

**IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF ILLINOIS**

PENNY WEBER and MILDRED
STOCKWELL, on behalf of themselves
and all others similarly situated,

Plaintiffs,

v.

WALMART INC.,

Defendant.

Civil Action No:

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Penny Weber and Mildred Stockwell (“Plaintiffs”), by and through undersigned counsel, bring this action on behalf of themselves and on behalf of all others similarly situated (the “Class” or “Proposed Class”) against Walmart, Inc. (“Walmart” or “Defendant”). Plaintiffs make the following allegations based on personal knowledge of the facts pertaining to themselves and on information and belief upon investigation that is reasonable as to all other matters. Plaintiffs allege as follows:

NATURE OF ACTION

1. This class action arises out of Walmart’s serendipitous collection, storage, review and use of Plaintiffs and the Class and their biometric identifiers¹ and biometric information² (together, “Biometric Data”) without obtaining any informed written consent nor providing consumers with data retention and destruction policies as required by the law.

¹ “‘Biometric identifier’ means a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry.” 740 Illinois Compiled Statutes (“ILCS”) 14/10.

² “‘Biometric information’ means any information, regardless of how it is captured, converted, stored, or shared, based on an individual’s biometric identifier used to identify an individual.” *Id.*

2. Biometric Data, collected and held in digital format is highly personal and sensitive information to Plaintiffs and the Class. The growing risk of data breaches along with the importance and private nature of some of this information has prompted many legislatures to act. The Illinois Legislature, for example, has held that “[b]iometrics are unlike other unique identifiers that are used to access finances or other sensitive information.” 740 ILCS 14/5(c) (Biometric Information Privacy Act) (hereafter, “BIPA”). These are highly immutable personal/private data to individuals because “[f]or example, social security numbers, when compromised, can be changed. Biometrics, however, are biologically unique to the individual; therefore, once compromised, the individual has no recourse, is at heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions.” *Id.*

3. Walmart’s stores in the state of Illinois are outfitted with cameras and other advanced video surveillance systems that – unbeknownst to customers in Illinois who enter the stores – surreptitiously collect, possess, or otherwise obtain Biometric Data, including recordings of an individual’s face (i.e., facial recognition technology).

4. Extracting an individual’s face geometry data in order to confirm a subsequent match of the individual’s face—also known as “facial recognition” or “faceprinting”—uses biological characteristics to verify an individual’s identity.

5. This is an incredibly lucrative field, with the industry expected to reach \$7 billion by 2024.³

6. That said, the dangers of the use of this technology are widely known – including

³ Facial Recognition Market Worth \$7.0 Billion by 2024, Markets and Markets, <https://www.prnewswire.com/news-releases/facial-recognition-market-worth-7-0-billion-by-2024--exclusive-report-by-marketsandmarkets-300876154.html>.

that individuals can be impersonated to gain access to personal information with Biometric Data.⁴

7. While things like Social Security numbers or credit card information can be changed if compromised, Biometric Data cannot be modified in such an easy way. If such information is exposed, it leaves victims with no means to prevent identify theft and unauthorized tracking with their Biometric Data.

8. The threats posed by facial recognition technology can be more insidious than the threats posed by the use of other biometric information, such as fingerprints. Indeed, as commentators have recognized, “facial recognition creates acute privacy concerns that fingerprints do not.”⁵

9. Recognizing the heightened importance of Biometric Data, and the potential for abuse, nonconsensual proliferation of it by third-parties, and other harms exposed onto Illinois residents, the Illinois Legislature passed BIPA, which contains a provision requiring that a private entity may not obtain and/or possess an individual’s Biometric Data unless it: (1) informs that person (or their representative) in writing that a biometric identifier or biometric information is being collected or stored; (2) informs that person in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; (3) receives a written release from the person (or their representative) for the collection of his or her biometric identifier or information; and (4) publishes publicly-available written retention schedules and guidelines for permanently destroying Biometric Data. 740 ILCS 14/15, *et seq.*

⁴ Elias Wright, The Future of Facial Recognition Is Not Fully Known: Developing Privacy and Security Regulatory Mechanisms for Facial Recognition in the Retail Sector, 29 Fordham Intell. Prop. Media & Ent. L.J. 611, 629 (2019).

⁵ What Facial Recognition Technology Means for Privacy and Civil Liberties: Hearing Before the Subcomm. On Privacy Tech & the Law of the S. Comm. On the Judiciary, 112th Cong. 1 (2012) (statement of Sen. Al Franken, Chairman, Subcomm. On Privacy, Tech. & the Law of the S. Comm. On the Judiciary), available at <https://www.govinfo.gov/content/pkg/CHRG-112shrg86599/pdf/CHRG-112shrg86599.pdf>.

