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

COREY HEARD, individually, and on behalf of all others similarly situated,	)	
Plaintiff,	)	**Case No.** 2023CH09013
v.	)	
RUSH UNIVERSITY HOSPITAL,	)	
Defendant.	)	

CLASS ACTION COMPLAINT

Plaintiff Corey Heard ("Plaintiff") individually and on behalf of all others similarly situated (the "Class"), by and through his attorneys, brings the following Class Action Complaint ("Complaint") pursuant to the Illinois Code of Civil Procedure, 735 ILCS §§ 5/2-801 and 2-802, against Rush University Hospital ("Rush" or "Defendant"), and its subsidiaries, to redress and curtail Defendant's unlawful collection, obtainment, use, storage, and disclosure of Plaintiff's sensitive and proprietary biometric identifiers and information ("biometric data"). Plaintiff alleges as follows upon personal knowledge as to himself, his own acts and experiences and, as to all other matters, upon information and belief, including investigation conducted by his attorneys.

NATURE OF THE ACTION

1. Defendant Rush operates a private hospital located in Chicago, Illinois, which conducts business within the city and in this Circuit.

2. Defendant employed Plaintiff as a respiratory therapist at times in 2022 and 2023.

3. At all relevant times, Rush facilities have used and continue to use biometric enabled automated medication and/or supply dispensing systems, including but not limited to the

Pyxis MedStation Systems, the Pyxis CIISafe system, the Pyxis Anesthesia system, and other similar Pyxis devices (collectively referred to as "Pyxis") by Becton, Dickinson and Company ("BD").

4. These systems authenticate user identities by capturing and utilizing their biometric identifiers and/or information. The Pyxis systems allow devices, software, and servers to function together and communicate with one another.

5. Defendant required authorized workers, including Plaintiff, to scan their biometric information, namely their fingerprint, in order to access medications.

6. When workers, like Plaintiff, are given access to Pyxis, they are enrolled in the system. Within Rush Hospital there are multiple Pyxis devices. Once a worker has registered his or her fingerprint with the system, they have access to multiple Pyxis devices throughout the hospital.

7. Unlike ID badges or key fobs—which can be changed or replaced if stolen or compromised—fingerprints are unique, permanent biometric identifiers associated with each worker. This exposes workers who are required to use Pyxis as a condition of their employment to serious and irreversible privacy risks. For example, if a database containing fingerprints or other sensitive, proprietary biometric data is hacked, breached, or otherwise exposed – like in the recent Google+, Equifax, Uber, Facebook/Cambridge Analytica, and Marriott data breaches or misuses—workers have no means by which to prevent identity theft, unauthorized tracking or other unlawful or improper use of this highly personal and private information.

8. Biometrics are not relegated to esoteric corners of commerce. Many businesses—such as hospitals—and financial institutions have incorporated biometric applications into their

workplace in the form of biometric timeclocks, and into consumer products, including such ubiquitous consumer products as checking accounts and cell phones.

9. In 2015, a data breach at the United States Office of Personnel Management exposed the personal identification information, including biometric data, of over 21.5 million federal employees, contractors, and job applicants. U.S. Off. of Personnel Mgmt., *Cybersecurity Incidents* (2018), *available at* www.opm.gov/cybersecurity/cybersecurity-incidents.

10. An illegal market already exists for biometric data. Hackers and identity thieves have targeted Aadhaar, the largest biometric database in the world, which contains the personal and biometric data – including fingerprints, iris scans, and a facial photograph – of over a billion Indian citizens. *See* Vidhi Doshi, *A Security Breach in India Has Left a Billion People at Risk of Identity Theft*, The Washington Post (Jan. 4, 2018), *available at* https://www.washingtonpost.com/news/worldviews/wp/2018/01/04/a-security-breach-in-india-has-left-a-billion-people-at-risk-of-identity-theft/?utm_term=.b3c70259f138.

11. In January 2018, an Indian newspaper reported that the information housed in Aadhaar was available for purchase for less than $8 and in as little as 10 minutes. Rachna Khaira, *Rs 500, 10 Minutes, and You Have Access to Billion Aadhaar Details*, The Tribune (Jan. 4, 2018), *available at* http://www.tribuneindia.com/news/nation/rs-500-10-minutes-and-you-have-access-to-billion-aadhaar-details/523361.html.

