YES / (NO)

EXHIBITS

CASE NO. 2019 CH 11575

DATE: 10/7/19

CASE TYPE: CLASS ACTION

PAGE COUNT: 22

CASE NOTE

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

KELLY O'SULLIVAN, individually, and on behalf of all others similarly situated,	)	
Plaintiff,	)	**Case No.** 2019CH11575
v.	)	
ALL-STAR, INC.,	)	
Defendant.	)	

CLASS ACTION COMPLAINT

Plaintiff Kelly O'Sullivan ("O'Sullivan" or "Plaintiff"), individually and on behalf of all others similarly situated (the "Class"), by and through her 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 All-Star, Inc. ("All-Star" or "Defendant"), its subsidiaries and affiliates, to redress and curtail Defendant's unlawful collection, use, storage, and disclosure of Plaintiff's sensitive and proprietary biometric data. Plaintiff alleges as follows upon personal knowledge as to herself, her own acts and experiences and, as to all other matters, upon information and belief, including investigation conducted by her attorneys.

NATURE OF THE ACTION

1. Defendant, All-Star is an Illinois corporation that owns and operates numerous franchise fast food restaurants throughout Illinois, including in this Circuit.

2. When Defendant hires an employee, including Plaintiff, he or she is enrolled in its employee database(s) using a scan of his or her fingerprint. Defendant uses the employee database(s) to monitor the time worked by its employees.

3. While many employers use conventional methods for tracking time worked (such as ID badges or punch clocks), Defendant's employees are required, as a condition of employment, to have their fingerprints scanned by a biometric timekeeping device.

4. Biometrics are not relegated to esoteric corners of commerce. Many businesses – such as Defendant's – and financial institutions have incorporated biometric applications into their workplace in the form of biometric timeclocks or authenticators, and into consumer products, including such ubiquitous consumer products as checking accounts and cell phones.

5. Unlike ID badges or time cards – which can be changed or replaced if stolen or compromised – fingerprints are unique, permanent biometric identifiers associated with each employee. This exposes Defendant's employees 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 Yahoo, eBay, Equifax, Uber, Home Depot, MyFitnessPal, Panera, Whole Foods, Chipotle, Omni Hotels & Resorts, Trump Hotels, Facebook/Cambridge Analytica, and Suprema 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.

6. 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.

7. 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 facial photographs – 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=.b3c70259fl38.

8. 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.

9. In August 2019, it was reported that South Korean biotechnology company Suprema experienced a hack of its Biostar 2 platform, which exposed the fingerprint and facial recognition data of over one million people to Israeli hackers. Chris Baraniuk, *Biostar Security Software 'Leaked a Million Fingerprints'*, BBC News (Aug. 14, 2019), available at https://www.bbc.com/news/technology-49343774.

10. In the United States, law enforcement, including the Federal Bureau of Investigation and Immigration and Customs Enforcement, have attempted to turn states' Department of Motor Vehicles databases into biometric data goldmines, using facial recognition technology to scan the faces of thousands of citizens, all without their notice or consent. Drew Harwell, *FBI, ICE Find State Driver's License Photos Are a Gold Mine for Facial-Recognition Searches*, The Washington Post (July 7, 2019), *available at* https://www.washingtonpost.com/technology/2019/07/07/fbi-ice-find-state-drivers-license-photos-are-gold-mine-facial-recognition-searches/?noredirect=on&utm_term=.da9afb2472a9.

11. This practice has been criticized by lawmakers. Some states, including Illinois, have refused to comply with law enforcement's invasive requests. *State Denying Facial Recognition Requests*, Jacksonville Journal-Courier (July 9, 2019), *available at* https://www.myjournalcourier.com/news/article/State-denying-facial-recognition-requests-14081967.php.

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, store and use Illinois citizens' biometrics, such as fingerprints.