10. Further, the entity must store, transmit, and protect from disclosure all Biometric Data using the industry's standard of care and in a manner at least as protective as the means used to protect other confidential and sensitive information. *Id.* No private entity may sell, lease, trade, or otherwise profit from a person's or customer's Biometric Data. *Id.* Finally, no private entity may disclose, redisclose, or otherwise disseminate a person's Biometric Data except with the subject's consent, to complete a financial transaction requested by the customer, or other narrowly prescribed situations. *Id.*

11. In direct violation of each of the foregoing provisions of § 15 of BIPA, as alleged here, Walmart is and has been actively collecting, storing, and using – without providing notice, obtaining informed written consent, or publishing data retention policies – the Biometric Data of thousands if not millions of Illinoisans who have unsuspectingly entered Walmart's stores.

12. Walmart does not notify Illinois residents that wish to enter their stores of this fact prior to their entry, nor does it attempt to obtain prior consent from customers for the collection, storage, and use of their Biometric Data. Walmart does not provide a policy, as required by law, establishing a retention schedule and guidelines for permanently destroying this Biometric Data either.

13. In addition, Walmart uses proprietary software from technology company Clearview AI, Inc. ("Clearview") to match facial scans taken with billions of facial scans maintained within Clearview's extensive facial recognition database (the "Biometric Database").

14. Walmart does not notify customers in the state of Illinois of this fact prior to store entry, nor does it obtain consent prior to disseminating or disclosing its Illinois customers' Biometric Data through Clearview's Biometric Database.

15. BIPA confers on Plaintiffs and all other similarly situated Illinois residents a right

to know about the facts of Biometric Data storage, collection, and use as it pertains to their own Biometric Data, and a right to know how long such risks will persist.

16. Moreover, the collection of this Biometric Data in Illinois from its citizens violates certain statutory and common law rights of consumers. For example, the Illinois Constitution states: “Every person shall find a certain remedy in the laws for all injuries and wrongs which he receives to his person, privacy, property or reputation. He shall obtain justice by law, freely, completely, and promptly.” IL Const. Art. I, Sec. 12.

17. As a result of the alleged actions above, Walmart failed to comply with its duties under applicable Illinois law. Walmart did and does not adequately disclose its Biometric Data collection practices to its customers in Illinois, never obtained written consent from any of its customers regarding its Biometric Data practices in Illinois, and never provided any data retention or destruction policies to any of its customers in Illinois. Moreover, Walmart invaded Plaintiffs’ and the Class’s privacy through the unauthorized collection, retention, and use of Plaintiffs’ Biometric Data in Illinois.

18. Plaintiffs bring this action to prevent Walmart from further violating the privacy rights of Illinois residents.

19. Plaintiffs also bring this action to recover statutory damages for Walmart’s unauthorized collection, storage, and use of these individuals’ Biometric Data.

JURISDICTION AND VENUE

20. This Court has subject matter jurisdiction over this lawsuit under the Class Action Fairness Act, 28 U.S.C. §1332(d), because: (1) the proposed class consists of over 100 members; (2) the parties are minimally diverse, as members of the class of plaintiffs are citizens of a state different from Defendant; and (3) the aggregate amount in controversy exceeds \$5,000,000,

exclusive of interest and costs.

21. This Court has personal jurisdiction over Defendant because Walmart owns and operates over a hundred stores in the state of Illinois. Defendant used and disseminated data derived directly from Illinois consumers, including Plaintiffs, and exposed residents of Illinois to ongoing privacy risks within the state of Illinois based on the unauthorized collection, capture, obtainment, disclosure, redisclosure, and dissemination of Biometric Data. The images and recordings Defendant used for the unlawful collection, capture, and obtainment of Biometric Data were taken at Walmart stores located in the state of Illinois. Defendant knew, or should have known, that its collection, capture, obtainment, disclosure, redisclosure, and dissemination of impacted individuals' Biometric Data would injure Illinois residents and citizens. Defendant knew or had reason to know that collecting, storing, using, disclosing, and disseminating Illinois citizens' and residents' Biometric Data without providing the requisite notice or obtaining the requisite consent would deprive Illinois citizens and residents of their statutorily protected privacy rights, neutralize Illinois citizens' and residents' ability to control access to their Biometric Data, and expose Illinois residents to potential surveillance and other privacy harms as they went about their lives within the State.

