

Return Date: No return date scheduled
Hearing Date: 1/22/2020 10:00 AM - 10:00 AM
Courtroom Number: N/A
Location: District 1 Court
Cook County, IL

FILED
1/22/2020 12:49 PM
DOROTHY BROWN
CIRCUIT CLERK
COOK COUNTY, IL
2019CH10636

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

**FAITH MENDENHALL, individually,)
and on behalf of all others similarly situated,)**

8175823

Plaintiff,)

Case No. 2019-CH-10636

v.)

**TOMS King (Illinois), LLC, and TOMS King,)
LLC,)**

Defendants.)

FIRST AMENDED CLASS ACTION COMPLAINT

Plaintiff Faith Mendenhall (“Mendenhall” or “Plaintiff”), by and through her attorneys, individually and on behalf of all others similarly situated (the “Class”), brings the following Amended Class Action Complaint (“Amended Complaint”) pursuant to the Illinois Code of Civil Procedure, 735 ILCS §§ 5/2-801 and 2-802, against TOMS King (Illinois), LLC and TOMS King, LLC (collectively, “Defendants”), their subsidiaries and affiliates, to redress and curtail Defendants’ 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 TOMS King (Illinois), LLC is a franchisee of the Burger King Corporation. TOMS King (Illinois), LLC owns and operates over a dozen Burger King locations throughout Illinois.

FILED DATE: 1/22/2020 12:49 PM 2019CH10636

2. Defendant TOMS King, LLC is the parent company and owner of TOMS King (Illinois), LLC.

3. When Defendants or one of their franchise locations hire an employee, including Plaintiff, he or she is enrolled in their employee database(s) using a scan of his or her fingerprint. Defendants use the employee database(s) to monitor the time worked by their hourly employees.

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

5. 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 or authenticators, and into consumer products, including such ubiquitous consumer products as checking accounts and cell phones.

6. 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 Defendants' 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, and Facebook/Cambridge Analytica 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.

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 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 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=.b3c70259f138.

9. 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>.

10. 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.

11. Notwithstanding the clear and unequivocal requirements of the law, Defendants disregard their employees’ statutorily protected privacy rights and unlawfully collect, store, disseminate, and use 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, 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; and
- c. Receive a written release from Plaintiff and others similarly situated to collect, store, disseminate, 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.

12. Accordingly, Plaintiff, on behalf of herself 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

13. Plaintiff Faith Mendenhall is a natural person and a citizen of the State of Illinois.

14. Defendant TOMS King (Illinois), LLC is a corporation that conducts business in the State of Illinois with its principal place of business in Cook County.

15. Defendant TOMS King, LLC is a corporation that conducts business in the State of Illinois and throughout Cook County, with its principal place of business in Illinois.

JURISDICTION AND VENUE

16. This Court has jurisdiction over Defendants pursuant to 735 ILCS § 5/2-209 because Defendants conduct business transactions in Illinois, committed the statutory violations alleged herein in Cook County and throughout Illinois, are registered to and do conduct business in Illinois.

17. Venue is proper in Cook County because Defendants conduct business in this State, conduct business transactions in Cook County, and committed the statutory violations alleged herein in Cook County and throughout Illinois.

FACTUAL BACKGROUND

I. The Biometric Information Privacy Act.

18. 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.

19. 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 that company’s fingerprint scanners were completely unaware that the scanners were not actually transmitting fingerprint data to the retailer who deployed the scanner, but rather to the now-bankrupt company, and that their unique biometric identifiers could now be sold to unknown third parties.

20. 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.

21. 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.

22. 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 or 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).

23. 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.

24. Biometric identifiers include retina and iris scans, voiceprints, fingerprints and facial 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.*

25. 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 disclosures. *See* 740 ILCS § 14/15(d)(1).

26. 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).

27. 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.

28. BIPA provides individuals with a private right of action, protecting their right to privacy regarding their biometrics. BIPA also protects individuals' rights to know the precise nature for which their biometrics are used and how they are being stored and ultimately destroyed, allowing individuals to make a truly informed choice. 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.

29. 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.

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

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

32. Specifically, when employees are hired, Defendants or one of their franchise locations require them to have their fingerprints scanned to enroll them in their employee database(s).

