☐ YES ☑ NO

EXHIBITS

CASE NO. 23Ch000544

DATE: 1-19-23

CASE TYPE: Class Action

PAGE COUNT: 26

CASE NOTE

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

SANDRA TRIO, individually, and on behalf of all others similarly situated,	)	
Plaintiff,	)	**Case No.** 2023CH00544
v.	)	
AMAZON WEB SERVICES, INC., A DELAWARE CORPORATION	)	
Defendant.	)	

CLASS ACTION COMPLAINT

Plaintiff Sandra Trio ("Plaintiff"), individually and on behalf of all others similarly situated (the "Class"), by and through her attorneys, brings the following Class Action Complaint ("Complaint") pursuant to the Illinois Code of Civil Procedure, 735 ILCS §§ 5/2-801 and 2-802, against Defendant Amazon Web Services, Inc. ("AWS" or "Defendant"), its subsidiaries and affiliates, to redress and curtail Defendant's unlawful collection, obtainment, use, storage, and disclosure of Plaintiff's sensitive and proprietary biometric identifiers and/or biometric information (collectively referred to herein as "biometric data" and/or "biometrics"). 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 AWS is a Delaware corporation and subsidiary of Amazon.com, Inc., and is one of, if not the, largest platforms and providers of artificial intelligence ("AI") and cloud computing services.

2. Plaintiff worked for New Albertson's, Inc. d/b/a Jewel-Osco, Inc., ("Jewel-Osco") in Illinois from April 2019 to June 2021 and was required to provide a scan of her facial geometry as part of a COVID-19 screening process on a "Turing Shield" biometric device to be cleared to work, prior to starting her shift, to have her temperature checked, confirm she was wearing a face mask, and otherwise cleared to work.

3. The Turing Shield is manufactured by Turing Video, Inc. ("Turing"), a technology company and provider of artificial intelligence integrated products that provide security and health solutions to companies across an array of industries.

4. The screening process begins by prompting users to text a number which triggers them to fill out a health questionnaire on their phone. Once this is complete, a QR code appears on the user's phone which is then scanned by the biometric screening device (*i.e.*, the Turing Shield) to initiate a temperature screening.

5. Users of the Turing Shield device, like Plaintiff, are required to stand in front of the device's camera which collects a scan of the user's facial geometry and utilizes an artificial intelligence algorithm to analyze the user's biometric data and signal an alert when it recognizes the user. The Turing Shield then locates the user's forehead and signals the kiosk's built-in thermal sensor to collect the user's forehead temperature. The facial recognition software may also be used to identify the presence of a mask on the user's face.

6. After the data is collected and stored, the kiosk analyzes the data to determine if the user has passed the COVID-19 screening protocol. If the user provides satisfactory results for the health questionnaire, temperature screening, and mask detection, the kiosk prints a badge indicating the user is cleared to enter the work environment. A negative result from the screening process will print a badge indicating the user has failed the screening.

7. Upon purchasing a Turing biometric screening device, including the Turing Shield, the customer has the opportunity to choose a "Network Solution," which allows for the collection of the customer's users' biometric data, including the results of their temperature scan and mask detection, to be stored on a cloud service hosted by Defendant AWS. The data is provided to entities using Turing biometric screening devices and software so it can do contact tracing by tracking employees or customer movement throughout a workplace or facility.

8. Upon information and belief, Turing contracted with AWS to host biometric data collected from its users of the biometric screening devices, including the Turing Shield and other Turing AI devices. Additionally, Turing retained AWS for its software services, including, but not limited to, its Rekognition program.

9. Rekognition is an image-recognition technology that Amazon markets and sells to businesses, governmental entities, and other third parties through AWS. According to AWS's own FAQ, the most common use cases for Rekognition include: "Searchable Image Library, Face-Based User Verification, Sentiment Analysis, Facial Recognition, and Image Moderation."[1]

10. The Turing devices and related software compare users' images, which involves detecting faces to identify and/or verify these users' identities.

11. AWS collects, stores, possesses, otherwise obtains, uses, and disseminates Turing users' biometric data to, amongst other things, further enhance AWS and its affiliated machine-learning and artificial intelligence technologies, including but not limited to Amazon Rekognition.

