☐ YES ☑ NO

EXHIBITS

CASE NO. 2020 CH 6036

DATE: 9/28/2020

CASE TYPE: Class Action

PAGE COUNT: 20

CASE NOTE

_____

_____

_____

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

MICHAEL JERINIC, individually, and on behalf of all others similarly situated,	)	
Plaintiff,	)	**Case No.** 2020CH06036
v.	)	
AMAZON.COM, INC. and AMAZON.COM, LLC.,	)	
Defendants.	)	

CLASS ACTION COMPLAINT

Plaintiff Michael Jerinic ("Plaintiff"), individually and on behalf of all others similarly situated (the "Class"), bring the following Class Action Complaint ("Complaint") pursuant to the Illinois Code of Civil Procedure, 735 ILCS §§ 5/2-801 and 2-802, against Amazon.com, Inc. and Amazon.com, LLC. ("Amazon" or "Defendant") 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 himself, his own acts and experiences and, as to all other matters, upon information and belief, including investigation conducted by his attorneys.

NATURE OF THE ACTION

1. Amazon.com, Inc. and Amazon.com, LLC., commonly known as "Amazon," is a leading multinational technology company, specializing in e-commerce, cloud-based servicing, streaming and artificial intelligence. It is considered one of the "Big Four" technology companies, alongside Google, Apple and Facebook.

2. Amazon has thousands of fulfillment centers and warehouses throughout the world, that service Amazon customers, including many in the State of Illinois.

3. Named Plaintiff, Michael Jerinic worked for Amazon as a Yard Marshall from November 2018 to August 2020 at one of its fulfillment warehouses located in Mundelein, Illinois.

4. In approximately June, 2020 and in response to growing safety concerns related to the COVID-19 pandemic, Amazon began requiring its workers, including Plaintiff, to provide a scan of their facial geometry, and possibly other biometric information, as part of a wellness check prior to being allowed access to the facility each day.

5. Plaintiff was required to have his facial geometry scanned by a facial recognition camera and have his temperature taken, before being allowed entry to the warehouse.

6. Upon information and belief, Defendant uses facial recognition devices and associated software at their fulfillment centers and warehouse locations throughout Illinois.

7. Defendant's facial recognition devices and associated software collect and capture biometric identifiers such as scans of an individual's facial geometry, retinas, and irises. Defendant also scans and records the workers' temperatures.

8. Facial geometry and other biometrics are unique and personal identifiers that cannot be changed.

9. As a result of Defendant's conduct, Plaintiff and the putative Class lost the right to control the collection, use, and storage of their biometric identifiers and information and were exposed to ongoing, serious, and irreversible privacy risks—simply by going into work.

10. Databases containing sensitive, proprietary biometric data can be hacked, breached, or otherwise exposed, as in the recently publicized Clearview AI, Suprema, and Facebook/Cambridge Analytica data breaches.

11. An illegal market 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.[1] 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.[2]

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 facial geometry scans.

13. Notwithstanding the clear and unequivocal requirements of the law, and despite being one of the leading forces in the technology sector, Amazon knowingly disregards Plaintiff's and other similarly situated employees' statutorily protected privacy rights and unlawfully collects, obtains, stores, disseminates, and uses Plaintiff's and other's similarly situated biometric data in violation of BIPA. Specifically, Defendant violated and continues to violate BIPA because they did not and continue not to:

a. Properly inform Plaintiff and others similarly situated in writing that biometric identifiers or biometric information are being collected, obtained or stored, as required by BIPA;

b. Properly inform Plaintiff and others similarly situated in writing of the specific purpose and length of time for which their facial scans and other biometric identifiers or biometric information were being collected, obtained, stored, and used, as required by BIPA;

c. Develop and adhere to a publicly available retention schedule and guidelines for permanently destroying Plaintiff's and other's similarly

[1] *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.

