

YES / NO

EXHIBITS

CASE NO. 2019 CH 14014

DATE: 12/5/19

CASE TYPE: CLASS ACTION

PAGE COUNT: 22

CASE NOTE

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

MICHELE JOHNSON, individually,)
and on behalf of all others similarly situated,)

7610205

Plaintiff,)

Case No. 2019CH14014

v.)

OM JOLIET WINGS, INC. and KALPESH)
PATEL,)

Defendant.)

CLASS ACTION COMPLAINT

Plaintiff Michele Johnson (“Johnson” or “Plaintiff”), by and through her attorneys, individually and on behalf of all others similarly situated (the “Class”), brings the following Class Action Complaint (“Complaint”) pursuant to the Illinois Code of Civil Procedure, 735 ILCS §§ 5/2-801 and 2-802, against OM Joliet Wings, Inc. (“Joliet Wings”) and Kalpesh Patel (“Patel”) (collectively “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 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 OM Joliet Wings, Inc. is a franchisee of Wingstop. Defendant owns and operates a Wingstop located in Joliet, Illinois.
2. Defendant Kalpesh Patel is the owner and operator of Defendant OM Joliet Wings, Inc. and at least 6 other Wingstop restaurants including OM South Holland Wings, Inc., OM

FILED DATE: 12/5/2019 11:08 AM 2019CH14014

Lansing Wings, Inc., OM Kedzie Wings, Inc., OM Broadway Wings, Inc., and OM Milwaukee Wings, Inc.

3. Upon information and belief, when Defendants or one of its affiliated facilities hires an employee, including Plaintiff, he or she is enrolled in an employee database shared and maintained by and between Defendants and the affiliate facilities to monitor the time worked by hourly employees.

4. While many employers use conventional methods for tracking time worked (such as ID badge swipes or punch clocks), Defendants' and their affiliated facilities' employees are required to have their fingerprints scanned by a biometric timekeeping device.

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. Biometrics are not relegated to esoteric corners of commerce. Many businesses – such as Defendants – 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.

7. 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 <https://www.opm.gov/cybersecurity/cybersecurity-incidents>.

8. 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. 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 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.

10. 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>.

11. In August 2018, it was widely reported that Suprema, a security company responsible for a web-based biometrics lock system that uses fingerprints and facial geometry scans in 1.5 million locations around the world, maintained biometric data and other personal information on a publicly accessible, unencrypted database. *Major Breach Found in Biometrics System Used by Banks, UK police and Defense Firms*, The Guardian (Aug. 14, 2019), available at <https://www.theguardian.com/technology/2019/aug/14/major-breach-found-in-biometrics-system-used-by-banks-uk-police-and-defence-firms>.

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 and store Illinois citizens' biometrics, such as fingerprints.

13. Notwithstanding the clear and unequivocal requirements of the law, Defendants disregard employees' statutorily protected privacy rights and unlawfully collect, store, disseminate, and use their employees' biometric data in violation of BIPA. Specifically, Defendants have violated and continue to violate BIPA because they did not and continue 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, disseminated and used, as required by BIPA;
- b. Provide a publicly available retention schedule and guidelines for permanently destroying Plaintiff's and other similarly-situated individuals' fingerprints, as required by BIPA;

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

15. Plaintiff Michele Johnson is a natural person and a citizen in the State of Illinois.

16. Defendant Joliet Wings is a corporation that is registered with the Illinois Secretary of State and conducts business in the State of Illinois.

17. Defendant Kalpesh Patel owns and operates Joliet Wings in the State of Illinois.

JURISDICTION AND VENUE

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

19. Venue is proper in Cook County because Defendants conduct business transactions in Cook County, own and operate locations in Cook County, and committed the statutory violations alleged herein in Cook County and throughout Illinois.

FACTUAL BACKGROUND

I. The Biometric Information Privacy Act

20. 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.

21. 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 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.

22. 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.

23. 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.

24. 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).

25. 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.

26. 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.*

27. 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).

28. 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).

29. 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.

30. 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.

31. 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.

32. 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.

33. However, Defendants failed to take note of the shift in Illinois law governing the collection, use, and dissemination of biometric data. As a result, Defendants continue to collect, store, use, and disseminate employees' biometric data in violation of BIPA.

34. Specifically, when employees are hired at one of Defendants' facilities, they are required to have their fingerprints scanned to enroll them in its employee database(s).

35. Upon information and belief, all hourly employees at Defendants' facilities are required to use their fingerprint to clock-in and clock-out for attendance purposes.

36. Upon information and belief, Defendants' facilities disseminate employees' biometric identifiers and/or information to a third-party vendor.

37. Upon information and belief, Defendants failed, and continue to fail, to inform their employees that they disclose or disclosed their fingerprint data to at least one third-party vendor for payroll purposes, and likely others; fail to inform employees that they disclose their fingerprint data to other, currently unknown, third parties, which host the biometric data in their data centers; fail to inform employees of the purposes and duration for which they collect their sensitive biometric data; and fail to obtain written releases from employees before collecting their fingerprint data.

38. Furthermore, Defendants failed to publish 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

39. 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. 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 it will be transmitted, and for how long. Defendants disregard these obligations and its employees' statutory rights and instead unlawfully collect, store, use, and disseminate employees' biometric identifiers and information, without ever receiving the individual's informed written consent required by BIPA.

40. Upon information and belief, Defendants lack retention schedules and guidelines for permanently destroying Plaintiff's and other similarly-situated individuals' biometric data and have 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 individual's last interaction with the company.

