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

BRANDY ACALEY, individually, and on behalf of all others similarly situated,	)	
Plaintiff,	)	**Case No.** 2021CH00034
v.	)	
ECOATM, LLC,	)	
Defendant.	)	

CLASS ACTION COMPLAINT

Plaintiff, Brandy Acaley, brings this Complaint ("Complaint"), by and through her attorneys, individually and on behalf of all others similarly situated (the "Class"), brings the following Class Action Complaint ("Complaint") pursuant to the Illinois Code of Civil Procedure, 735 ILCS §§ 5/2-801 and 2-802, against EcoATM, LLC ("EcoATM" or "Defendant") to redress and curtail Defendant's unlawful collection, use, storage, and disclosure of Plaintiff's sensitive biometric data. Plaintiff alleges as follows upon personal knowledge as to herself, her own acts and experiences and, as to all other matters, upon information and belief, including investigation conducted by her attorneys.

NATURE OF THE ACTION

1. Defendant, EcoATM, develops, manufactures, and maintains self-serve kiosks used to recycle smart devices. EcoATM has installed thousands of these kiosks in stores across the United States and throughout Cook County, including Walmart, Kroger, and other major retailers.

2. EcoATM requires its users to provide biometric identifiers and/or biometric information ("biometric data"), in the form of their facial geometry, in order to use the services provided by the kiosks.

3. Facial geometry is a unique, permanent biometric identifier associated with each user that cannot be changed or replaced if stolen or compromised. This exposes users to serious and irreversible privacy risks. For example, if a database containing facial geometry or other sensitive, proprietary biometric data is hacked, breached, or otherwise exposed – like in the recent Yahoo, eBay, Equifax, Uber, Home Depot, MyFitnessPal, Panera, Whole Foods, Chipotle, Omni Hotels & Resorts, Trump Hotels and Facebook/Cambridge Analytica data breaches – website users have ***no*** means by which to prevent identity theft, unauthorized tracking, and other improper or unlawful use of this highly personal and private information.

4. 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.

5. 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 hand prints, iris scans, and a facial photograph – of over a billion Indian citizens. See Vidhi Doshi, A Security Breach in India Has Left a Billion People at Risk of Identity Theft, The Washington Post (Jan. 4, 2018), available at https://www.washingtonpost.com/news/worldviews/wp/2018/01/04/a-security-breach-in-india-has-left-a-billion-people-at-risk-of-identity-theft/?utm_term=.b3c70259fl38.

6. 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.

7. 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.

8. 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.

9. 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.

10. Recognizing the need to protect its citizens from situations like these, Illinois enacted the Biometric Information Privacy Act ("BIPA"), 740 ILCS 14/1, *et seq.*, specifically to regulate the collection and storage of Illinois citizens' biometrics, such as facial geometry.

11. Notwithstanding the clear and unequivocal requirements of the law, Defendant disregards users' statutorily protected privacy rights and unlawfully collects, stores, and uses their biometric data in violation of BIPA. Specifically, Defendant has violated and continues to violate BIPA because it did not and continues not to:

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

b. Provide a publicly available retention schedule and guidelines for permanently destroying Plaintiff's and other similarly situated individuals' facial geometry, as required by BIPA; and

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

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

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

PARTIES

13. Plaintiff Brandy Acaley is a natural person and a citizen of the State of Illinois.

14. Defendant EcoATM is a corporation organized under the laws of the state of Delaware with a principal place of business in San Diego, California. EcoATM conducts business in Illinois, including in Cook County.

JURISDICTION AND VENUE

15. This Court has jurisdiction over Defendant pursuant to 735 ILCS 5/2-209 because it conducts business transactions in Illinois and committed statutory violations and tortious acts in Illinois.

16. Venue is proper in Cook County because Defendant conducts business in Cook County and committed statutory violations in Cook County.

FACTUAL BACKGROUND

I. The Biometric Information Privacy Act.

17. 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.

18. 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 hand print 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

had used that company's fingerprint scanners were completely unaware the scanners were not 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.

19. 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.

20. 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.

21. 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 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.

See 740 ILCS 14/15(b).