13. Notwithstanding the clear and unequivocal requirements of the law, Defendant disregards Plaintiff's and other similarly-situated employees' statutorily protected privacy rights and unlawfully collects, stores, disseminates, and uses Plaintiff's and other similarly-situated employees' biometric data in violation of BIPA. Specifically, Defendant 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, stored, and used, as required by BIPA;

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

c. Obtain a written release from Plaintiff and others similarly situated to collect, store, disseminate, or otherwise use their 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. Accordingly, Plaintiff, on behalf of herself as well as the putative Class, 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

15. Plaintiff Kelly O'Sullivan is a natural person and a citizen of the State of Illinois.

16. Defendant All-Star is an Illinois corporation, with its principal place of business in Bourbonnais, Illinois. All-Star is registered with the Illinois Secretary of State and conducts business in the State of Illinois, including Cook County.

JURISDICTION AND VENUE

17. 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.

18. Venue is proper in Cook County because Defendant conducts business transactions in Cook County and committed the statutory violations alleged herein in Cook County.

FACTUAL BACKGROUND

I. The Biometric Information Privacy Act.

19. 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.

20. 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.

21. 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.

22. 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.

23. 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, 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).

24. 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.

25. 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*.

26. BIPA 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).

27. 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).

28. 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 a heightened risk for identity theft and left without any recourse.

29. 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 biometrics and creates a private right of action for lack of statutory compliance.

30. 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.

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

32. However, Defendant failed to take note of the shift in Illinois law governing the collection, use, storage, and dissemination of biometric data. As a result, Defendant continues to collect, store, use and disseminate its employees' biometric data in violation of BIPA.

33. Specifically, when employees are hired at one of All-Star's franchise locations, Defendant requires them to have their fingerprint scanned to enroll them in its employee database(s).

34. Upon information and belief, Defendant requires its franchise locations to use an employee time tracking system that requires employees to use their fingerprint as a means of

authentication. In accordance with Defendant's policy, employees are required to use their fingerprints to clock-in and clock-out, recording their time worked.

35. Upon information and belief, Defendant fails to inform employees that it collects, stores, and uses their fingerprint data; fails to inform employees that it discloses or disclosed their fingerprint data to at least one third-party vendor and likely others; fails to inform employees that it discloses their fingerprint data to other, currently unknown, third parties, which host the biometric data in their data centers; fails to inform employees of the purposes and duration for which it collects their sensitive biometric data; and, fails to obtain written releases from employees before collecting their fingerprints.

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

37. The Pay by Touch bankruptcy that catalyzed the passage of BIPA, as well as the recent data breaches, highlight why such conduct – where individuals are aware that they are providing a fingerprint, but not aware of 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 their biometric data, where it will be transmitted, for what purposes, and for how long. Defendant disregards these obligations and employees' statutory rights and instead unlawfully collects, stores, uses, and disseminates employees' biometric identifiers and information, without first receiving the individual's informed written consent required by BIPA.

38. Upon information and belief, 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 Plaintiff's and other similarly-situated individuals' 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.

39. Defendant does not tell Plaintiff and others similarly situated what might happen to their biometric data if and when Defendant merges with another company, or worse, if and when Defendant's business folds, or when the other third parties that have received employees' biometric data businesses fold.

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

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

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

III. Plaintiff Kelly O'Sullivan's Experience

43. Plaintiff Kelly O'Sullivan had her fingerprint data collected by All-Star when she worked as a Crew Member from August 2014 until approximately August 2017 at its Wendy's facility located at 2430 E. Lincoln Highway, New Lenox, IL 60451.

44. As a condition of her employment, Plaintiff was required to scan her fingerprint so Defendant could use it as an authentication method to track her time and breaks.

45. Defendant stores Plaintiff's fingerprint data in its employee database(s).

46. Plaintiff was required to scan her fingerprint each time she began and ended her workday, as well as each time she clocked in and out for breaks.