41. Plaintiff and those similarly situated are not told what might happen to their biometric data if and when Defendants merge with another company or worse, if and when Defendants' businesses fold, or when the other third parties that have received employees' biometric data businesses fold.

42. Since Defendants neither publish a BIPA-mandated data retention policy nor disclose the purposes for their collection and use of biometric data, Defendants' and their facilities' employees have no idea the extent to whom Defendants sell, disclose, re-disclose, or otherwise disseminate their biometric data. Moreover, Plaintiff and others similarly situated are not told to whom Defendants currently disclose their biometric data to, or what might happen to their biometric data in the event of a merger or a bankruptcy.

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

44. By and through the actions detailed above, Defendants disregarded Plaintiff's and other similarly-situated individuals' legal rights in violation of BIPA.

III. Plaintiff Michele Johnson's Experience

45. Plaintiff Michele Johnson worked as a Cook at Joliet Wings' Wingstop, located at 2410 W Jefferson Street, Joliet IL. 60435, from October to November of 2019.

46. As a condition of employment, Johnson *was required* to scan her fingerprint so Defendants could use it as an authentication method to track her time.

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

48. Plaintiff was required to scan her fingerprint each time she clocked in for work and clocked out of work.

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

50. Plaintiff has never been informed of any written, publicly available biometric data retention policy developed by Defendants, nor has she ever been informed of whether Defendants will ever permanently delete her biometric data.

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

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

53. No amount of time or money can compensate Plaintiff if her biometric data is compromised by the lax procedures through which Defendants captured, stored, used, and

disseminated her and other similarly-situated individuals' biometrics. Moreover, Plaintiff would not have provided her biometric data to Defendants if she had known that they would retain such information for an indefinite period of time without her consent.

54. 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”).

55. 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 Defendants. *Rosenbach*, 2019 IL 123186, ¶ 40.

CLASS ALLEGATIONS

56. 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.

57. 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.

58. 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 for one or more Defendants or any of its affiliated facilities in the State of Illinois who had their fingerprints collected, captured, received, obtained, maintained, stored, or disclosed by Defendants during the applicable statutory period.

59. 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

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

Commonality

61. 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 and the Class's biometric identifiers or biometric information;
- B. Whether Defendants properly informed Plaintiff and the Class of its purposes for collecting, using, storing, and disseminating their biometric identifiers or biometric information;
- C. Whether Defendants 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 Defendants have disclosed or re-disclosed Plaintiff's and the Class's biometric identifiers or biometric information;
- E. Whether Defendants have sold, leased, traded, or otherwise profited from Plaintiff's and the Class's biometric identifiers or biometric information;
- F. Whether Defendants developed a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within three years of its last interaction with the individual, whichever occurs first;
- G. Whether Defendants comply with any such written policy (if one exists);
- H. Whether Defendants used Plaintiff's and the Class's fingerprints to identify them;
- I. Whether Defendants' violations of BIPA have raised a material risk that Plaintiff's and the Class'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 intentionally and/or recklessly.

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

Adequacy

63. 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

64. 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.

65. 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

66. 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.

67. 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 a Written, Publicly-Available Retention Schedule

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

69. 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).

70. Defendants fail to comply with these BIPA mandates.

71. Defendant Joliet Wings is a corporation registered to do business in Illinois during the statutory period and thus qualifies as a “private entity” under BIPA. *See* 740 ILCS § 14/10.

72. Defendant Patel is a “private entity” under the Biometric Information Privacy Act. 740 ILCS 14/10.

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

74. 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.

75. Defendants 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).

76. Upon information and belief, Defendants lack 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.

77. 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 Defendants 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

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

79. 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).

80. Defendants fail to comply with these BIPA mandates.

81. Defendant Joliet Wings is a corporation registered to do business in Illinois during the statutory period and thus qualifies as a “private entity” under BIPA. *See* 740 ILCS § 14/10.

82. Defendant Patel is a “private entity” under the Biometric Information Privacy Act. 740 ILCS 14/10.

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

84. 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.

85. Defendants 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).

86. Defendants 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 Defendants 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).

87. By collecting, storing, using, and disseminating Plaintiff's and the Class's 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.*

88. 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 Defendants 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)

THIRD CAUSE OF ACTION

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

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

90. 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).

91. Defendants fail to comply with this BIPA mandate.

92. Defendant Joliet Wings is a corporation registered to do business in Illinois during the statutory period and thus qualifies as a "private entity" under BIPA. *See* 740 ILCS § 14/10.

93. Defendant Patel is a "private entity" under the Biometric Information Privacy Act. 740 ILCS 14/10.

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

95. 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.

96. 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).

97. By disclosing, redisclosing, or otherwise disseminating Plaintiff’s and the Class’s 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.*

98. 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 Defendants 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 Michele Johnson 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 Michele Johnson 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 Defendants’ 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 Defendants to collect, 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: December 5, 2019

Respectfully Submitted,

/s/ Megan E. Shannon

Ryan F. Stephan
STEPHAN ZOURAS, LLP
 100 N. Riverside Plaza
 Suite 2150
 Chicago, Illinois 60606
 312.233.1550
 312.233.1560 *f*
 Firm ID: 43734
 mshannon@stephanzouras.com
 rstephan@stephanzouras.com

**ATTORNEYS FOR PLAINTIFF
AND THE PUTATIVE CLASS**

CERTIFICATE OF SERVICE

I, the attorney, hereby certify that on December 5, 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/ Megan E. Shannon

ClassAction.org

This complaint is part of ClassAction.org's searchable class action lawsuit database and can be found in this post: [Wingstop Franchisee Illegally Collected Employees' Biometric Information, Class Action Claims](#)