22. Venue is proper in this District under 28 U.S.C. §1391(b)(2) because a substantial part of the acts or omissions giving rise to the claims occurred here, and Plaintiff Weber is domiciled in this district.

PARTIES

23. Plaintiff Penny Weber is a citizen and resident of Alton, Illinois.

24. Plaintiff Mildred Stockwell is a citizen and resident of Decatur, Illinois.

25. Defendant Walmart, Inc. is a corporation with its corporate headquarters located in

Bentonville, Arkansas.

FACTUAL ALLEGATIONS

I. BIOMETRIC INFORMATION PRIVACY ACT (“BIPA”) OF ILLINOIS

26. In 2008, the Illinois Legislature passed BIPA in large part because it determined the “very serious need [for] protections for the citizens of Illinois when it comes to biometric information.” Illinois House Transcript, 2008 Reg. Sess. No. 276. BIPA makes it illegal to, among other things, for a private entity to “collect, capture, purchase, receive through trade, or otherwise obtain a person’s or a customer’s biometric identifiers biometric information, unless it first:

- a. informs the subject ... in writing that a biometric identifier or biometric information is being collected or stored;
- 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 or the subject’s legally authorized representative.” 740 ILCS 14/15 (b).

27. To “collect” means is the act of gathering together, and is separate from possession, which is not an element of collection.

28. The plain and ordinary meaning of the word “possession” is the act of having or taking into control, including without regard to ownership.

29. A private entity that controls Biometric Data, therefore, possesses Biometric Data under Section 15(a).

30. To facilitate these informed notice and consent provisions, Section 15(a) of BIPA

also provides:

A private entity in possession of biometric identifiers or biometric information must develop 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 3 years of the individual's last interaction with the private entity, whichever occurs first. 740 ILCS 14/15(a).

31. Section 15(c) of the BIPA makes it unlawful for any private entity to, among other things, "sell, lease, trade, or otherwise profit from a person's or a customer's biometric identifier or biometric information." 740 ILCS 14/15(c).

32. Section 15(d) of the BIPA makes it unlawful for any private entity to, among other things:

[D]isclose, redisclose, or otherwise disseminate a person's or a customer's biometric identifier or biometric information unless: (1) the subject of the biometric identifier or biometric information...consents to the disclosure or redisclosure; (2) the disclosure or redisclosure completes a financial transaction requested or authorized by the subject of the biometric identifier or the biometric information...; (3) the disclosure or redisclosure is required by State or federal law or municipal ordinance; or (4) the disclosure is required pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction. 740 ILCS 14/15(d).

33. To enforce BIPA's requirements, the legislature included a private right of action authorizing "[a]ny person aggrieved by a violation" to sue and recover for each violation damages of \$1,000 for a negligent violation, or \$5,000 in the event of an intentional or reckless violation, plus attorneys' fees, costs, and appropriate injunctive relief. 740 ILCS 14/20.

34. BIPA seeks to safeguard the Biometric Data of individuals in Illinois.

35. As alleged below, Walmart's practice of collecting, storing, and using individuals' Biometric Data without obtaining informed written consent violates all three prongs of §15(b) of BIPA. Walmart's failure to provide a publicly available written policy regarding a schedule and guidelines for the retention and permanent destruction of individuals' Biometric Data also violates

§15(a) of BIPA. Walmart's use of Clearview's Biometric Database was an unlawful dissemination and disclosure of Biometric Data, in violation of §§15(c)-(d) of BIPA.

II. WALMART'S VIOLATIONS OF BIPA AND RELATED SURVEILLANCE SYSTEMS

36. Walmart is a major brick-and-mortar retailer with thousands of stores across the U.S. and approximately 160 stores within the state of Illinois and is one of the largest companies in terms of revenue in the world.

37. Every Walmart store is outfitted with cameras and video surveillance directed at consumers, including those within the state of Illinois, and many of them have the capability to collect Biometric Data from customers.

38. Unbeknownst to its customers, Walmart's security systems surreptitiously collect, possess, or otherwise obtain customers' Biometric Data without notifying them and without obtaining their consent.

39. Clearview is a software company with a facial recognition platform, which it develops and distributes across the country and world, including in Illinois. Clearview advertises this platform as a "revolutionary, all-in-one, facial recognition platform."

40. Clearview developed the Biometric Database by scouring open-access social media platforms such as Facebook, Twitter, and Instagram to rip Biometric Data from individuals across the world.