12. AWS wrongfully profits from the facial scans it has collected or otherwise obtained through users of Turing AI products by using the biometric data it obtains to improve its machine learning and AI technologies, such as Amazon Rekognition, thereby making these technologies

[1] *Amazon Rekognition – FAQs*, https://aws.amazon.com/rekognition/faqs/?nc=sn&loc=7 (last visited July 27, 2022).

and services more profitable to AWS, which sells them to businesses, law enforcement agencies, and other entities.

13. Facial geometry scans are unique, permanent biometric identifiers associated with each user that cannot be changed or replaced if stolen or compromised. AWS's unlawful collection, obtainment, storage, and use of Turing users' biometric data exposes them to serious and irreversible privacy risks. For example, if AWS's database containing facial geometry scans or other sensitive, proprietary biometric data is hacked, breached, or otherwise exposed – like in the Equifax, Facebook/Cambridge Analytica, and Suprema data breaches – Turing users have ***no*** means by which to prevent identity theft, unauthorized tracking or other unlawful or improper use of this highly personal and private information.

14. 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.

15. 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 geometries – 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.

16. 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.

17. In August 2019, 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 Defence 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.

18. 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.

19. 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.

20. 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, otherwise obtain, store, use, and disseminate Illinois citizens' biometrics, such as facial geometry scans.

21. Notwithstanding the clear and unequivocal requirements of the law, AWS disregarded Plaintiff's and other similarly situated Turing users' statutorily protected privacy rights and unlawfully collected, otherwise obtained, stored, disseminated, and used Plaintiff's and other similarly-situated Turing users' biometric data in violation of BIPA. Specifically, AWS violated BIPA because it did not:

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

b. Develop and adhere to a publicly available retention schedule and guidelines for permanently destroying Plaintiff's and other similarly-situated Turing users' facial geometry scans, as required by BIPA;

c. Obtain a written release from Plaintiff and others similarly situated to collect, obtain, store, or use their facial geometry scans, as required by BIPA; and

d. Obtain consent from Plaintiff and others similarly situated to disclose, redisclose, or otherwise disseminate their facial geometry scans to third parties as required by BIPA.

22. Although AWS has been collecting Turing users' biometric identifiers and biometric information for years, it failed to comply with BIPA.

23. Accordingly, Plaintiff, on behalf of herself as well as the putative Class, seeks an Order: (1) declaring that AWS's conduct violated BIPA; (2) requiring AWS to cease the unlawful activities discussed herein; and (3) awarding statutory damages to Plaintiff and the proposed Class.

PARTIES

24. Plaintiff Sandra Trio is a natural person and a resident of the State of Illinois.

25. Defendant Amazon Web Services, Inc. is a Delaware corporation that is registered to do business in Illinois.

JURISDICTION AND VENUE

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

27. Venue is proper in Cook County because Defendant conducts business in this State, conducts business transactions in Cook County, and committed the statutory violations alleged herein in Cook County, Illinois.

FACTUAL BACKGROUND

I. The Biometric Information Privacy Act.

28. 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.

29. In late 2007, a biometrics company called Pay by Touch, which provided major retailers throughout the State of Illinois with fingerprint scanners to facilitate consumer transactions, filed for bankruptcy. That bankruptcy was alarming to the Illinois Legislature because suddenly there was a serious risk that millions of fingerprint records – which, like other unique biometric identifiers, can be linked to people's sensitive financial and personal data – could now be sold, distributed, or otherwise shared through the bankruptcy proceedings without adequate

protections for Illinois citizens. The bankruptcy also highlighted the fact that most consumers who used the company's fingerprint scanners were completely unaware that the scanners were not actually transmitting fingerprint data to the retailer who deployed the scanner, but rather to the now-bankrupt company, and that their unique biometric identifiers could now be sold to unknown third parties. *See* Illinois House Transcript, 2008 Reg. Sess. No. 276, p. 249.

30. 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.

31. 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.

32. 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).

33. Biometric identifiers include retina and iris scans, voiceprints, scans of hand and fingerprints, and – most importantly here – face geometries. *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.*

34. BIPA establishes standards for how companies must handle Illinois citizens' biometric identifiers and biometric information. *See, e.g.*, 740 ILCS § 14/15(c)-(d). For example, BIPA prohibits private entities from disclosing a person's or customer's biometric identifier or biometric information without first obtaining consent for such disclosure. *See* 740 ILCS § 14/15(d)(1).

35. 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).

36. 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. 740 ILCS § 14/5.