47. Defendant did not inform Plaintiff in writing or otherwise of the purpose(s) and length of time for which her fingerprint data was being collected, did not receive a written release from Plaintiff to collect, store, or use her fingerprint data, did not publish a publicly available retention schedule and guidelines for permanently destroying Plaintiff's fingerprint data, and did not obtain Plaintiff's consent before disclosing or disseminating her biometric data to third parties.

48. Plaintiff has never been informed of the specific limited purposes or length of time for which Defendant collects, stores, uses and/or disseminates her biometric data.

49. Plaintiff has never been informed of any biometric data retention policy developed by Defendant and made available to the public, nor had she ever been informed of whether Defendant would ever permanently delete her biometric data.

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

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

52. No amount of time or money can compensate Plaintiff if her biometric data has been compromised by the lax procedures through which Defendant captures, stores, uses, and disseminates her and other similarly-situated individuals' biometrics. Moreover, Plaintiff would

not have provided her biometric data to Defendant if she had known that Defendant would retain such information for an indefinite period of time without her consent.

53. 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").

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

CLASS ALLEGATIONS

55. Pursuant to the Illinois Code of Civil Procedure, 735 ILCS § 5/2-801, Plaintiff brings claims on her 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.

56. 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(s) 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.

57. 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 in the State of Illinois who had their biometric identifiers and/or biometric information collected, captured, received, or otherwise obtained, maintained, stored, or disclosed by Defendant during the applicable statutory period.

58. 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. Plaintiff's claims are typical of the claims of the class; and,

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

Numerosity

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

Commonality

60. 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, maintained, stored 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, using, storing and disseminating their biometric identifiers or biometric information;

C. Whether Defendant properly obtained a written release (as defined in 740 ILCS § 14/10) to collect, use, store and disseminate Plaintiff's and the

Class's biometric identifiers or biometric information;

D. Whether Defendant has disclosed or redisclosed 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 complies with any such written policy (if one exists);

H. Whether Defendant's violations of BIPA have raised a material risk that Plaintiff's and the putative Class' biometric data will be unlawfully accessed by third parties;

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 or recklessly.

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

Adequacy

62. 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

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

members.

64. 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

65. 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.

66. 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

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

68. 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).

69. Defendant fails to comply with these BIPA mandates.

70. Defendant qualifies as a "private entity" under BIPA. *See* 740 ILCS § 14/10.

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

72. 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.

73. Defendant failed to publish 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).

74. Upon information and belief, 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 or 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.

75. On behalf of herself 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, 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

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

77. 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).

78. Defendant fails to comply with these BIPA mandates.

79. Defendant 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 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 systematically and automatically collected, 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).

83. Defendant did not inform Plaintiff and the Class in writing that their biometric identifiers and/or biometric information were being collected, 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, stored, used, and disseminated as required by 740 ILCS § 14/15(b)(1)-(2).

84. By collecting, storing, and using 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 or biometric information as set forth in BIPA. *See* 740 ILCS § 14/1, *et seq*.

85. On behalf of herself 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, 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).

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

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

87. 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).

88. Defendant fails to comply with this BIPA mandate.

89. Defendant qualifies as a "private entity" under BIPA. *See* 740 ILCS § 14/10.

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

91. 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.

92. 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).

93. 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 or biometric information as set forth in BIPA. *See* 740 ILCS § 14/1, *et seq.*

94. On behalf of herself 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, 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 Kelly O'Sullivan 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 Kelly O'Sullivan 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 and/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, store, use 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 7, 2019

Respectfully Submitted,

/s/ Haley R. Jenkins

Ryan F. Stephan
Haley R. Jenkins
Stephan Zouras, LLP
100 N. Riverside Plaza, Suite 2150
Chicago, Illinois 60606
312.233.1550
312.233.1560 *f*
rstephan@stephanzouras.com
hjenkins@stephanzouras.com
Firm ID: 43734
ATTORNEYS FOR PLAINTIFF

CERTIFICATE OF SERVICE

I, the attorney, hereby certify that on October 7, 2019, I electronically 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/ Haley R. Jenkins