41. Walmart, as well as a host of other retailers throughout the country, uses the Biometric Database provided by Clearview for a gamut of reasons, including for security at its stores. After Walmart uploads a local image of an individual into the app, Clearview's algorithm compares the facial geometry of the individual in the image to the billions of facial images in the

Biometric Database to find a match.

42. Through its use of the Biometric Database, Walmart obtains, accesses, and uses Biometric Data of Illinoisans, including the Biometric Data of Plaintiffs and class members.

43. Walmart's U.S. Privacy Policy specifically acknowledges the fact that its surveillance equipment may capture "biometric information."⁶

44. Walmart's continued use of facial recognition-enabled video surveillance systems at its Illinois stores demonstrates that Walmart has violated and continues to violate BIPA as it relates to the Biometric Data of Illinoisans, including Plaintiffs and the Class. The Company's system recognizes facial characteristics and features, and captures, collects, and stores biometric data for later use by Walmart.

45. Separate from its in-store collection and storage of Illinois residents' Biometric Data, Walmart sends its customer's Biometric Data through Clearview's algorithm, which is another method of capturing, collecting, possessing, and using Biometric Data from its Illinois customers without their information or consent, and in direct violation of BIPA.

46. Unbeknownst to the average consumer, and in direct violation of §15(b)(1) of BIPA, Walmart scans, collects, and stores its customers' Biometric Data and identifiers in an electronic database. This occurs when customers, or prospective customers, simply step foot in Walmart's stores. Walmart engages in this practice without informing its customers in writing that it is using surveillance technology that collects and stores biometric information, as is required by BIPA.

47. In direct violation of §§15(b)(2) and 15(b)(3) of BIPA, Walmart did not inform

⁶ <https://corporate.walmart.com/privacy-security/walmart-privacy-policy>, (last accessed Oct. 25, 2022).

Plaintiffs and other Illinois residents – who were subjected to video surveillance recording within its stores – of the specific purpose and length of term for which their biometrics would be collected, stored, and used, nor did they obtain a written release from any of these individuals.

48. In direct violation of §15(a) of BIPA, Walmart does not have written, publicly available policies identifying their retention schedules or guidelines for permanently destroying any of these biometric identifiers or biometric information.

49. In direct violation of §15(c) of BIPA, by sending customers' facial geometries through the Clearview Biometric Database, Walmart engages in the selling, leasing, trading, or otherwise profiting from a person's Biometric Data.

50. In direct violation of §15(d) of BIPA, by sending customers' facial geometries through the Clearview Biometric Database, Walmart discloses, rediscloses, or otherwise disseminates customers' Biometric Data without the requisite consent or authorization.

III. PLAINTIFFS' EXPERIENCES

51. Plaintiff Weber is an Illinois Resident. She has entered Walmart's stores on numerous occasions in the past three years.

52. Among numerous other visits to Walmart, Plaintiff Weber entered a Walmart Store on October 10, 2022 in Wood River, Illinois.

53. Plaintiff Stockwell is an Illinois resident. She has entered Walmart's stores on numerous occasions in the past three years.

54. Among numerous other visits to Walmart, Plaintiff Stockwell entered a Walmart store on July 5, 2022, in Decatur, Illinois.

55. On information and belief, each Illinois Walmart location entered into by Plaintiff Stockwell and Plaintiff Weber is equipped with a facial recognition-enabled video surveillance

system.

56. Plaintiffs did not know that Walmart would collect, obtain, store, and/or use their biometric identifiers or biometric information. Plaintiffs did not give informed written consent to collect, obtain, store, and/or use their Biometric Data, nor were Plaintiffs presented with or made aware of any publicly available retention schedule regarding their Biometric Data.

57. Likewise, Plaintiff Stockwell and Plaintiff Weber were never provided with the requisite statutory disclosures nor an opportunity to prohibit or prevent the collection, storage, or use of their unique biometric identifiers and/or biometric information.

58. By collecting, obtaining, storing, and using Plaintiff Stockwell's and Plaintiff Weber's Biometric Data without their consent, written or otherwise, Walmart invaded Plaintiff Stockwell's and Plaintiff Weber's statutorily protected right to privacy in their Biometric Data.

59. In direct violation of §§15(b)(2) and 15(b)(3) of BIPA, Walmart never informed Plaintiff Stockwell or Plaintiff Weber of the specific purpose and length of time for which their Biometric Data would be collected, stored, and used, nor did Defendant even attempt to obtain a written release from Plaintiff Stockwell or Plaintiff Weber.