37. 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, otherwise obtain, store, use, and disseminate biometrics and creates a private right of action for lack of statutory compliance. 740 ILCS § 14/20.

38. Plaintiff, like the Illinois legislature, recognizes how imperative it is to keep biometric identifiers and biometric information secure. Biometric data, unlike other personal identifiers such as a social security number, cannot be changed or replaced if hacked or stolen.

II. Defendant Violated the Biometric Information Privacy Act.

39. AWS's Rekognition is a major biometric-based facial recognition platform that violates BIPA's basic requirements.

40. AWS provides cloud-computing services to millions of customers around the world including Turing. These services include infrastructure technologies, like computing, storage, database, and networking as well as machine learning and analytics. AWS's services utilize AWS's and Amazon's hardware, software, and global infrastructure. As a result, instead of owning and maintaining physical data centers, servers, or computing power, companies like Turing can pay AWS to provide these services.

41. AWS contracted with Turing to host and store its user database. AWS obtained, stored, and used Turing users' biometric identifiers and biometric information to enhance its machine learning and AI technologies.

42. Users of a Turing Shield device are required to stand in front of the device's camera which collects the user's facial geometry and utilizes an artificial intelligence algorithm to analyze the user's biometric information and signal an alert when it recognizes the user. The device then locates the user's forehead and signals the kiosk's built-in thermal sensor to collect the user's

forehead temperature. The facial recognition software may also be used to identify the presence of a mask on the user's face.

43. When Turing customers sign up to use the AWS-hosted Turing product, they are asked to sign up for a "Network Solution" where by AWS hosts users' biometric data collected by a Turing device. The hosted data is then provided to entities so they can do contact tracing by tracking employee and customer movement throughout a workplace or facility.

44. AWS obtains, stores, possesses, and uses Turing users' facial geometry by way of hosting, cloud-computing, and networking Turing customers' user database.

45. Further, these facial geometry scans are obtained by, hosted, and stored in AWS's own servers and databases, and AWS uses Turing users' biometric data to enhance its machine learning and AI technology programs, including but not limited to, Rekognition.

46. AWS disregards Turing users' privacy rights and further violates their statutorily-protected rights to control the collection, obtainment, use, and storage of their sensitive biometric data.

47. AWS failed to inform Plaintiff and other Turing users that it disclosed their face geometry data to other Amazon entities and other third parties that host the biometric data in their data centers; failed to inform Turing users of the purposes and duration for which AWS collected or obtained, stored, possessed, and used their sensitive biometric data, including to enhance and improve its machine learning and AI technologies for profit; and, failed to obtain written releases from Turing users before collecting or obtaining, storing, and using their facial geometry scans.

48. AWS failed to develop or adhere to a written, publicly available policy identifying its retention schedule and guidelines for permanently destroying Turing users' biometric data when

the initial purpose for collecting or obtaining their biometrics is no longer relevant, as required by BIPA.

49. AWS unlawfully collected or obtained, stored, used, and disseminated Turing users' biometric identifiers and biometric information, without first receiving the individual's informed written consent required by BIPA.

50. AWS lacked retention schedules and guidelines for permanently destroying Plaintiff's and other similarly situated individuals' biometric data. Plaintiff is unaware as to whether AWS has destroyed her biometric data or the biometric data of others similarly situated who have not given consent for AWS's biometric data collection, otherwise obtainment, use, storage, and dissemination.

51. Since AWS neither published a BIPA-mandated data retention policy nor disclosed the purposes for its collection, obtainment, possession, and use of biometric data, Plaintiff had no idea at the time of collection whether AWS sold, disclosed, redisclosed, or otherwise disseminated her biometric data. Moreover, Plaintiff and others similarly situated were not told at the time of collection or otherwise obtainment to whom AWS disclosed their biometric data, or what might happen to their biometric data in the event of a merger or a bankruptcy.

52. AWS disclosed, or otherwise disseminated Plaintiff's and putative class members' biometric data to other Amazon entities and subsidiaries, AWS customers, and likely others.

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

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

III. Plaintiff Sandra Trio's Experience

55. Plaintiff Sandra Trio worked as a cake decorator for New Albertson's, Inc. d/b/a Jewel-Osco, from approximately April 2019 to at least June 2021 at its store located at 1501 E Algonquin Rd, Algonquin, IL 60102.