[2] 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.

situated facial scans and other biometric identifiers or biometric information, as required by BIPA;

d. Obtain a written release from Plaintiff and others similarly situated to collect, obtain, capture, or otherwise obtain their facial scans and other biometric identifiers or biometric information, as required by BIPA; and

e. Obtain consent from Plaintiff and others similarly situated to disclose, redisclose, or otherwise disseminate their facial scans and other biometric identifiers or biometric information to a third party, as required by BIPA.

14. Accordingly, Plaintiff, on behalf of himself as well as the putative Class, seeks an Order: (1) declaring that Amazon's conduct violates BIPA; (2) requiring Defendant's to cease the unlawful activities discussed herein; and (3) awarding statutory damages to Plaintiff and the putative Class.

PARTIES

15. Plaintiff Michael Jerinic is a natural person and at all relevant times was a resident of the State of Illinois.

16. Defendant Amazon.com, Inc. is a Delaware corporation that is registered to do business in Illinois.

JURISDICTION AND VENUE

17. This Court has jurisdiction over Defendant pursuant to 735 ILCS § 5/2-209 because Defendant conducts business in Illinois, has locations in Illinois, and committed statutory violations alleged herein in Cook County, Illinois.

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

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 [sic] 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—including at retail grocery stores—filed for bankruptcy. That bankruptcy alarmed 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 to third parties 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 Pay by Touch, 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 <u>each</u> 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 that 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, obtained, stored, and used;

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

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

See 740 ILCS § 14/15(b).

24. Biometric identifiers include facial scans, retina and iris scans, voiceprints, scans of hands, and fingerprints. *See* 740 ILCS § 14/10. Biometric information is defined separately to include any information based on an individual's biometric identifier that is used to identify an individual. *Id.*

25. BIPA establishes standards for how companies must handle 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).

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—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 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.

29. Plaintiff, like the Illinois legislature, recognize 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.

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

31. 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 their employees' biometric data in violation of BIPA.

32. In 2019, Amazon faced a similar lawsuit alleging that Amazon's "Alexa" devices retained minor users' voice prints and information without proper consent in violation of BIPA. There, Amazon was accused by guardians of minors of unlawful collection, use, storage and disclosure of minor users' biometric data through the use of its "Alexa" devices and voice printing system.

33. Yet, despite these prior accusations and Defendant's knowledge of BIPA, here, when employees arrive at the Amazon facility and/or warehouse, their facial identifiers and geometry are scanned, tracked, and uploaded.

34. Defendant fails to inform its employees that it is collecting, obtaining or storing biometric data; fails to inform employees of the specific purposes and duration for which it collects and obtains their sensitive biometric data; fails to obtain written releases from employees before collecting or obtaining their sensitive biometric data; and fails to inform employees that it discloses their sensitive biometric data to other Amazon entities, to the third-party biometric device and software vendor(s), and to other, currently unknown, third parties, which, *inter alia*, host and/or analyze the biometric data.

35. Defendant also 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 has been satisfied or within three years of the individual's last interaction with the Defendant, whichever occurs first, as required by BIPA.

36. The Pay by Touch bankruptcy that catalyzed the passage of BIPA, as well as the recent data breaches, highlights why such conduct—where individuals are aware they are providing a biometric identifier, 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 how

crucial it is for individuals to understand when providing biometric identifiers, such as facial scans, who exactly is collecting their biometric data, where the biometric data will be transmitted and for what purposes, and how long the biometric data will be retained. Defendant disregards these obligations and employees' statutory rights and instead unlawfully collects, stores, uses, and disseminates employees' biometric identifiers and information, all without receiving the informed written consent required by the BIPA.

37. Defendant lacks retention schedules and guidelines for permanently destroying Plaintiff's and the putative Class's biometric data and has not and will not destroy Plaintiff's and the putative Class's biometric data as required by BIPA.

38. Defendant fails to inform its workers what will happen to their biometric data in the event Defendant merges with another company or ceases operations, or what will happen in the event the third parties that receive, store, and/or manage Plaintiff's and the putative Class's biometric data from Defendant cease operations.

