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

SAMUEL LOPEZ, individually, and on behalf of all others similarly situated,	
Plaintiff,	**Case No.** 2023CH05692
v.	
ASCENSION HEALTH and ASCENSION SAINT JOSEPH-CHICAGO,	
Defendants.	

CLASS ACTION COMPLAINT

Plaintiff Samuel Lopez ("Plaintiff"), by and through his attorneys, on behalf of himself and the Class set forth below (collectively referred to as "Plaintiffs"), brings the following Class Action Complaint ("Complaint") pursuant to the Illinois Code of Civil Procedure, 735 ILCS §5/2-801 and §2-802, against Ascension Health ("Ascension") and Ascension Saint Joseph-Chicago ("Saint Joseph") (collectively referred to as "Defendants"), their subsidiaries and affiliates, to redress and curtail Defendants' unlawful collection, use, storage, and disclosure of Plaintiff's sensitive 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 Ascension Health is a private, not-for-profit health corporation headquartered in St. Louis, Missouri. Ascension Health owns, manages, and operates multiple medical locations and care centers within Illinois and Cook County including, but not limited to, Ascension Saint Joseph-Chicago, Ascension Alexian Brothers, Ascension Holy Family, Ascension

Mercy, Ascension Resurrection, Ascension Saint Alexus, Ascension Saint Mary, Ascension Saint Francis and Ascension Medical Group.

2. Defendant Ascension Saint Joseph-Chicago is a private, not-for-profit hospital located in Chicago, Illinois and operating in this Circuit. Upon information and belief, Ascension is Saint Joseph's parent company.

3. Ascension Health facilities – including Ascension Saint Joseph-Chicago – have used and continue to use biometric enabled dispensing systems, including but not limited to a Pyxis MedStation™ ES System ("Pyxis" or "Medstation") by Becton, Dickinson and Company ("BD"). BD's website describes Pyxis as "an automated medication dispensing system supporting decentralized medication management" that "helps clinicians dispense medications in a safe, efficient way and provides enterprise-ready integration capabilities previously not seen in other medication management systems."[1]

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. When employees are provided access to the Pyxis Medstations, they are enrolled in the system. Ascension Health uses the systems to monitor access to certain restricted materials, *e.g.,* pharmaceuticals.

6. All employees of Defendants who use the systems are required to first enroll scans of their fingerprint. Each subsequent time the employee needs to retrieve medicine or other items from the systems, they are required to provide a live scan of their fingerprint to be compared to their original enrollment scan saved on the device.

---

[1] *See* https://www.bd.com/en-uk/products/medication-management/point-of-care/pyxis-medstation-es-system, last accessed Nov. 17, 2022.

7. Pyxis systems are configured so that functional processing and storage of the unique user templates are shared with the servers.

8. 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 employee. This exposes employees who are required to use biometric devices, like the Pyxis devices, 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 – employees have ***no*** means by which to prevent identity theft, unauthorized tracking or other unlawful or improper use of this highly personal and private information.

9. 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.

10. 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.

11. 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.

12. 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.

13. 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.

14. Notwithstanding the clear and unequivocal requirements of the law, Defendants disregard the statutorily protected privacy rights of their employees and unlawfully collect, store, disseminate and use their employees' biometric data in violation of BIPA. Defendants violated and continue to violate BIPA, because they do not:

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.

15. 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 fingerprints were being collected, stored, disseminated and used; (2) provided a publicly available retention schedule or guidelines for permanent destruction of their biometric data; and (3) provided (nor did they execute) a written release, as required by BIPA.

16. Defendants improperly disclose their employees' fingerprint data to at least one out-of-state third-party vendor.

17. Defendants lack retention schedules and guidelines for permanently destroying Plaintiff's biometric data and have not and will not destroy Plaintiff's biometric data as required by BIPA.

18. Plaintiff and others similarly situated are aggrieved by Defendants' failure to destroy their biometric data when the initial purpose for collecting or obtaining such data has been satisfied or within three years of the employee's last interactions with Defendants.

19. Plaintiff and others similarly situated have suffered an injury in fact based on Defendants' violations of his legal rights.

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

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

22. Defendants are directly liable for, and had actual knowledge of, the BIPA violations alleged herein.

23. Accordingly, Plaintiff, on behalf of himself as well as the putative Class, seeks an Order: (1) declaring that Defendants' conduct violates BIPA; (2) requiring Defendants to cease the

unlawful activities discussed herein; and (3) awarding statutory damages to Plaintiff and the proposed Class.

PARTIES

24. Plaintiff Samuel Lopez is a natural person and a citizen in the State of Illinois.

25. Defendant Ascension Saint Joseph-Chicago is an Illinois not-for-profit corporation, and a subsidiary of Ascension Health, that is registered with the Illinois Secretary of State and conducts business in the State of Illinois, including Cook County.

26. Defendant Ascension Health is a Missouri not-for-profit corporation that is registered with the Illinois Secretary of State and conducts business in the State of Illinois, including Cook County.