22. Biometric identifiers include retina and iris scans, voiceprints, finger scans and fingerprints, and – most importantly here – facial geometry. *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*.

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

24. 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).

25. 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.

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

of action if there is a qualifying data breach, BIPA strictly regulates the manner in which entities may collect, store, use, and disseminate biometrics and creates a private right of action for lack of statutory compliance.

27. Plaintiff, like the Illinois legislature, recognizes how imperative it is to keep biometric data secure. Biometric data, 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.

28. By the time BIPA passed through the Illinois Legislature in mid-2008, most companies who had experimented with using Illinoisans' biometric data as an authentication method stopped doing so.

29. However, Defendant failed to take note of the shift in Illinois law governing the collection, use, and dissemination of biometric data. As a result, Defendant continues to collect, store, use, and disseminate users' biometric data in violation of BIPA.

30. Specifically, Defendant requires users of its kiosks to submit to at least two facial geometry scans. First, a camera at Defendant's kiosk captures and collects a contemporaneous scan of the user's facial geometry through the use of face-based biometric software..

31. Next, Defendant requires the user to insert his or her government-issued identification card into the kiosk. Defendant scans the government-issued identification card ("ID card") and extracts, captures, and collects facial geometry data from the ID card.

32. Defendant's kiosks analyze and compare the facial geometry data captured from the user's contemporaneous scan to the facial geometry data captured from scan of the user's ID card in order to calculate the similarity of the data.

33. If Defendant's kiosk determines the facial geometry data from the two scans are sufficiently similar, the user is permitted to complete recycling his or her used device. If the facial geometry data from the two scans is not similar, the kiosk will terminate the session and prevent the user from continued use of the device.

34. Defendant stores the facial geometry data captured and collected from both the contemporaneous scan and the ID card scan of each user in its database.

35. EcoATM fails to inform users that EcoATM is collecting, storing, or using their sensitive biometric data, the extent of the purposes for which it collects their sensitive biometric data, or to whom the data is disclosed, if it all.

36. Defendant fails to develop or adhere to a written, publicly-available policy identifying its retention schedule and guidelines for permanently destroying users' biometric data when the initial purpose for collecting or obtaining their biometrics is no longer relevant, as required by BIPA.

37. In addition, EcoATM profits from the use of users' biometric data. For instance, EcoATM markets its biometric verification features as superior options to typical methods of identity verification and theft prevention. By marketing Defendant's products and services in this manner, Defendant obtains a competitive advantage in the secondary device-sales market and secures profits from its use of biometric data, all while failing to comply with the minimum requirements for handling users' biometric data established by BIPA.

38. The Pay by Touch bankruptcy that catalyzed the passage of BIPA, as well as the recent Equifax and Uber data breaches, highlight why conduct such as Defendant's – where individuals are aware that they are providing facial geometry, but not aware of to whom or for what purposes they are doing so – is dangerous. The Pay by Touch bankruptcy spurred Illinois

citizens and legislators into realizing that it is crucial for individuals to understand when providing biometric identifiers, such as facial geometry, who exactly is collecting their biometric data, where it will be transmitted, for what purposes, and for how long. Defendant disregards these obligations and Plaintiff's statutory rights. Instead, Defendant unlawfully collects, stores, uses and disseminates Plaintiff's biometric identifiers and information, without ever receiving the individual's informed written consent required by BIPA.

39. Defendant lacks retention schedules and guidelines for permanently destroying Plaintiff's and other similarly situated individuals' biometric data and has not and will not destroy Plaintiff's and other similarly situated individuals' biometric data when the initial purpose for collecting or obtaining such data has been satisfied or within three years of the user's last interactions with the company.

40. Plaintiff and other similarly situated individuals are not told what might happen to their biometric data if and when Defendant merges with another company, or worse, if and when Defendant's entire organization folds.

41. Because Defendant neither publishes a BIPA-mandated data retention policy nor discloses the purposes for its collection of biometric data, users have no idea whether Defendant sells, discloses, re-discloses, or otherwise disseminates their biometric data. Moreover, Plaintiff and others similarly situated are not told to whom Defendant currently discloses their biometric data, or what might happen to their biometric data in the event of a merger or a bankruptcy.