39. These violations of BIPA raise a material risk that Plaintiff's and the putative Class's biometric data will be unlawfully accessed by third parties.

40. By and through the actions detailed above, Defendant disregards Plaintiff's and the putative Class's legal rights in violation of BIPA.

41. Defendant knew, including through their involvement in previous BIPA litigation, that the aforementioned actions were in direct violation of BIPA, yet they implemented and continued their practice of violating Plaintiff's and the putative Class's legal rights without regard to the law.

III. Plaintiff's Experience

42. Plaintiff worked for Amazon at its fulfillment warehouse located in Mundelein, IL, From November 2019 to August 2020.

43. These facial recognition devices are utilized to scan employees' facial geometry and take their temperature prior to entering the facility for work.

44. Defendant collects, captures, or otherwise obtains and stores Plaintiff's biometric data, including facial geometry scans and other biometric identifiers, in a database.

45. Amazon discloses Plaintiff's sensitive biometric data to other entities, third-party biometric device and software vendor(s), and to other, currently unknown, third parties, which, *inter alia*, host and/or analyze the biometric data.

46. Defendant never (1) informed Plaintiff in writing or otherwise that it was collecting, obtaining or storing their biometric data or of the specific purpose(s) and length of time for which his biometric data was being collected; (2) received a written release from Plaintiff to collect, obtain, store, or use his biometric data; developed or adhered to a publicly available retention schedule and guidelines for permanently destroying Plaintiff's biometric data; or obtained Plaintiff's consent for any disclosure or dissemination of his biometric data to third parties.

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

48. Plaintiff has never seen, been made aware of, or been able to find, view, or access a publicly available biometric data retention policy developed by Defendant, nor has he ever seen, been made aware of, or been able to find, view, or access any policies regarding whether Defendant will ever permanently delete his biometric data.

49. No retention schedules or destruction guidelines relating to biometric data were in Plaintiff's onboarding materials when he began working for Amazon.

50. No retention schedules or destruction guidelines relating to biometric data are available to Plaintiff on a company intranet.

51. No retention schedules or destruction guidelines relating to biometric data are posted on the premises.

52. No employees at Amazon's warehouse has ever informed Plaintiff of, or provided Plaintiff with, any retention schedules or destruction guidelines relating to biometric data obtainment.

53. Plaintiff has not been provided with nor ever signed a written release allowing Defendant to collect, capture, obtain, store, use, or disseminate his biometric data.

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

55. No amount of time or money can compensate Plaintiff if his biometric data has been compromised by the intentional, reckless, and/or negligent procedures through which Defendant captures, stores, uses, and disseminates his and the putative Class's biometric data. Moreover, Plaintiff would not have provided his biometric data to Defendant if he had known Defendant would retain such information for an indefinite period of time without his consent.

56. A showing of actual damages is not necessary in order to state a claim under BIPA. *See Rosenbach v. Six Flags Entm't 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").

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

CLASS ALLEGATIONS

58. Pursuant to the Illinois Code of Civil Procedure, 735 ILCS § 5/2-801, Plaintiff brings claims on his own behalf and as 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 for the violations described herein.

59. Under the Illinois Code of Civil Procedure, 735 ILCS § 5/2-801, Plaintiff seeks certification of the following Class:

> All employees who entered Defendant's locations in the State of Illinois who had their facial geometry scans, biometric identifiers, and/or biometric information collected, captured, received, or otherwise obtained, maintained, stored, disclosed, or disseminated by Defendant during the applicable statutory period.

60. Excluded from the Class are Defendant's officers and directors, and any judge, justice, or judicial officials presiding over this matter and their immediate families.

61. 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

62. There are at least many thousands of putative Class members. The exact number of Class members can easily be determined from Defendant's records.