56. While employed by Jewel-Osco, Plaintiff was required to scan her facial geometry on a Turing Shield device as part of a COVID-19 screening process to be cleared to work.

57. Utilizing the "Network Solution," Turing subsequently stored Plaintiff's biometric data in a database(s) hosted by AWS.

58. Through hosting and networking Turing users' database, AWS scanned, collected otherwise obtained, possessed, and used Plaintiff's facial geometry.

59. AWS used and continues to use Turing users' biometric data to enhance its machine learning and AI technologies, including Rekognition.

60. AWS failed to: (1) inform Plaintiff in writing or otherwise of the purpose(s) and length of time for which her facial geometry was being collected, otherwise obtained, used, and stored; (2) obtain a written release from Plaintiff to collect, otherwise obtain, store, or use her facial geometry data; (3) obtain Plaintiff's consent before disclosing, re-disclosing, or disseminating her biometric data to other Amazon entities and/or other third parties; and (4) AWS did not develop or adhere to a publicly available retention schedule and guidelines for permanently destroying facial geometry data.

61. Plaintiff was not informed of the specific limited purposes or length of time for which AWS collected otherwise obtained, stored, used, and disseminated her biometric data. Among other things, AWS never informed her that this biometric data would be used to improve AWS's Rekognition technology, which AWS sells to third parties at a profit.

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

63. Plaintiff has never been provided with nor ever signed a written release stating that AWS could use her biometric data to improve its machine learning and AI technologies it sells to businesses and other entities.

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

65. No amount of time or money can compensate Plaintiff if her biometric data has been compromised by the lax procedures through which AWS captures, otherwise obtains, stores, uses, and disseminates her and other similarly situated individuals' biometrics. Moreover, Plaintiff would not have provided her biometric data to AWS if she had known that AWS would retain such information without her consent.

66. A showing of actual damages is not necessary 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").

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

CLASS ALLEGATIONS

68. 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.

69. 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, stored, and used; (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.

70. 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 who used a Turing biometric device in the State of Illinois and had their facial geometry collected, captured, received, otherwise obtained, maintained, stored, used, and/or disclosed by AWS during the applicable statutory period.

71. 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

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

Commonality

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

A. Whether AWS collected, captured, maintained, stored, or otherwise obtained Plaintiff's and the Class's biometric identifiers or biometric information;

B. Whether AWS properly informed Plaintiff and the Class of the purposes for collecting, obtaining, using, storing, and disseminating their biometric identifiers or biometric information;

C. Whether AWS properly obtained a written release (as defined in 740 ILCS § 14/10) and/or consent to collect, obtain, use, store, and disseminate Plaintiff's and the Class's biometric identifiers or biometric information;

D. Whether AWS has disclosed or redisclosed Plaintiff's and the Class's biometric identifiers or biometric information;

E. Whether AWS developed a BIPA-compliant written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within three years of its last interaction with the individual, whichever occurs first;

F. Whether AWS complied with any such BIPA-compliant written policy (if one exists);

G. Whether AWS profited from the use of the biometric identifiers and biometric information it collected or otherwise obtained via Turing biometric devices by using that biometric data to enhance and train machine learning and AI technologies it sold to businesses, governmental entities, and other organizations.

H. Whether AWS'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;

I. Whether AWS used Plaintiff's and the Class's facial geometry to identify

them;

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

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

74. Plaintiff anticipates that AWS will raise defenses that are common to the class.

Adequacy

75. 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

76. 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.

77. 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. 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

78. 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.

79. 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

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

81. 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).

82. AWS failed to comply with these BIPA mandates.

83. AWS is a Delaware corporation and, therefore, qualifies as a "private entity" under BIPA. *See* 740 ILCS § 14/10.

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

85. 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.

86. AWS failed to develop and adhere to a publicly available retention schedule or guidelines for permanently destroying biometric identifiers and biometric information as specified and required by BIPA. *See* 740 ILCS § 14/15(a).

87. AWS lacked a retention schedule and guidelines for permanently destroying Plaintiff's and the Class's biometric data.

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 AWS to comply with BIPA's requirements for the collection, obtainment, storage, and use of biometric identifiers and biometric information as described herein; (3) statutory damages of $5,000 for each intentional and/or reckless violation of BIPA pursuant to 740 ILCS § 14/20(2) or, in the alternative, statutory damages of $1,000 for each negligent violation of BIPA pursuant to 740 ILCS § 14/20(1); and (4) reasonable attorneys' fees and costs and other litigation expenses pursuant to 740 ILCS § 14/20(3).