JURISDICTION AND VENUE

27. This Court has jurisdiction over Defendants pursuant to 735 ILCS 5/2-209 because they conduct business transactions in Illinois, committed statutory violations and tortious acts in Illinois, and are registered to conduct business in Illinois.

28. Venue is proper in Cook County because Defendants conduct business in Cook County and committed the statutory violations alleged herein in Cook County and throughout Illinois.

FACTUAL BACKGROUND

I. The Biometric Information Privacy Act.

29. 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 weary of this then-growing yet unregulated technology. *See* 740 ILCS 14/5.

30. 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. The bankruptcy was alarming to the Illinois legislature because there was suddenly a serious risk that millions of fingerprint records – which, similar to 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 the scanners were not 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.

31. 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.

32. 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.

33. 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 or stored;

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, 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).

34. 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.

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 that 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. The Illinois legislature enacted BIPA due to the increasing use of biometric data in financial and security settings, the general public's hesitation to using 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.

39. 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, store, use, and disseminate biometric and creates a private right of action for lack of statutory compliance.

40. 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. Defendants Violate the Biometric Information Privacy Act.

41. By the time BIPA passed through the Illinois legislature in mid-2008, most companies who had experimented using employees' biometric data as an authentication method stopped doing so.

42. However, Defendants failed to take note of the shift in Illinois law governing the collection and use of biometric data. As a result, Defendants continue to collect, store, use and disseminate biometric data of the employees of Ascension Saint Joseph-Chicago in violation of BIPA.

43. Specifically, Defendants require Plaintiff and other employees to have their fingerprints collected and stored on Defendants' Pyxis systems so that Defendants can monitor employee access to medications and other items.

44. Upon information and belief, Defendants failed to inform their employees that their fingerprint data is disclosed to at least one out-of-state third-party vendor; failed to inform their employees of the purposes and duration for which it collects their sensitive biometric data; and failed to obtain written releases from their employees before collecting their fingerprints.

45. Defendant Ascension Saint Joseph-Chicago fails to inform its employees that their fingerprint data is disclosed to at least one out-of-state third-party vendor; fails to inform its employees of the purposes and duration for which it collects their sensitive biometric data; and fails to obtain written releases from its employees before collecting their fingerprints.

46. Furthermore, Defendants fail to provide their employees with a written, publicly available policy identifying their retention schedule and guidelines for permanently destroying employees' fingerprints when the initial purpose for collecting or obtaining their fingerprints is no longer relevant, as required by BIPA.

47. Defendants fail to provide their employees with a written, publicly available policy identifying their retention schedule and guidelines for permanently destroying employees' fingerprints when the initial purpose for collecting or obtaining their fingerprints is no longer relevant, as required by BIPA.

48. The Pay by Touch bankruptcy, which triggered the passage of BIPA, highlights why such conduct – where individuals are aware that they are providing a fingerprint but are not aware to whom or for what purposes they are doing so – is dangerous. This 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 their biometric data, where it will be transmitted, for what purposes it will be transmitted, and for how long.

49. Defendants disregard these obligations and the statutory rights of their employees and instead unlawfully collect, store, use and disseminate their biometric identifiers and information, without ever receiving the individuals' informed written consent required by BIPA.

50. Upon information and belief, Defendants lack retention schedules and guidelines for permanently destroying Plaintiff's biometric data and have not and will not destroy Plaintiff's biometric data when the initial purpose for collecting or obtaining such data has been satisfied or within three years of the employee's last interaction with the company.

51. Defendants' employees are not told what might happen to their biometric data if and when any Defendant merges with another company or worse, if and when any Defendants' businesses fold.

52. Since Defendants have never published a BIPA-mandated data retention policy nor disclosed the purposes for their collection of biometric data, their employees have no idea whether Defendants sold, disclosed, re-disclosed, or otherwise disseminated their biometric data. Moreover, Plaintiff is not told to whom Defendants currently disclose his biometric data to, or what might happen to his biometric data in the event of a merger or a bankruptcy.

53. These violations have raised a material risk that Plaintiff's biometric data will be unlawfully accessed by third parties.

54. By and through the actions detailed above, Defendants disregarded Plaintiff's legal rights in violation of BIPA.

III. Plaintiff Samuel Lopez's Experience

55. Plaintiff Samuel Lopez worked as an Inventory Coordinator for Ascension Saint Joseph-Chicago located at 2900 N. Lake Shore Dr., Chicago, IL, 60657. Plaintiff worked for Defendants from approximately March 2020 to March 2022.

56. As an employee of Defendants, Plaintiff was required to have his fingerprints scanned to access medications and other items for patient care.

57. Specifically, Plaintiff was required to scan and enroll his fingerprints with Defendants' Pyxis systems at Ascension Saint Jospeh-Chicago. Defendants collected and/or otherwise obtained Plaintiff's biometric data upon Plaintiff's enrollment.

58. Defendants subsequently stored Plaintiff's fingerprint data in their database(s).

59. Defendants did not obtain Plaintiff's consent before disclosing or disseminating his biometric data to third parties.