Commonality

63. 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, received, or otherwise obtained, maintained, stored, or disclosed or disseminated Plaintiff's and the Class's biometric identifiers or biometric information;

B. Whether Defendant informed Plaintiff and the Class that it was collecting or storing their biometric identifiers and biometric information;

C. Whether Defendant properly informed Plaintiff and the Class of the specific purpose and duration for which Defendant was collecting, using, storing, and disseminating their biometric identifiers or biometric information;

D. 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;

E. Whether Defendant has disclosed, redisclosed, or otherwise disseminated Plaintiff's and the Class's biometric identifiers or biometric information;

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

G. 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;

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

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

J. Whether Defendant used Plaintiff's and the Class's biometric identifiers, including scans of their facial geometry, to identify them;

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

L. Whether the violations of BIPA were committed intentionally or recklessly.

64. Plaintiff anticipates Defendant will raise defenses that are common to Plaintiff and the Class.

Adequacy

65. 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 serving as class counsel.

Typicality

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

67. Upon information and belief, there are no other Class members who have an interest in individually controlling the prosecution of his individual claims, especially in light of the relatively small value of each claim. 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

68. 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.

69. 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 and Destruction Guidelines

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

71. 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 destruction 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 destroy the biometric information. *See* 740 ILCS § 14/15(a).

72. Defendant fails to comply with these BIPA mandates.

73. Defendant Amazon.com, Inc. is a Delaware corporation that is registered to do business in Illinois, and therefore, qualifies as a "private entity" under BIPA. *See* 740 ILCS § 14/10.

74. Plaintiff and the putative Class are individuals who have had their "biometric identifiers" and "biometric information" collected by Defendant, as explained in detail in Sections II and III, *supra*. *See* 740 ILCS § 14/10.

75. 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).

76. 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 Plaintiff's and Class members' last interaction with Defendant, whichever occurs first.

77. On behalf of himself and the putative 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 Collecting or 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).

80. Defendant failed to comply with these BIPA mandates.

81. Defendant Amazon.com, Inc. is a Delaware corporation that is registered to do business in Illinois, and therefore, qualifies as a "private entity" under BIPA. *See* 740 ILCS § 14/10.

82. Plaintiff and the putative Class are individuals who have had their "biometric identifiers" and "biometric information" collected by Defendant, as explained in detail in Sections II and III, *supra*. *See* 740 ILCS § 14/10.

83. Defendant systematically and automatically collected, captured, or otherwise obtained Plaintiff's and the putative Class's biometric identifiers and/or biometric information without first obtaining the written release required by 740 ILCS § 14/15(b)(3).

84. Defendant never informed Plaintiff and the putative Class in writing that their biometric identifiers and/or biometric information were being collected, captured, or otherwise obtained, nor did Defendant ever inform Plaintiff and the putative 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).

85. By collecting, capturing, or otherwise obtaining Plaintiff's and the putative 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.*

86. On behalf of himself and the putative 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 or Dissemination of Biometric Identifiers and Information Before Obtaining Consent

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

88. BIPA prohibits private entities from disclosing or disseminating 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).

89. Defendant fails to comply with this BIPA mandate.

90. Defendant Amazon.com, Inc. is a Delaware corporation that is registered to do business in Illinois, and therefore, qualifies as a "private entity" under BIPA. *See* 740 ILCS § 14/10.

91. Plaintiff and the putative Class are individuals who have had their "biometric identifiers" and "biometric information" collected by Defendant, as explained in detail in Sections II and III, *supra*. *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 himself and the putative 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 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 Michael Jerinic 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 or, in the alternative, were negligent;

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 and to delete and destroy any biometric identifiers and information previously collected from Class members;

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: September 28, 2020

Respectfully Submitted,

/s/Ryan F. Stephan
Catherine T. Mitchell
STEPHAN ZOURAS, LLP
100 N. Riverside Plaza, Suite 2150
Chicago, Illinois 60606
Telephone: (312) 233-1550
Facsimile: (312) 233-1560
rstephan@stephanzouras.com
cmitchell@stephanzouras.com
Firm ID: 43734
Counsel for Plaintiff and the Putative Class