12. Recognizing the need to protect its citizens from situations like these, Illinois enacted the Biometric Information Privacy Act ("BIPA"), 740 ILCS 14/1, *et seq.*, specifically to regulate companies that collect, obtain, store and use Illinois citizens' biometrics, such as fingerprints.

13. Notwithstanding the clear and unequivocal requirements of the law, Defendant disregards Pyxis users' statutorily protected privacy rights and unlawfully collects, obtains, stores, disseminates, and uses their biometric data in violation of BIPA. Specifically, Defendant has violated and continues to violate BIPA because it did not and continues not to:

a. Properly inform Plaintiff and others similarly situated in writing of the specific purpose and length of time for which their fingerprints were being collected, obtained, stored, and used, as required by BIPA;

b. Receive a written release from Plaintiff and others similarly situated to collect, obtain, store, or otherwise use their fingerprints, as required by BIPA;

c. Provide a publicly available retention schedule and guidelines for permanently destroying Plaintiff's and other similarly-situated individuals' fingerprints, as required by BIPA; and

d. Obtain consent from Plaintiff and others similarly situated to disclose, redisclose, or otherwise disseminate their fingerprints to a third party as required by BIPA.

14. Plaintiff and other similarly-situated individuals are aggrieved because they were not: (1) informed in writing of the purpose and length of time for which their biometric data was being collected, obtained, stored, disseminated and used; (2) provided a publicly available retention schedule or guidelines for permanent destruction of the biometric data; and (3) provided (nor did they execute) a written release, as required by BIPA.

15. Defendant Rush obtained users' biometric data directly from its Pyxis devices.

16. Upon information and belief, Defendant improperly discloses Plaintiff's and other similarly-situated individuals' fingerprint data to at least one out-of-state third-party vendor, Becton, Dickinson and Company.

17. Upon information and belief, Defendant improperly discloses Plaintiff's and other similarly-situated individuals' fingerprint data to other, currently unknown, third parties, including, but not limited to third parties that host biometric data in their data center(s).

18. Defendant lacks retention schedules and guidelines for permanently destroying Plaintiff's and other similarly-situated individuals' biometric data and has not and will not destroy their biometric data as required by BIPA.

19. Plaintiff and others similarly situated are aggrieved by Defendant's failure to destroy their biometric data when the initial purpose for collecting or obtaining such data has been satisfied or within three years of Plaintiff's and others similarly-situated individuals' employment at Rush.

20. Plaintiff and others similarly situated have suffered an injury in fact based on Defendant's improper disclosures of their biometric data to third parties.

21. Plaintiff and others similarly situated have suffered an injury in fact based on Defendant's violations of their legal rights.

22. These violations have raised a material risk that Plaintiff's and other similarly-situated individuals' biometric data will be unlawfully accessed by third parties.

23. Rush workers have a proprietary right to control their biometric information. In failing to comply with the requirements of BIPA, Defendant intentionally interferes with each worker's right of possession and control over their valuable, unique, and permanent biometric data.

24. Defendant is directly liable for, and had actual knowledge of, the BIPA violations alleged herein.

25. Accordingly, Plaintiff seeks an Order: (1) declaring that Defendant's conduct violates BIPA; (2) requiring Defendant to cease the unlawful activities discussed herein; and (3) awarding statutory damages to Plaintiff and the proposed Class.

PARTIES

26. Plaintiff Corey Heard is a natural person and a resident of the State of Illinois.

27. Defendant Rush University Hospital is an Illinois corporation that is registered with the Secretary of State and conducts business in the State of Illinois, including Cook County.

JURISDICTION AND VENUE

28. This Court has jurisdiction over Defendant pursuant to 735 ILCS § 5/2-209 because it conducts business transactions in Illinois, committed statutory violations and tortious acts in Illinois, and is registered to conduct business in Illinois.

29. Venue is proper in Cook County because Defendant is authorized to conduct business in this State, Defendant conducts business transactions in Cook County, and Defendant committed the statutory violations alleged herein in Cook County and throughout Illinois.

