

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

PAMELA READDY, individually and on
behalf of all others similarly situated,

Plaintiff,

v.

KINDRED THC CHICAGO LLC and
KINDRED SYCAMORE, LLC d/b/a
KINDRED HOSPITAL-SYCAMORE,

Defendants.

Case No.: 2022CH01581

CLASS ACTION COMPLAINT

Plaintiff Pamela Readdy (“Pamela” or “Plaintiff”) brings this Class Action Complaint against Defendants Kindred THC Chicago LLC and Kindred Sycamore, LLC d/b/a Kindred Hospital-Sycamore (“collectively, “Defendants”) to put a stop to their unlawful collection, use, storage, and disclosure of Plaintiff’s and the putative Class members’ sensitive biometric data. Plaintiff, for Plaintiff’s Class Action Complaint, alleges as follows upon personal knowledge as to Plaintiff’s own acts and experiences and, as to all other matters, upon information and belief.

NATURE OF THE ACTION

1. As a result of a 2017 class action lawsuit (*Heard v. THC – Northshore, Inc. d/b/a Kindred Chicago Lakeshore, et al.*, Case No. 2017 CH 16818 (Cook County, Illinois)), the Defendants paid \$2.25 million to settle allegations that it violated the Biometric Information Privacy Act, 740 ILCS 14/1, *et seq.* (“BIPA”) for privacy violations associated with collecting and storing employees’ biometric information when they clocked in and out of work. While

Defendants were released of liability in that lawsuit, and apparently began requesting written consent to use its biometric timeclocks, the Defendants still do not get their employees' written consent for the use of biometric scans used by medication dispenser systems.

2. Specifically, Defendants use the Pyxis MedStation system, and related Pxyis devices (collectively referred to as "Pyxis"), all of which are automated medication dispensing systems that require users to scan a fingerprint to access the device and systems. Defendants require users to scan their biometric information, namely their fingerprint, to gain access to the Pyxis devices.

3. While there are tremendous benefits to using biometric systems in the workplace, there are also serious risks. Unlike identification cards or numbers—which can be changed or replaced if stolen or compromised—fingerprints are unique, permanent biometric identifiers associated with the employee. This exposes employees to serious and irreversible privacy risks. For example, if a fingerprint database is hacked, breached, or otherwise exposed, employees have no means by which to prevent identity theft and unauthorized tracking.

4. Despite this law, Defendants disregarded their employees' statutorily protected privacy rights and unlawfully collects, stores, and uses their biometric data in violation of the BIPA. Specifically, Defendants have violated (and continue to violate) the BIPA because it did not, with respect to its Pyxis system:

- Properly inform Plaintiff and the Class members in writing of the specific purpose and length of time for which their fingerprints were being collected, stored, and used for the Pyxis system;
- Receive a written release from Plaintiff or the members of the Class to collect, capture, or otherwise obtain fingerprints for the Pyxis system, as required by the BIPA.

5. Accordingly, this Complaint seeks an order: (i) declaring that Defendants' conduct

violates the BIPA; (ii) requiring Defendants to cease the unlawful activities discussed herein; and (iii) awarding liquidated damages to Plaintiff and the proposed Class.

6. As BIPA has been on the books for nearly 15 years and the Defendants have been *actually aware* of BIPA for a half decade and even paid \$2.25 million to settle prior violations, this Complaint seeks all damages available including heightened liquidated damages per violation.

PARTIES

7. Plaintiff is a natural person and citizen of the State of Illinois.

8. Defendants are a Kentucky-based healthcare organization that operates six hospitals in Illinois, including three in Chicago.

JURISDICTION AND VENUE

9. This Court has jurisdiction over Defendants pursuant to 735 ILCS 5/2-209 because Defendants conduct business transactions in Illinois and have committed tortious acts in Illinois.

10. Venue is proper in Cook County because Defendants operate throughout this County.

FACTUAL BACKGROUND

I. The Biometric Information Privacy Act.

11. In the early 2000's, major national corporations started using Chicago and other locations in Illinois to test "new [consumer] applications of biometric-facilitated financial transactions, including finger-scan technologies at grocery stores, gas stations, and school cafeterias." 740 ILCS 14/5(b). Given its relative infancy, an overwhelming portion of the public became weary of this then-growing, yet unregulated technology. *See* 740 ILCS 14/5.