60. In direct violation of §15(a) of BIPA, Walmart does not have written, publicly available policies identifying their retention schedules or guidelines for permanently destroying any of Plaintiff Stockwell's or Plaintiff Weber's Biometric Data.

61. In direct violation of §15(c) of BIPA, by sending Plaintiffs' facial geometries through the Biometric Database, Walmart engages in the selling, leasing, trading, or otherwise profiting from Plaintiff Stockwell's Biometric Data.

62. In direct violation of §15(d) of BIPA, by sending Plaintiffs' facial geometries through the Biometric Database, Walmart discloses, rediscloses, or otherwise disseminates

Plaintiffs' Biometric Data without the requisite consent or authorization.

FRAUDULENT CONCEALMENT AND TOLLING

63. Any applicable statute of limitations has been tolled by Defendant's knowing and active concealment of their unlawful conduct. Throughout the Class Period, Defendant affirmatively and fraudulently concealed their unlawful conduct.

64. Plaintiffs and Class members did not discover, nor could they have discovered through the exercise of reasonable diligence, the existence of the hidden and ambiguous privacy policies and terms of use.

65. Further, the very nature of Defendant's conduct was secret and self-concealing. Defendant used advanced video management systems capable of facial recognition and capturing Biometric Data and other technologies without adequately informing impacted individuals that their Biometric Data was being collected and potentially disseminated.

66. As a result of Defendant's fraudulent concealment, all applicable statutes of limitations affecting the claims of Plaintiffs and the Class have been tolled.

CLASS ALLEGATIONS

67. **Class Definition:** Plaintiffs bring this action pursuant to Fed. R. Civ. P. 23 ("Rule 23") and seek class certification of all claims for relief herein on behalf of a class defined as follows:

All individuals who, while in the State of Illinois, had their Biometric Data collected, captured, received, obtained, stored, sold, leased, traded, disclosed, redisclosed, disseminated, and/or otherwise profited from and/or used by Walmart without their consent.

The following are excluded from the Class: (1) any Judge presiding over this action and members of his or her family; (2) Defendant, Defendant's subsidiaries, parents, successors,

predecessors, and any entity in which Defendant has a controlling interest (including current and former employees, officers, or directors); (3) persons who properly execute and file a timely request for exclusion from the Class; (4) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; and (5) the legal representatives, successors, and assigns of any such excluded persons.

68. **Numerosity:** Members of the Class are so numerous that their individual joinder is impracticable. Upon information and belief, members of the Class number in the thousands. The precise size of the Class and Class members' identities are unknown to Plaintiffs at this time but may be determined through discovery. Further, the size and relatively modest value of the claims of the individual members of the Class renders joinder impractical. Accordingly, utilization of the class action mechanism is the most economically feasible means of determining and adjudicating the merits of this litigation. Moreover, the Class is ascertainable and identifiable from Defendant's records.

69. **Typicality:** Plaintiffs' claims are typical of the claims of the Class members because Plaintiffs had their Biometric Data collected, used, and profited from by Walmart upon use of their stores, and therefore, Plaintiffs' claims arise from the same common course of conduct giving rise to the claims of the members of the Class and the relief sought is common to the Class.

70. **Commonality and Predominance:** Common and well-defined questions of fact and law exist as to all members of the Class and predominate over any questions affecting only individual class members. These common legal and factual questions include, but are not limited to, the following:

- a. whether Walmart collected or otherwise obtained Plaintiffs' and the Class's Biometric Data;

- b. whether Walmart properly informed Plaintiffs and the Class that it collected, used, and stored their Biometric Data as required by BIPA;
- c. whether Walmart obtained a written release (as defined in 740 ILCS 14/10) to collect, use, and store Plaintiffs' and the Class's Biometric Data;
- d. whether Walmart developed and made available to the public a written policy establishing a retention schedule and guidelines for permanently destroying Biometric Data when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 3 years of their last interaction, whichever occurs first, as required by BIPA;
- e. whether Walmart used Plaintiffs' and the Class's Biometric Data to identify them;
- f. whether Walmart's violations of BIPA were committed intentionally, recklessly, or negligently;
- g. whether Plaintiffs and members of the Class sustained damages as a result of Walmart's activities and practices referenced above, and, if so, in what amount; and
- h. whether Walmart profited from the activities and practices referenced above, and, if so, in what amount.