FACTUAL BACKGROUND

I. The Biometric Information Privacy Act

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

31. 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, like other 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

used the 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 their unique biometric identifiers could now be sold to unknown third parties.

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

33. Additionally, to ensure compliance, BIPA provides that, for each violation, the prevailing party may recover $1,000 or actual damages, whichever is greater, for negligent violations and $5,000, or actual damages, whichever is greater, for intentional or reckless violations. 740 ILCS 14/20.

34. 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:

a. Informs the subject in writing that a biometric identifier or biometric information is being collected, stored and used;

b. Informs the subject in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, obtained, stored, and used; and

c. Receives a written release executed by the subject of the biometric identifier or biometric information.

See 740 ILCS § 14/15(b).

35. 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. *Id.*

36. BIPA also establishes standards for how companies must handle Illinois citizens' biometric identifiers and biometric information. *See, e.g.,* 740 ILCS § 14/15(c)-(d). For example, BIPA prohibits private entities from disclosing a person's or customer's biometric identifier or biometric information without first obtaining consent for such disclosure. *See* 740 ILCS § 14/15(d)(1).

37. BIPA also prohibits selling, leasing, trading, or otherwise profiting from a person's biometric identifiers or biometric information (740 ILCS § 14/15(c)) and 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).

38. BIPA also enforces a standard of care to be upheld by private entities in possession of biometric identifiers or information. For example, BIPA prohibits private entities from failing to store, transmit, and protect from disclosure of biometric data "using the reasonable standard of care within the entity's industry" or "in a manner that is the same or more protective than the manner in which the private entity stores, transmits, and protects other confidential and sensitive information." 740 ILCS § 14/15(e).

39. The Illinois legislature enacted BIPA due to the increasing use of biometric data in financial and security settings, the general public's hesitation to use biometric information, and—most significantly—the unknown ramifications of biometric technology. Biometrics are

biologically unique to the individual and, once compromised, an individual is at heightened risk for identity theft and left without any recourse.

40. BIPA provides individuals with a private right of action, protecting their right to privacy regarding their biometrics as well as protecting their rights to know the precise nature for which their biometrics are used and how they are being stored and ultimately destroyed. Unlike other statutes that only create a right of action if there is a qualifying data breach, BIPA strictly regulates the manner in which entities may collect, obtain, store, use, and disseminate biometrics and creates a private right of action for lack of statutory compliance.

41. Plaintiff, like the Illinois legislature, recognizes how imperative it is to keep biometric information secure. Biometric information, unlike other personal identifiers such as a social security number, cannot be changed or replaced if hacked or stolen.

II. Defendant Violates the Biometric Information Privacy Act.

42. By the time BIPA passed through the Illinois legislature in mid-2008, most companies who had used individuals' biometric data stopped doing so.

43. Defendant failed to take note of the shift in Illinois law governing the collection, use and dissemination of biometric data. As a result, Defendant collected, obtained, stored, used and disseminated their workers' biometric data in violation of BIPA.

44. Specifically, when an authorized worker begins at Rush, they are required to have their fingerprint scanned in order to enroll them in the Pyxis system and related database(s).

45. Rush fails to inform the authorized workers that Defendant is collecting, storing, or using their sensitive biometric data, the extent of the purposes for which they collect their sensitive biometric data, or to whom the data is disclosed.

46. Rush fails to provide workers a written, publicly-available policy identifying its retention schedule and guidelines for permanently destroying workers' biometric data when the initial purpose for collecting or obtaining their biometrics is no longer relevant, as required by BIPA.

47. The Pay by Touch bankruptcy that catalyzed the passage of BIPA highlights why such conduct—where individuals are aware that they are providing a fingerprint but not aware to whom or for what purposes they are doing so—is dangerous. That bankruptcy spurred Illinois citizens and legislators into realizing that it is crucial for individuals to understand when providing biometric identifiers, such as a fingerprint, who exactly is collecting or obtaining their biometric data, where it will be transmitted and for what purposes, and for how long. Defendant disregards these obligations and these workers' statutory rights and instead unlawfully collects, obtains, stores, uses and disseminates their biometric identifiers and information, without ever receiving the individual's informed written consent required by BIPA.