SECOND CAUSE OF ACTION
Violation of 740 ILCS § 14/15(b): Failure to Obtain Informed Written Consent and Release Before Obtaining Biometric Identifiers or Information

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

90. 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).

91. AWS fails to comply with these BIPA mandates.

92. AWS is a Delaware corporation and, therefore, qualifies as a "private entity" under BIPA. *See* 740 ILCS § 14/10.

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

94. 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.

95. AWS systematically and automatically collected, captured, otherwise obtained, and used 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).

96. AWS did not inform Plaintiff and the Class in writing that their biometric identifiers and/or biometric information were being collected, captured, otherwise obtained, and/or used nor did AWS 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, captured, otherwise obtained, and/or used as required by 740 ILCS § 14/15(b)(1)-(2).

97. By collecting, capturing, otherwise obtaining, and using Plaintiff's and the Class's biometric identifiers and biometric information as described herein, AWS 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 AWS to comply with BIPA's requirements for the collection, storage, obtainment, 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(c): Profiting from Biometric Identifiers or Biometric Information Obtained Through Hosting and Networking Turing Devices

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

100. BIPA prohibits private entities in possession of biometric identifiers or biometric information from selling, leasing, trading, or otherwise profiting from a person's or a customer's biometric identifier or biometric information. *See* 740 ILCS § 14/15(c).

101. AWS fails to comply with this BIPA mandate.

102. AWS is a Delaware corporation and, therefore, qualifies as a "private entity" under BIPA. See 740 ILCS § 14/10.

103. Plaintiff and the Class are individuals who have had their "biometric identifiers" collected and/or otherwise obtained by AWS (in the form of their facial geometry), as explained in detail in Sections II and III, supra. See 740 ILCS § 14/10.

104. 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.

105. AWS has possession of Plaintiff's and Class Members' biometric identifiers and biometric information and, without informing them, profited from their biometric identifiers and biometric information by using that biometric data to enhance and train its machine learning and AI technologies, including but not limited to Amazon's Rekognition technology, which are marketed and sold to businesses, governmental entities, and other organizations.

106. By profiting from its undisclosed use of Plaintiff's and Class Members' biometric identifiers and biometric information, AWS violated the substantive privacy interests that BIPA protects.

107. 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 AWS to cease profiting from the use of their biometric identifiers and biometric information; (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).

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

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

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

110. AWS fails to comply with this BIPA mandate.

111. AWS is a Delaware corporation and, therefore, qualifies as a "private entity" under BIPA. *See* 740 ILCS § 14/10.

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

113. 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.

114. To this day, AWS systematically and automatically discloses, rediscloses, or otherwise disseminates Plaintiff's and the Class's biometric identifiers and/or biometric information without obtaining the consent required by 740 ILCS § 14/15(d)(1).

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

116. 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 AWS to comply with BIPA's requirements for the collection, obtainment, storage, use, and dissemination of biometric identifiers and biometric information as described herein; (3) statutory damages of $5,000 for each intentional and/or reckless violation of BIPA pursuant to 740

ILCS § 14/20(2) or, in the alternative, statutory damages of $1,000 for each negligent violation of BIPA pursuant to 740 ILCS § 14/20(1); and (4) reasonable attorneys' fees and costs and other litigation expenses pursuant to 740 ILCS § 14/20(3).

PRAYER FOR RELIEF

Wherefore, Plaintiff Sandra Trio 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 Sandra Trio as Class Representative, and appointing Stephan Zouras, LLP as Class Counsel;

B. Declaring that AWS'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 AWS's actions, as set forth above, were intentional and/or reckless;

E. Awarding injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and the Class;

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 19, 2023

Respectfully Submitted,

/s/ Andrew C. Ficzko

Ryan F. Stephan
James B. Zouras
Andrew C. Ficzko
Catherine Mitchell
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
aficzko@stephanzouras.com
cmitchell@stephanzouras.com
Firm ID No. 43734

Attorneys for Plaintiff and the Putative Class Members

CERTIFICATE OF SERVICE

I, the attorney, hereby certify that on January 19, 2023, I 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/ Andrew C. Ficzko

ClassAction.org