71. **Adequate Representation:** Plaintiffs have retained competent counsel experienced in prosecuting complex consumer class actions. Plaintiffs and their counsel are committed to vigorously prosecuting this class action. Moreover, Plaintiffs and their counsel can fairly and adequately represent and protect the interests of the Class because their interests do not conflict with the interests of the Class Plaintiffs seek to represent. Plaintiffs have raised viable statutory claims of the type reasonably expected to be raised by members of the Class and will vigorously pursue those claims. If necessary, Plaintiffs may seek leave of this Court to amend this

Class Action Complaint to include additional Class representatives to represent the Class or additional claims as may be appropriate.

72. **Superiority:** A class action is superior to other available methods for the fair and efficient adjudication of this controversy because individual litigation of the claims of all Class members is impracticable. Each individual Class member may lack the resources to undergo the burden and expense of individual prosecution of the complex and extensive litigation necessary to establish Defendant's liability. Moreover, even if every member of the Class could afford to pursue individual litigation, the Court system could not. Individual litigation of numerous cases would be unduly burdensome to the courts. Individualized litigation would also present the potential for inconsistent or contradictory judgments, and it would magnify the delay and expense to all parties and to the court system resulting from multiple trials of the same factual issues. By contrast, the maintenance of this action as a class action, with respect to some or all of the issues presented herein, presents few management difficulties, conserves the resources of the parties and of the court system, and protects the rights of each member of the Class. Class treatment of the liability issues will ensure that all claims and claimants are before this Court for consistent adjudication of the liability issues. Plaintiffs anticipate no difficulty in the management of this action as a class action. Class-wide relief is essential to compel compliance with BIPA.

COUNT 1
Violation of 740 ILCS 14/1, et seq.
(On Behalf of Plaintiffs and the Class)

73. Plaintiffs incorporate the foregoing allegations as if fully set forth herein.

74. Plaintiffs bring this claim individually and on behalf of the members of the proposed Class against Defendant Walmart.

75. Section 15(a) of the BIPA requires that:

[Any] private entity in possession of biometric identifiers or biometric information must develop 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 3 years of the individual's last interaction with the private entity, whichever occurs first. 740 ILCS 14/15(a).

76. Section 15(b) of the BIPA makes it unlawful for any private entity to, among other things:

[C]ollect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifier or biometric information, unless it 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).

77. Section 15(c) of the BIPA makes it unlawful for any private entity to, among other things, "sell, lease, trade, or otherwise profit from a person's or a customer's biometric identifier or biometric information."

740 ILCS 14/15(c).

78. Section 15(d) of the BIPA makes it unlawful for any private entity to, among other things:

[D]isclose, redisclose, or otherwise disseminate a person's or a customer's biometric identifier or biometric information unless: (1) the subject of the biometric identifier or biometric information . . . consents to the disclosure or redisclosure; (2) the disclosure or redisclosure completes a financial transaction requested or authorized by the subject of the biometric identifier or the biometric information . . .; (3) the disclosure or redisclosure is required by State or federal law or municipal ordinance; or (4) the disclosure is required pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction. 740 ILCS 14/15(d).

79. Defendant is a corporation and thus qualifies as a "private entity" under BIPA. See 740 ILCS 14/10.

80. Plaintiffs and the Class members are individuals who had their biometrics collected

and stored by Defendant. See 740 ILCS 14/10.

81. Defendant does not provide a written, publicly available retention schedule and guidelines for permanently destroying the Biometric Data of Plaintiffs or Class members, as required by BIPA. See 740 ILCS 14/15(a). Defendant's failure to provide such a schedule and guidelines constitutes an independent violation of the statute.

82. Defendant systematically collected, used, and stored Plaintiffs' and Class members' Biometric Data derived from Plaintiffs' and Class members' facial geometry without first obtaining the written release required by 740 ILCS 14/15(b)(3), and thereby uniformly invaded Plaintiffs' and each Class member's statutorily protected right to privacy in their Biometric Data. Likewise, Defendant failed to properly inform Plaintiffs or members of the Class in writing that their Biometric Data was being collected, stored, or otherwise obtained, and of the specific purpose and length of term for which those biometrics were being collected, stored, and used, as required by 740 ILCS 14/15(b)(1)-(2).

83. Defendant knowingly sold, leased, traded, and/or otherwise profited from Plaintiffs' and the BIPA Class's Biometric Data. See 740 ILCS 14/15(c).