60. Neither Defendant obtained Plaintiff's consent before disclosing or disseminating his biometric data to each other through their shared database.

61. Plaintiff has never seen, been able to access, or been informed of any publicly available biometric data retention policy or guidelines developed by Defendants, nor has he ever seen, been able to access, or been informed of whether Defendants would ever permanently delete his biometric data.

62. Plaintiff has never been provided with, nor ever signed, a written release allowing Defendants to collect, capture, obtain, store, use and/or disseminate his biometric data.

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

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 representatives 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 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, 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 employees under BIPA:

> All individuals working for Defendants in the State of Illinois who had their fingerprints collected, captured, received, or otherwise obtained or disclosed by the Defendants 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 Plaintiff are typical of the claims of the class; and,

D. The 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 the payroll records of Defendants.

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 Defendants' failure to comply with BIPA. The common questions of law and fact include, but are not limited to the following:

A. Whether Defendants collected, captured or otherwise obtained Plaintiff's biometric identifiers or biometric information;

B. Whether Defendants properly informed Plaintiff of their purposes for collecting, using, and storing his 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's biometric identifiers or biometric information;

D. Whether Defendants have disclosed or re-disclosed Plaintiff's biometric identifiers or biometric information;

E. Whether Defendants have sold, leased, traded, or otherwise profited from Plaintiff's biometric identifiers or biometric information;

F. Whether Defendants developed a compliant 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 with the employee, whichever occurs first;

G. Whether Defendants comply with their written policies;

H. Whether Defendants used Plaintiff's fingerprints to identify him;

I. Whether Defendants' violations of BIPA have raised a material risk that Plaintiff's biometric data will be unlawfully accessed by third parties;

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

K. Whether the violations of BIPA were committed willfully.

b. Plaintiff anticipates that Defendants will raise defenses that are common to the class.

Adequacy

70. The 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

71. The claims asserted by the Plaintiff are typical of the class members he seeks to represent. The Plaintiff has the same interests and suffers from the same unlawful practices as the class members.

72. 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

73. 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.

74. 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 Defendants 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

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

76. 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).

77. Defendants failed to comply with this BIPA mandate.

78. Defendants are corporations registered to do business in Illinois and therefore qualify as "private entities" under BIPA. *See* 740 ILCS § 14/10.

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

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

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

82. Defendants lacked retention schedules and guidelines for permanently destroying Plaintiff's and the Class members' biometric data and did not destroy Plaintiff's and the Class's biometric data when the initial purpose for collecting or obtaining such data had been satisfied, or within three years of the individual's last interaction with the company.

83. 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 Defendants 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

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

85. BIPA requires companies to obtain informed written consent from individuals 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).

86. Defendants failed to comply with this BIPA mandate.

87. Defendants are corporations registered to do business in Illinois and therefore qualify as a "private entities" under BIPA. *See* 740 ILCS § 14/10.

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

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

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

91. Defendants did not properly inform Plaintiff and the Class members in writing that their biometric identifiers and/or biometric information were being collected, obtained, stored, used, and disseminated, nor did Defendants properly inform Plaintiff and the Class members 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).

92. By collecting, obtaining, storing, using, and disseminating Plaintiff's and Class members' biometric identifiers and biometric information as described herein, Defendants 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.*

93. 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 Defendants 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

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

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

96. Defendants failed to comply with this BIPA mandate.

97. Defendants are corporations registered to do business in Illinois and therefore qualify as "private entities" under BIPA. *See* 740 ILCS § 14/10.

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

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

100. Defendants 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).

101. By disclosing, redisclosing, or otherwise disseminating Plaintiff's and the Class members' biometric identifiers and biometric information as described herein, Defendants 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.*

102. On behalf of himself and the Class, Plaintiff seek: (1) declaratory relief; (2) injunctive and equitable relief as is necessary to protect the interests of Plaintiff and the Class by

requiring Defendants 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 Samuel Lopez 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 Samuel Lopez as Class Representative, and appointing Stephan Zouras, LLP, as Class Counsel;

B. Declaring that Defendants' 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, negligent 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 Defendants to comply with BIPA when possessing, collecting, obtaining, storing, using, destroying, and/or disseminating biometric identifiers and/or biometric information;

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 any such other and further relief as equity and justice may require.

Date: June 15, 2023

Respectfully Submitted,

/s/ Ryan F. Stephan
Ryan F. Stephan
James B. Zouras
Catherine T. Mitchell
Stephan Zouras, LLP
222 W. Adams Street, Suite 2020
Chicago, Illinois 60606
312.233.1550
312.233.1560 *f*
Firm ID: 43734
rstephan@stephanzouras.com
jzouras@stephanzouras.com
cmitchell@stephanzouras.com

CERTIFICATE OF SERVICE

I, the attorney, hereby certify that on June 15, 2023, I filed the attached with the Clerk of the Court using the ECF system, which will send such filing to all attorneys of record.

/s/ Ryan F. Stephan

ClassAction.org