12. In late 2007, a biometrics company called Pay By Touch—which provided major retailers throughout the State of Illinois with fingerprint scanners to facilitate consumer

transactions—filed for bankruptcy. That bankruptcy was alarming to the Illinois Legislature because suddenly there was a serious risk that millions of fingerprint records—which, are unique biometric identifiers, can be linked to people’s sensitive financial and personal data—could now be sold, distributed, or otherwise shared through the bankruptcy proceedings without adequate protections for Illinois citizens. The bankruptcy also highlighted the fact that most consumers who had used that company’s fingerprint scanners were completely unaware that the scanners were not actually transmitting fingerprint data to the retailer who deployed the scanner, but rather to the now-bankrupt company, and that unique biometric identifiers could now be sold to unknown third parties.

13. Recognizing the “very serious need [for] protections for the citizens of Illinois when it [came to their] biometric information,” Illinois enacted the BIPA in 2008. *See* Illinois House Transcript, 2008 Reg. Sess. No. 276; 740 ILCS 14/5.

14. The BIPA is an informed consent statute which achieves its goal by making it unlawful for a company to, among other things, “collect, capture, purchase, receive through trade, or otherwise obtain a person’s or a customer’s biometric identifiers or biometric information, unless it *first*:

- (1) informs the subject . . . in writing that a biometric identifier or biometric information is being collected or stored;
- (2) informs the subject . . . in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; and
- (3) receives a written release executed by the subject of the biometric identifier or biometric information.

740 ILCS 14/15(b).

15. BIPA specifically applies to employees who work in the State of Illinois. BIPA

defines a “written release” specifically “in the context of employment [as] a release executed by an employee as a condition of employment.” 740 ILCS 14/10.

16. Biometric identifiers include retina and iris scans, voiceprints, scans of hand and face geometry, and—most importantly here—fingerprints. *See* 740 ILCS 14/10. Biometric information is separately defined to include any information based on an individual’s biometric identifier that is used to identify an individual. *See id.*

17. The BIPA also establishes standards for how employers must handle Illinois employees’ biometric identifiers and biometric information. *See* 740 ILCS 14/15(c)–(d). For instance, the BIPA requires companies to develop and comply with a written policy—made available to the public—establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting such identifiers or information has been satisfied or within three years of the individual’s last interaction with the company, whichever occurs first. 740 ILCS 14/15(a).

18. Ultimately, the BIPA is simply an informed consent statute. Its narrowly tailored provisions place no absolute bar on the collection, sending, transmitting or communicating of biometric data. For example, the BIPA does not limit what kinds of biometric data may be collected, sent, transmitted, or stored. Nor does the BIPA limit to whom biometric data may be collected, sent, transmitted, or stored. The BIPA simply mandates that entities wishing to engage in that conduct must make proper disclosures and implement certain reasonable safeguards.

II. Defendants Violate the Biometric Information Privacy Act.

19. By the time the BIPA passed through the Illinois Legislature in mid-2008, many companies who had experimented with using biometric data as an authentication method stopped doing so, at least for a time. That is because Pay By Touch’s bankruptcy, described in Section I

above, was widely publicized and brought attention to consumers' discomfort with the use of their biometric data.

20. Unfortunately, Defendants failed to take note of the passage of the BIPA even though it has been in effect for over a decade and Defendants are presumed to know the law. Defendants continued to collect, store, and use their employees' biometric data in violation of the BIPA.

21. Specifically, when employees worked at Defendants, they are required to have their fingerprints scanned in order to enroll them in its fingerprint database.

22. Defendants use an employee medication dispensing system that requires employees to use their fingerprints as a means of authentication. Unlike a traditional methods, employees have to use their fingerprint to access medications at work.

23. Defendants failed to inform their employees of the complete purposes for which it collects their sensitive biometric data or to whom the data is disclosed, if at all.

24. Defendants failed to inform employees that they were sharing their finger print data with third-party vendors for the biometric Pyxis system or obtain employees' consent to do so.

25. Defendants similarly failed to provide their employees with a written, publicly available policy identifying its retention schedule, and guidelines for permanently destroying its employees' fingerprints when the initial purpose for collecting or obtaining their fingerprints is no longer relevant, as required by the BIPA. An employee who leaves the company does so without any knowledge of when their biometric identifiers will be removed from Defendants' databases—or if they ever will be.

26. The Pay By Touch bankruptcy that catalyzed the passage of the BIPA highlights why conduct such as Defendants' —whose employees are aware that they are providing biometric

identifiers but are not aware of to whom or the full extent of the reasons they are doing so—is so dangerous. That bankruptcy spurred Illinois citizens and legislators to realize a critical point: it is crucial for people to understand when providing biometric data who exactly is collecting it, who it will be transmitted to, for what purposes, and for how long. But Defendants disregard these obligations, and instead unlawfully collects, stores, and uses its employees' biometric identifiers and information without proper consent.

27. Ultimately, Defendants disregard their employees' statutorily protected privacy rights by violating the BIPA.

FACTS SPECIFIC TO PLAINTIFF

28. Plaintiff worked for Defendants in Illinois and scanned her fingerprint in the Pyxis system at Defendants' location to access medication.