84. Defendant also disclosed, redisclosed, and/or otherwise disseminated Plaintiffs' and the Class's Biometric Data without obtaining the consent from Plaintiffs' and the Class and/or their authorized representatives. The disclosure, redisclosure, and/or dissemination by Defendant of Plaintiffs' and the Class's Biometric Data was not to complete a financial transaction requested or authorized by Plaintiffs or members of the Class, nor was the disclosure and/or redisclosure required by state or federal law, municipal ordinance, or required pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction. See 740 ILCS 14/15(d).

85. Plaintiffs and the Class have been directly harmed by Defendant's violations of

Sections 14/15(a)-(d) of BIPA. They have been deprived of their control over their valuable information and otherwise suffered monetary and non-monetary losses. By depriving Plaintiffs and the Class of control over their valuable information, Defendants misappropriated the value of their Biometric Data. Based on information and belief, Defendant has profited from its unlawful conduct.

86. Each instance in which Defendant collected, stored, used, or otherwise obtained Plaintiffs' and/or members of the Class's Biometric Data as described herein constitutes a separate violation of the statutory right of Plaintiffs and each Class member to keep private this Biometric Data, as set forth in BIPA, 740 ILCS 14/1, et seq.

87. On behalf of themselves and members of the proposed Class, Plaintiffs seeks: (1) injunctive and equitable relief as is necessary to protect the interests of Plaintiffs and the Class by requiring Defendant to comply with BIPA's requirements, including BIPA's requirements for the collection, storage, and use of biometric identifiers and biometric information as described herein, and for the provision of the requisite written disclosure to consumers; (2) statutory damages of \$5,000 for each and every intentional and reckless violation of BIPA pursuant to 740 ILCS 14/20(2), or, alternatively, statutory damages of \$1,000 for each and every violation pursuant to 740 ILCS 14/20(1) if the violations are found to have been committed negligently; and (3) reasonable attorneys' fees and costs and other litigation expenses pursuant to 740 ILCS 14/20(3).

COUNT II
Unjust Enrichment/Restitution
(On Behalf of Plaintiffs and the Class)

88. Plaintiffs hereby reallege and incorporate by reference the allegations contained in the paragraphs above as if fully set forth herein.

89. Defendants obtained a monetary benefit from Plaintiffs and Class Members to their

detriment. Defendants did so by profiting off of the covert collection of the Biometric Data of Plaintiffs and Class Members, while exposing Plaintiffs and Class members to great risks of surveillance. None of this conduct was authorized by Plaintiffs and Class Members

90. Defendant appreciated, accepted, and retained the benefit exposed on it under inequitable and unjust circumstances arising from Defendant's conduct toward Plaintiffs and Class Members as described herein.

91. Defendant was unjustly enriched by its unlawful misappropriation of Plaintiffs' and the Class's Biometric Information. Through its unlawful conduct, Defendant received and retained a benefit it otherwise would not have achieved. By depriving Plaintiffs and the Class of control over their valuable Biometric Data, Defendant took control of and misappropriated the value of their Biometric Data. Defendant's conduct also exposed Plaintiffs and the Class to a heightened risk of an invasion of their privacy.

92. Defendants acquired and caused to be acquired Plaintiffs' and Class Members' Biometric Data through inequitable means in that they acquired it without the consent and permission required by Illinois law.

93. There is not an adequate remedy at law here. It would be unjust and unfair for Walmart to retain any of the benefits obtained from its unlawful misappropriation of Plaintiffs' and the Class's Biometric Data. Defendant should be ordered to disgorge the monies that it unjustly received from the misappropriation of Plaintiffs' and the Class's Biometric Data.

COUNT III
Request for Relief Under the Declaratory Judgment Act
28 U.S.C. §§2201, et seq.
(On Behalf of Plaintiffs and the Class)

94. Plaintiffs hereby reallege and incorporate by reference the allegations contained in

the paragraphs above as if fully set forth herein.

95. Under the Declaratory Judgment Act, 28 U.S.C. §§2201, et seq., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and that violate the terms of the statutes described herein.

96. An actual controversy has arisen in the wake of Defendant's unlawful collection, disclosure, sale, and misuse of Plaintiffs' and the Class's photographs and biometric identifiers and information without their consent, as alleged herein, in violation of Defendant's common law and statutory duties.

97. Plaintiffs continue to suffer injury and damages, as described herein, as Defendant continues to collect, disclose, sell, and misuse Plaintiffs' and Class members' photographs and biometric identifiers and information.

98. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

- Defendant continues to owe a legal duty to not collect, disclose, sell, and otherwise misuse Plaintiffs' and Class members' photographs and biometric identifiers and information under, among other things, the common law and the BIPA, 740 ILCS 14/1, et seq.
- Defendant continues to breach its legal duties to Plaintiffs and Class members by continuing to collect, disclose, sell, and otherwise misuse Plaintiffs' and Class members' photographs and biometric identifiers and information; and
- Defendant's ongoing breaches of its legal duty continue to cause Plaintiffs and Class members harm.

99. The Court should also issue corresponding injunctive relief, including, but not limited to, enjoining Defendant from engaging in the unlawful conduct alleged in this claim and requiring Defendant to delete all photographs and biometric identifiers and information of Plaintiffs and Class members and cease further collecting of such information or engaging in any activities that would result in the disclosure, sale, or misuse of Plaintiffs' and Class members' photographs and biometric identifiers and information. If an injunction is not issued, Plaintiffs will suffer irreparable injury and lack an adequate legal remedy in the event the statutory or common law does not prohibit, among other things, the collection, disclosure, sale, and misuse of photographs and biometric identifiers and information. Illinois specifically constrains the collection, disclosure, and sale of biometric information and recognizes a person's right to maintain such personal information as private. In light of Defendant's pervasive flaunting of such rights, including the continued collection, disclosure, sale, and misuse of Plaintiffs' and Class members' photographs and biometric identifiers and information, the risk of continued violations of Illinois law and the common law is real, immediate, and substantial. Plaintiffs do not have an adequate remedy at law because many of the resulting injuries are recurring and Plaintiffs will be forced to bring multiple lawsuits to rectify the same conduct.

100. The hardship to Plaintiffs and the Class if an injunction is not issued exceeds the hardship to Defendant if an injunction is issued. On the other hand, the cost to Defendant of complying with an injunction by complying with Illinois law and the common law by ceasing to engage in the misconduct alleged herein is relatively minimal, and Defendant has a pre-existing legal obligation to avoid invading the privacy rights of consumers.

101. Issuance of the requested injunction will serve the public interest by preventing ongoing collection, disclosure, sale, and misuse of photographs and biometric identifiers and

information without consent, thus eliminating the injuries that would result to Plaintiffs and the Class.

PRAYER FOR RELIEF

102. WHEREFORE, Plaintiffs, on behalf of themselves and the proposed Class, respectfully requests that this Court enter an Order:

- a. Certifying this case as a class action on behalf of the Class defined above, appointing Plaintiffs as representatives of the Class, and appointing their counsel as Class Counsel;
- b. Declaring that the actions of Defendant, as set out above, violate BIPA, 740 ILCS 14/1, et seq.;
- c. Awarding compensatory, non-compensatory, statutory, exemplary, and punitive damages;
- d. Awarding injunctive and other equitable relief as is necessary to protect the interests of the Class, including, among other things, an order requiring that Defendant ensures its collection, storage, and usage of Biometric Data complies with BIPA;
- e. Awarding Plaintiffs and the Class statutory damages of \$5,000 for each and every intentional and/or reckless violation of BIPA pursuant to 740 ILCS 14/20(2), and statutory damages of \$1,000 for each and every negligent violation of BIPA pursuant to 740 ILCS 14/20(1);
- f. Awarding restitution of all monies, expenses, and costs due to Plaintiffs and the Class;
- g. Awarding Plaintiffs and the Class reasonable litigation expenses and attorneys'

fees;

- h. Awarding Plaintiffs and the Class pre- and post-judgment interest, to the extent allowable;
- i. Awarding injunctive and other equitable relief, as necessary, to protect the interests of the Class, including, among other things, an order requiring Defendants to comply with the BIPA and enjoining Defendants from engaging in the unlawful conduct alleged herein; and
- j. Awarding such other and further relief as equity and justice may require.

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand that this matter be tried before a jury.

Date: October 28, 2022

Respectfully Submitted,

s/ 

Bryan J. O'Connor
WHITESIDE & GOLDBERG, LTD.
155 N. Michigan Ave. - Suite 540
Chicago, IL 60601
Phone: (312) 334-6875

William M. Audet (SBN 117456)*
Ling Y. Kuang (SBN 296873)*
Kurt D. Kessler (SBN 327334)*
AUDET & PARTNERS, LLP
711 Van Ness, Suite 500
San Francisco, CA 94102-3229
Telephone: 415.568.2555
waudet@audetlaw.com
lkuang@audetlaw.com
kkessler@audetlaw.com

**Application for pro hac vice forthcoming*

Counsel for Plaintiffs and Proposed Class