48. Remarkably, Defendant has created the same situation that Pay by Touch did by assembling a database of biometric data through broadly deployed fingerprint scanners, but failed to comply with the law specifically designed to protect individuals whose biometrics are collected in these circumstances. Defendant disregards these obligations and its Illinois workers' statutory rights and instead unlawfully collects, obtains, stores, uses, and disseminates workers' biometric identifiers and information without ever receiving the individual's informed written consent required by BIPA.

49. Workers are not told what might happen to their biometric data if and when Defendant merges with another company or worse, if and when Defendant's businesses folds, or when the other third parties that have received their biometric data businesses fold.

50. Since Defendant neither publishes a BIPA-mandated data-retention policy nor discloses the purposes for its collection, obtainment and use of biometric data, workers have no idea whether Defendant sells, discloses, re-discloses, or otherwise disseminates their biometric data. Moreover, Plaintiff and others similarly situated are not told to whom Defendant currently discloses their biometric data, or what might happen to their biometric data in the event of a merger or bankruptcy.

51. These violations have raised a material risk that Plaintiff's and other similarly-situated individuals' biometric data will be unlawfully accessed by third parties.

52. By and through the actions detailed above, Defendant disregards Plaintiff's and other similarly-situated individuals' legal rights in violation of BIPA.

III. Named Plaintiff's Experience

53. Plaintiff Corey Heard worked as a Respiratory Therapist for Rush Hospital located at 1041 S Ashland Ave, Chicago, IL 60607 at times in 2022 and 2023.

54. Plaintiff ***was required*** to scan and enroll his fingerprint in Defendant's Pyxis devices so his fingerprint could be used as an authentication method to access the Pyxis devices and system.

55. Defendant subsequently stored Plaintiff's fingerprint data in its internal hospital systems.

56. Plaintiff was required to scan his fingerprint each time he accessed the Pyxis devices.

57. Plaintiff has never been informed of the specific limited purposes or length of time for which Defendant collected, stored, used and/or disseminated his biometric data.

58. Plaintiff has never been informed of any biometric data retention policy developed by Defendant, nor has he ever been informed of whether Defendant will ever permanently delete his biometric data.

59. Plaintiff has never been provided with nor ever signed a written release allowing Defendant to collect, store, use or disseminate his biometric data.

60. Plaintiff has continuously and repeatedly been exposed to the risks and harmful conditions created by Defendant's violations of BIPA as alleged herein.

61. No amount of time or money can compensate Plaintiff if his biometric data is compromised by the lax procedures through which Defendant captured, obtained, stored, used, and disseminated his and other similarly-situated individuals' biometrics. Moreover, Plaintiff would not have provided his biometric data to Defendant if he had known that Defendant would retain such information for an indefinite period of time without his consent.

62. A showing of actual damages is not necessary in order to state a claim under BIPA. *See Rosenbach v. Six Flags Ent. Corp.*, 2019 IL 123186, ¶ 40 ("[A]n individual need not allege some actual injury or adverse effect, beyond violation of his or her rights under the Act, in order to qualify as an "aggrieved" person and be entitled to seek liquidated damages and injunctive relief pursuant to the Act").

63. As Plaintiff is not required to allege or prove actual damages in order to state a claim under BIPA, he seeks statutory damages under BIPA as compensation for the injuries caused by Defendant. *Rosenbach*, 2019 IL 123186, ¶ 40.

CLASS ALLEGATIONS

64. Pursuant to the Illinois Code of Civil Procedure, 735 ILCS 5/2-801, Plaintiff brings claims on his own behalf and as a representative of all other similarly-situated individuals pursuant

to BIPA, 740 ILCS § 14/1, *et seq.*, to recover statutory penalties, prejudgment interest, attorneys' fees and costs, and other damages owed.

65. As discussed *supra*, Section 14/15(b) of BIPA prohibits a company from, among other things, collecting, capturing, purchasing, receiving through trade, or otherwise obtaining a person's or a customer's biometric identifiers or biometric information, unless it first (1) informs the individual in writing that a biometric identifier or biometric information is being collected, obtained or stored; (2) informs the individual in writing of the specific purpose and length of time for which a biometric identifier or biometric information is being collected, obtained, stored, and used; ***and*** (3) receives a written release executed by the subject of the biometric identifier or biometric information. 740 ILCS § 14/15.

