) But the Contract includes an explicit indemnification provision for breaches of Section 25—Section 18(c)—and it expressly limits Kronos’s indemnification duties to claims involving a resulting security breach. (*See* Contract § 18(c)(i)-(v).) The alleged failure to obtain employee consents or publish a privacy policy with a retention schedule and destruction guidelines under BIPA cannot be reimagined as data security breaches. Hyatt cannot use the common law to circumvent the Contract and thereby expand Kronos’s indemnification duties beyond the scope to which the Parties agreed.

Count III is improperly pled in any event. Implied contractual indemnity “is a contract implied in law arising from the legal obligation of an indemnitee to satisfy liability caused by actions of his indemnitor.” *Riley Acquisitions, Inc. v. Drexler*, 408 Ill. App. 3d 397, 405 (1st Dist. 2011).

The principle behind the theory of implied contractual indemnity is that, “where one party’s breach of contract **causes a second party to breach a separate contract with a third party**, the second party may shift its contractual liability to the first party. Indemnity is justified in such instances because a party who breaches a contract can be held liable for damages which naturally arise from the breach, provided that such damages were reasonably within the contemplation of the parties as a probable result of the breach.”

Id. (citing *Zielinski v. Miller*, 277 Ill. App. 3d 735, 740 (1st Dist. 2011) (emphasis added)). Hyatt does not allege that Kronos’s purported breach of Section 25 caused it to breach any contract. Nor does Hyatt allege that Kronos’s purported breach caused it to commit a tort for which it actually is blameless. *See Zielinski*, 277 Ill. App. 3d at 739 (“Implied tort indemnity is a common law doctrine which shifts the entire responsibility for tort-related losses from a blameless tortfeasor to a truly culpable one.”) Simply put, Count III misunderstands implied indemnity altogether. It should be dismissed.

CONCLUSION

For all the reasons stated herein, the Court should dismiss Hyatt’s third-party complaint against Kronos for failure to state a claim.

Dated: March 22, 2022

Respectfully submitted,

KRONOS INCORPORATED

By: /s/ Erin Bolan Hines
One of Its Attorneys

Melissa A. Siebert

Erin Bolan Hines
Maveric Ray Searle
SHOOK, HARDY & BACON L.L.P.
111 South Wacker Drive
Chicago, IL 60606
Tel: (312) 704-7700
Fax: (312) 558-1195
Email: masiebert@shb.com
ehines@shb.com
msearle@shb.com
Firm No. 58950