33. Defendants use an employee time tracking system that requires employees to use their fingerprint as a means of authentication. In accordance with Defendants' policy, all hourly employees are required to use their fingerprints to clock-in and clock-out, recording their time worked.

34. Defendants failed to inform any employees that they disclose or disclosed their fingerprint data to third-parties, including third parties which host the biometric data in their data centers, and failed to inform their employees of the purposes and duration for which they collect their sensitive biometric data.

35. At no time did Defendants secure written releases from employees before collecting their fingerprints.

36. Furthermore, Defendants fail to provide 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.

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. 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, and for how long. Defendants disregard these obligations and employees' statutory rights and instead unlawfully collects, stores, uses and disseminates franchise employees' biometric identifiers and information, without ever receiving the individual's informed written consent required by BIPA.

38. 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 employee's last interaction with the company.

39. Plaintiff and others 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' business folds, or when the other third parties that have received employees' biometric data businesses fold.

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

41. These violations have raised 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, Defendants disregarded Plaintiff's and other similarly-situated individuals' legal rights in violation of BIPA.

III. Plaintiff Faith Mendenhall's Experience

43. Plaintiff Faith Mendenhall worked for TOMS King (Illinois), LLC as an hourly-paid staff member from March 2019 to June 2019 at its Burger King franchise location located at 159 US Highway 45 Grayslake, IL 60030.

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

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

46. Plaintiff was required to scan her fingerprint each time she began and ended her workday.

47. Plaintiff was never informed of the specific limited purposes or length of time for which Defendants collect, store, use and/or disseminate her biometric data.

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

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

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

51. 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 Defendants would retain such information for an indefinite period of time without her consent.

52. 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”).

53. 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

54. 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.

55. 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.

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

All individuals working in the State of Illinois who had their fingerprints collected, captured, received, or otherwise obtained or disclosed by one or more of the Defendants during the applicable statutory period.

57. 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

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

Commonality

59. 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, received or otherwise obtained Plaintiff's and the Class's biometric identifiers or biometric information;
- B. Whether Defendants properly informed Plaintiff and the Class of their 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 redisclosed 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 their last interaction with the individual, whichever occurs first;
- G. Whether Defendants complied with any such written policy (if one exists);
- H. Whether Defendants' 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 Defendants 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.
60. Plaintiff anticipates that Defendants will raise defenses that are common to the class.

Adequacy

61. 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

62. 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.

63. 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

64. 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.

65. 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

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

67. 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).

68. Defendants fail to comply with these BIPA mandates.

69. Each Defendant qualifies as a “private entity” under BIPA. *See* 740 ILCS § 14/10.

70. 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.

71. 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.

72. 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).

73. Upon information and belief, Defendants lack retention schedules and guidelines for permanently destroying Plaintiff’s and the Class’s biometric data and have 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.

74. 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

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

76. 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).

77. Defendants fail to comply with these BIPA mandates.

78. Each Defendant qualifies as a “private entity” under BIPA. *See* 740 ILCS § 14/10.

79. 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.

80. 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.

81. 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).

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

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

84. 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).

THIRD CAUSE OF ACTION

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

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

86. 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).

87. Defendants fail to comply with this BIPA mandate.

88. Each Defendant qualifies as a “private entity” under BIPA. *See* 740 ILCS § 14/10.

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

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

91. 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).

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

93. 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 Faith Mendenhall 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 Faith Mendenhall 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 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 Defendants 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: January 22, 2020

Respectfully Submitted,

/s/ Megan E. Shannon

Ryan F. Stephan
James B. Zouras
Megan E. Shannon
STEPHAN ZOURAS, LLP
100 N. Riverside Plaza
Suite 2150
Chicago, Illinois 60606
312.233.1550
312.233.1560 *f*
rstephan@stephanzouras.com
jzouras@stephanzouras.com
mshannon@stephanzouras.com

Firm ID: 43734
ATTORNEYS FOR PLAINTIFF

FILED DATE: 1/22/2020 12:49 PM 2019CH10636

CERTIFICATE OF SERVICE

I, the attorney, hereby certify that on January 22, 2020, 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