66. Plaintiff seeks class certification under the Illinois Code of Civil Procedure, 735 § ILCS 5/2-801 for the following class of similarly-situated individuals under BIPA:

> All individuals working in the State of Illinois who had their fingerprints, or any other biometric identifiers and/or biometric information, collected, captured, received, or otherwise obtained or disclosed by Defendant during the applicable statutory period.

67. This action is properly maintained as a class action under 735 ILCS § 5/2-801 because:

A. The class is so numerous that joinder of all members is impracticable;

B. There are questions of law or fact that are common to the class;

C. The claims of the Named Plaintiff are typical of the claims of the class; and,

D. The Named Plaintiff will fairly and adequately protect the interests of the class.

Numerosity

68. The total number of putative class members exceeds fifty (50) individuals. The exact number of class members can easily be determined from Rush's records.

Commonality

69. There is a well-defined commonality of interest in the substantial questions of law and fact concerning and affecting the Class in that Plaintiff and all members of the Class have been harmed by Defendant's failure to comply with BIPA. The common questions of law and fact include, but are not limited to the following:

A. Whether Defendant collected, captured or otherwise obtained Plaintiff's and the Class's biometric identifiers or biometric information;

B. Whether Defendant properly informed Plaintiff and the Class of its purposes for collecting, obtaining, using, storing and disseminating their biometric identifiers or biometric information;

C. Whether Defendant obtained a written release (as defined in 740 ILCS § 14/10) to collect, obtain, use, store and disseminate Plaintiff's and the Class's biometric identifiers or biometric information;

D. Whether Defendant has disclosed or re-disclosed Plaintiff's and the Class's biometric identifiers or biometric information;

E. Whether Defendant has sold, leased, traded, or otherwise profited from Plaintiff's and the Class's biometric identifiers or biometric information;

F. Whether Defendant 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 its last interaction with the individual, whichever occurs first;

G. Whether Defendant stored, transmitted, and protected Plaintiff's and the Class's biometric data from disclosure using a reasonable standard of care;

H. Whether Defendant complies with any such written policy (if one exists);

I. Whether Defendant used Plaintiff's and the Class's fingerprints to identify them;

J. Whether the violations of BIPA were committed negligently; and

K. Whether the violations of BIPA were committed intentionally and/or recklessly.

70. Plaintiff anticipates that Defendant will raise defenses that are common to the class.

Adequacy

71. Plaintiff will fairly and adequately protect the interests of all members of the class, and there are no known conflicts of interest between Plaintiff and class members. Plaintiff, moreover, has retained experienced counsel who are competent in the prosecution of complex litigation and who have extensive experience acting as class counsel.

Typicality

72. The claims asserted by Plaintiff are typical of the class members they seek to represent. Plaintiff have the same interests and suffer from the same unlawful practices as the class members.

73. Upon information and belief, there are no other class members who have an interest individually controlling the prosecution of his or her individual claims, especially in light of the relatively small value of each claim and the difficulties involved in bringing individual litigation against one's employer. However, if any such class member should become known, he or she can "opt out" of this action pursuant to 735 ILCS § 5/2-801.

Predominance and Superiority

74. The common questions identified above predominate over any individual issues, which will relate solely to the quantum of relief due to individual class members. A class action is superior to other available means for the fair and efficient adjudication of this controversy because individual joinder of the parties is impracticable. Class action treatment will allow a large number of similarly-situated persons to prosecute their common claims in a single forum simultaneously, efficiently and without the unnecessary duplication of effort and expense if these claims were brought individually. Moreover, as the damages suffered by each class member are relatively small

in the sense pertinent to class action analysis, the expenses and burden of individual litigation would make it difficult for individual class members to vindicate their claims.

75. Additionally, important public interests will be served by addressing the matter as a class action. The cost to the court system and the public for the adjudication of individual litigation and claims would be substantially more than if claims are treated as a class action. Prosecution of separate actions by individual class members would create a risk of inconsistent and varying adjudications, establish incompatible standards of conduct for Defendant and/or substantially impair or impede the ability of class members to protect their interests. The issues in this action can be decided by means of common, class-wide proof. In addition, if appropriate, the Court can and is empowered to fashion methods to efficiently manage this action as a class action.