29. As an employee, Defendants required Plaintiff to scan Plaintiff's fingerprint so that it could use it as an authentication method. Defendants subsequently stored Plaintiff's fingerprint data in their databases.

30. Each time Plaintiff needed medications dispensed, Plaintiff was required to scan her fingerprint so it could be used as an authentication method to access Defendant's Pyxis devices.

31. Plaintiff was required to scan her fingerprint each time she accessed any one of Defendant's Pyxis devices.

32. Defendants never informed Plaintiff of the specific limited purposes or length of time for which they collected, stored, or used fingerprints.

33. Similarly, Defendants never informed Plaintiff of any biometric data retention policy it developed, nor whether they will ever permanently delete fingerprints.

34. Plaintiff never signed a written release allowing Defendants to collect or store

fingerprints.

35. Plaintiff has continuously and repeatedly been exposed to the risks and harmful conditions created by Defendants' violations of the BIPA alleged herein.

36. Plaintiff now seeks liquidated damages under BIPA as compensation for the injuries Defendants has caused.

CLASS ALLEGATIONS

37. **Class Definition:** Plaintiff brings this action pursuant to 735 ILCS 5/2-801 on behalf of Plaintiff and a Class of similarly situated individuals, defined as follows:

All persons who had their fingerprints collected, captured, received, otherwise obtained, or disclosed by Defendants after April 1, 2019 while in Illinois and who used the Pyxis system.

The following people are excluded from the Class: (1) any Judge presiding over this action and members of their families; (2) Defendants, Defendants' subsidiaries, parents, successors, predecessors, and any entity in which the Defendants or their parents have a controlling interest and its current or former officers and directors; (3) persons who properly execute and file a timely request for exclusion from the Class; (4) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; (5) Plaintiff's counsel and Defendants' counsel; (6) the legal representatives, successors, and assigns of any such excluded persons, (7) any claim that was released as a result of the settlement in *Heard v. THC – Northshore, Inc. d/b/a Kindred Chicago Lakeshore, et al.*, Case No. 2017 CH 16818 (Cook County, Illinois).

38. **Numerosity:** The exact number of Class members is unknown to Plaintiff at this time, but it is clear that individual joinder is impracticable. Defendants have collected, captured, received, or otherwise obtained biometric identifiers or biometric information from at least hundreds of employees who fall into the definition of the Class. Ultimately, the Class members

will be easily identified through Defendants' records.

39. **Commonality and Predominance:** There are many questions of law and fact common to the claims of Plaintiff and the Class, and those questions predominate over any questions that may affect individual members of the Class. Common questions for the Class include, but are not necessarily limited to the following:

- a) whether Defendants collected, captured, or otherwise obtained Plaintiff's and the Class' biometric identifiers or biometric information;
- b) whether Defendants properly informed Plaintiff and the Class of its purposes for collecting, using, and storing their biometric identifiers or biometric information;
- c) whether Defendants obtained a written release (as defined in 740 ILCS 14/10) to collect, use, and store Plaintiff and the Class' biometric identifiers or biometric information;
- d) whether Defendants have sold, leased, traded, or otherwise profited from Plaintiff and the Class's biometric identifiers or biometric information;
- e) whether Defendants developed a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within three years of their last interaction, whichever occurs first;
- f) whether Defendants comply with any such written policy (if one exists); and
- g) whether Defendants used Plaintiff and the Class' fingerprints to identify them.

40. **Adequate Representation:** Plaintiff will fairly and adequately represent and protect the interests of the Class and have retained counsel competent and experienced in complex litigation and class actions. Plaintiff has no interests antagonistic to those of the Class, and Defendants have no defenses unique to Plaintiff. Plaintiff and their counsel are committed to vigorously prosecuting this action on behalf of the members of the Class, and have the financial resources to do so. Neither Plaintiff nor their counsel have any interest adverse to those of the other

members of the Class.

41. **Appropriateness:** This class action is appropriate for certification because class proceedings are superior to all others available methods for the fair and efficient adjudication of this controversy and joinder of all members of the Class is impracticable. The damages suffered by the individual members of the Class are likely to have been small relative to the burden and expense of individual prosecution of the complex litigation necessitated by Defendants' wrongful conduct. Thus, it would be virtually impossible for the individual members of the Class to obtain effective relief from Defendants' misconduct. Even if members of the Class could sustain such individual litigation, it would not be preferable to a class action because individual litigation would increase the delay and expense to all parties due to the complex legal and factual controversies presented in their Complaint. By contrast, a class action presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court. Economies of time, effort, and expense will be fostered and uniformity of decisions will be ensured.