FIRST CAUSE OF ACTION

Violation of 740 ILCS § 14/15(a): Failure to Institute, Maintain and Adhere to Publicly-Available Retention Schedule

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

77. BIPA 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 (at most three years after the company's last interaction with the individual); and (ii) actually adhere to that retention schedule and actually delete the biometric information. *See* 740 ILCS § 14/15(a).

78. Defendant fails to comply with these BIPA mandates.

79. Defendant Rush is a corporation registered to do business in Illinois and thus qualifies as a "private entity" under BIPA. *See* 740 ILCS § 14/10.

80. Plaintiff and the Class are individuals who have had their "biometric identifiers" collected or otherwise obtained by Defendant (in the form of their fingerprints), as explained in detail in Sections II and III, *supra*. *See* 740 ILCS § 14/10.

81. Plaintiff's and the Class's biometric identifiers were used to identify them and, therefore, constitute "biometric information" as defined by BIPA. *See* 740 ILCS § 14/10.

82. Defendant failed to provide a publicly available retention schedule or guidelines for permanently destroying biometric identifiers and biometric information as specified by BIPA. *See* 740 ILCS § 14/15(a).

83. Defendant lacks retention schedules and guidelines for permanently destroying Plaintiff's and the Class's biometric data and has not and will not destroy Plaintiff's and the Class's biometric data when the initial purpose for collecting or obtaining such data has been satisfied or within three years of the individual's last interaction with the company.

84. On behalf of himself and the Class, Plaintiff seeks: (1) declaratory relief; (2) injunctive and equitable relief as is necessary to protect the interests of Plaintiff and the Class by requiring Defendant to comply with BIPA's requirements for the collection, obtainment, storage, and use of biometric identifiers and biometric information as described herein; (3) statutory damages of $5,000 for each intentional and/or reckless violation of BIPA pursuant to 740 ILCS 14/20(2) or, in the alternative, statutory damages of $1,000 for each negligent violation of BIPA pursuant to 740 ILCS 14/20(1); and (4) reasonable attorneys' fees and costs and other litigation expenses pursuant to 740 ILCS 14/20(3).

SECOND CAUSE OF ACTION

Violation of 740 ILCS § 14/15(b): Failure to Obtain Informed Written Consent and Release Before Obtaining Biometric Identifiers or Information

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

86. BIPA requires companies to obtain informed written consent from workers before acquiring their biometric data. Specifically, 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).

87. Defendant fails to comply with these BIPA mandates.

88. Defendant Rush is a corporation registered to do business in Illinois and thus qualifies as a "private entity" under BIPA. *See* 740 ILCS § 14/10.

89. Plaintiff and the Class are individuals who have had their "biometric identifiers" collected or otherwise obtained by Defendant (in the form of their fingerprints), as explained in detail in Sections II and III, *supra*. *See* 740 ILCS § 14/10.

90. Plaintiff's and the Class's biometric identifiers were used to identify them and, therefore, constitute "biometric information" as defined by BIPA. *See* 740 ILCS § 14/10.

91. Defendant systematically and automatically collected, obtained, used, stored and disseminated Plaintiff's and the Class's biometric identifiers and/or biometric information without first obtaining the written release required by 740 ILCS 14/15(b)(3).

92. Defendant did not inform Plaintiff and the Class in writing that their biometric identifiers and/or biometric information were being collected, obtained, stored, used and disseminated, nor did Defendant inform Plaintiff and the Class in writing of the specific purpose(s)

and length of term for which their biometric identifiers and/or biometric information were being collected, obtained, stored, used and disseminated as required by 740 ILCS 14/15(b)(1)-(2).

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

94. On behalf of himself and the Class, Plaintiff seeks: (1) declaratory relief; (2) injunctive and equitable relief as is necessary to protect the interests of Plaintiff and the Class by requiring Defendant to comply with BIPA's requirements for the collection, obtainment, storage, use and dissemination of biometric identifiers and biometric information as described herein; (3) statutory damages of $5,000 for each intentional and/or reckless violation of BIPA pursuant to 740 ILCS 14/20(2) or, in the alternative, statutory damages of $1,000 for each negligent violation of BIPA pursuant to 740 ILCS 14/20(1); and (4) reasonable attorneys' fees and costs and other litigation expenses pursuant to 740 ILCS 14/20(3).

THIRD CAUSE OF ACTION

Violation of 740 ILCS § 14/15(d): Disclosure of Biometric Identifiers and Information Before Obtaining Consent

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

96. BIPA prohibits private entities from disclosing a person's or customer's biometric identifier or biometric information without first obtaining consent for that disclosure. *See* 740 ILCS 14/15(d)(1).

97. Defendant fails to comply with this BIPA mandate.

98. Defendant Rush is a corporation registered to do business in Illinois and thus qualifies as a "private entity" under BIPA. *See* 740 ILCS § 14/10.

99. Plaintiff and the Class are individuals who have had their "biometric identifiers" collected or otherwise obtained by Defendant (in the form of their fingerprints), as explained in detail in Sections II and III, *supra*. *See* 740 ILCS § 14/10.

100. Plaintiff's and the Class's biometric identifiers were used to identify them and, therefore, constitute "biometric information" as defined by BIPA. *See* 740 ILCS § 14/10.

101. Defendant systematically and automatically disclosed, redisclosed, or otherwise disseminated Plaintiff's and the Class's biometric identifiers and/or biometric information without first obtaining the consent required by 740 ILCS 14/15(d)(1).

102. By disclosing, redisclosing, or otherwise disseminating Plaintiff's and the Class's biometric identifiers and biometric information as described herein, Defendant violated Plaintiff's and the Class's rights to privacy in their biometric identifiers and/or biometric information as set forth in BIPA. *See* 740 ILCS 14/1, *et seq.*

103. On behalf of himself and the Class, Plaintiff seeks: (1) declaratory relief; (2) injunctive and equitable relief as is necessary to protect the interests of Plaintiff and the Class by requiring Defendant to comply with BIPA's requirements for the collection, obtainment, storage, use and dissemination of biometric identifiers and biometric information as described herein; (3) statutory damages of $5,000 for each intentional and/or reckless violation of BIPA pursuant to 740 ILCS § 14/20(2) or, in the alternative, statutory damages of $1,000 for each negligent violation of BIPA pursuant to 740 ILCS § 14/20(1); and (4) reasonable attorneys' fees and costs and other litigation expenses pursuant to 740 ILCS § 14/20(3).

PRAYER FOR RELIEF

Wherefore, Plaintiff Corey Heard respectfully requests that this Court enter an Order:

A. Certifying this case as a class action on behalf of the Class defined above, appointing Plaintiff Corey Heard as Class Representative, and appointing Stephan Zouras, LLP as Class Counsel;

B. Declaring that Defendant's actions, as set forth above, violate BIPA;

C. Awarding statutory damages of $5,000 for *each* intentional and/or reckless violation of BIPA pursuant to 740 ILCS § 14/20(2) or, in the alternative, statutory damages of $1,000 for *each* negligent violation of BIPA pursuant to 740 ILCS § 14/20(1);

D. Declaring that Defendant's actions, as set forth above, were intentional or reckless;

E. Awarding injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and the Class, including an Order requiring Defendant to collect, obtain, store, use, destroy and disseminate biometric identifiers and/or biometric information in compliance with BIPA;

F. Awarding Plaintiff and the Class their reasonable attorneys' fees and costs and other litigation expenses pursuant to 740 ILCS § 14/20(3);

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.

Date: October 25, 2023

Respectfully Submitted,

/s/ Ryan F. Stephan

Ryan F. Stephan
James B. Zouras
Catherine Mitchell
Lauren A. Warwick
STEPHAN ZOURAS, LLP
222 W. Adams Street, Suite 2020
Chicago, Illinois 60606
312.233.1550
312.233.1560*f*
jzouras@stephanzouras.com
rstephan@stephanzouras.com
cmitchell@stephanzouras.com
lwarwick@stephanzouras.com

ATTORNEYS FOR PLAINTIFF

CERTIFICATE OF SERVICE

I, the attorney, hereby certify that on October 25, 2023, I filed the attached with the Clerk of the Court using the electronic filing system which will send such filing to all attorneys of record.

/s/ Ryan F. Stephan

ClassAction.org