CAUSE OF ACTION
Violation of 740 ILCS 14/1, *et seq.*
(On Behalf of Plaintiff and the Class)

42. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

43. The BIPA requires companies to obtain informed written consent from employees before acquiring their biometric data. Specifically, the BIPA makes it unlawful for any private entity to "collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifiers or biometric information, unless [the entity] first: (1) informs the subject . . . in writing that a biometric identifier or biometric information is being collected or stored; (2) informs the subject . . . in writing of the specific purpose and length of term for which

a biometric identifier or biometric information is being collected, stored, and used; *and* (3) receives a written release executed by the subject of the biometric identifier or biometric information....” 740 ILCS 14/15(b) (emphasis added).

44. The BIPA also mandates that companies in possession of biometric data establish and maintain a satisfactory biometric data retention (and—importantly—deletion) policy. Specifically, those companies must: (i) make publicly available a written policy establishing a retention schedule and guidelines for permanent deletion of biometric data (*i.e.*, when the employment relationship ends); and (ii) actually adhere to that retention schedule and actually delete the biometric information. *See* 740 ILCS 14/15(a).

45. Unfortunately, Defendants fail to comply with these BIPA mandates.

46. Defendants each qualify as a “private entity” under the BIPA. *See* 740 ILCS 14/10.

47. Plaintiff and the Class are individuals who had their “biometric identifiers” collected by Defendants (in the form of their fingerprints), as explained in detail in Section II. *See* 740 ILCS 14/10.

48. Plaintiff and the Class’ biometric identifiers or information based on those biometric identifiers were used to identify them, constituting “biometric information” as defined by the BIPA. *See* 740 ILCS 14/10.

49. Defendants violated 740 ILCS 14/15(b)(3) by failing to obtain written releases from Plaintiff and the Class before it collected, used, and stored their biometric identifiers and biometric information.

50. Defendants violated 740 ILCS 14/15(b)(1) by failing to inform Plaintiff and the Class in writing that their biometric identifiers and biometric information were being collected and stored.

51. Defendants violated 740 ILCS 14/15(b)(2) by failing to inform Plaintiff and the Class in writing of the specific purpose and length of term for which their biometric identifiers or biometric information was being collected, stored, and used.

52. Defendants violated 740 ILCS 14/15(a) by failing to publicly provide and follow a retention schedule or guideline for permanently destroying its employees' biometric identifiers and biometric information.

53. Defendants violated 740 ILCS 14/15(d) by sharing and disclosing employees' biometric identifiers and biometric information without consent.

54. By collecting, storing, and using Plaintiff's and the Class' biometric identifiers and biometric information as described herein, Defendants violated Plaintiff's and the Class' rights to privacy in their biometric identifiers or biometric information as set forth in the BIPA, 740 ILCS 14/1, *et seq.*

55. On behalf of themselves and the Class, Plaintiff seeks: (1) injunctive and equitable relief as is necessary to protect the interests of the Plaintiff and the Class by requiring Defendants to comply with the BIPA's requirements for the collection, storage, and use of biometric identifiers and biometric information as described herein; (2) liquidated damages for each of Defendants' violations of the BIPA pursuant to 740 ILCS 14/20; and (3) reasonable attorneys' fees and costs and expenses pursuant to 740 ILCS 14/20(3).

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and the Class, respectfully requests that the Court enter an Order:

A. Certifying this case as a class action on behalf of the Class defined above, appointing Plaintiff as representative of the Class, and appointing their counsel as Class Counsel;

- B. Declaring that Defendants' actions, as set out above, violate the BIPA;
- C. Awarding statutory damages for each of Defendants' violations of the BIPA, pursuant to 740 ILCS 14/20;
- D. Awarding other equitable relief as is necessary to protect the interests of the Class, including an Order requiring Defendants to collect, store, and use biometric identifiers or biometric information in compliance with the BIPA;
- F. Awarding Plaintiff and the Class their reasonable litigation expenses and attorneys' fees;
- G. Awarding Plaintiff and the Class pre- and post-judgment interest, to the extent allowable; and
- H. Awarding such other and further relief as equity and justice may require.

Dated: February 24, 2022

Respectfully submitted,

**Pamela Readdy, individually and on behalf of all
others similarly situated,**

By: /s/ David Fish
One of Plaintiff's Attorneys

David Fish
dfish@fishlawfirm.com
Mara Baltabols
mara@fishlawfirm.com
FISH POTER BOLAÑOS, P.C
200 East Fifth Avenue, Suite 123
Naperville, Illinois 60563
Tel: 630.355.7590
Fax: 630.778.0400
docketing@fishlawfirm.com