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

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

III. Plaintiff Brandy Acaley's Experience.

44. Plaintiff began visiting Defendant's kiosks in 2016 in order to recycle several of her smart devices. Plaintiff has used the kiosk multiple times during the past year including twice in June 2020 and again in November 2020, at different kiosk locations located inside Walmart stores in Rockford, IL.

45. To use the kiosk, Plaintiff was required to provide a contemporaneous, "real time" scan of her facial geometry while she used Defendant's kiosk. Plaintiff was additionally required to provide her driver's license.

46. Defendant captured and collected Plaintiff's facial geometry data from both the contemporaneous scan of Plaintiff and from its scan of her driver's license.

47. Defendant subsequently stored Plaintiff's biometric data in its database(s).

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

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

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

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

52. Unlike a social security number that can be changed, no amount of time or money can compensate Plaintiff if her biometric data is compromised by the lax procedures through which Defendant captured, stored, used, and disseminated her and other similarly situated individuals'

biometrics. Plaintiff would not have provided her biometric data to Defendant if she had known that it would retain such information for an indefinite period of time without her consent.

53. 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").

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

CLASS ALLEGATIONS

55. 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.

56. As discussed *supra*, Section 14/15(b) of BIPA prohibits a company from, among other things, collecting, obtaining, 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, obtained, or stored; (2) informs the individual in writing of the specific purpose(s) and length of time for which a biometric identifier or biometric information is being collected, obtained, stored, and used; ***and*** (3) receives a written release executed by the subject of the biometric identifier or biometric information. 740 ILCS § 14/15.

57. 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 the State of Illinois who had their biometric identifiers and information collected, captured, received, obtained, maintained, stored, or disclosed by Defendant during the applicable statutory period.

58. This action is properly maintained as a class action under 735 ILCS 5/2-801 because:

A. The class is so numerous that joinder of all members is impracticable;

B. There are questions of law or fact that are common to the class;

C. The claims of the Plaintiff are typical of the claims of the class; and,

D. The Plaintiff will fairly and adequately protect the interests of the class.

Numerosity

59. The total number of putative class members exceeds fifty (50) individuals. The exact number of class members may easily be determined from Defendant's database.

Commonality

60. 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 not limited to the following:

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

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

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

D. Whether Defendant has disclosed or re-disclosed Plaintiff's and the Class' biometric identifiers or biometric information;

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

F. 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;

G. Whether Defendant complies with any such written policy (if one exists);

H. Whether Defendant used Plaintiff's and the Class' facial geometry to identify them;

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

J. Whether the violations of BIPA were committed negligently;

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

61. Plaintiff anticipates that Defendant will raise defenses that are common to the class.

Adequacy

62. Plaintiff will fairly and adequately protect the interests of all members of the class, and there are no known conflicts of interest Plaintiff and class members. Plaintiff, moreover, has retained experienced counsel that are competent in the prosecution of complex litigation and who have extensive experience acting as class counsel.

Typicality

63. 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.

64. 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

65. 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.

66. 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

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

68. 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).

69. Defendant fails to comply with these BIPA mandates.

70. Defendant EcoATM is a Delaware corporation that conducts business in Illinois and thus qualifies as a "private entity" under BIPA. *See* 740 ILCS § 14/10.

71. 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.

72. 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.

73. Defendant failed to provide a publicly available retention schedule or guidelines for permanently destroying biometric identifiers and biometric information as specified by BIPA. *See* 740 ILCS § 14/15(a).

74. 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 and the Class's biometric data when the initial purpose for collecting or obtaining such data has been satisfied or within three years of the individual's last interaction with the company.

75. 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 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 willful 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

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

77. 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).

78. Defendant fails to comply with these BIPA mandates.

79. Defendant EcoATM is a Delaware corporation that conducts business in Illinois and thus qualifies as a "private entity" under BIPA. *See* 740 ILCS § 14/10.

80. 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.

81. 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.

82. Defendant systematically and automatically collected, used, and stored Plaintiff's biometric identifiers and/or biometric information without first obtaining the written release required by 740 ILCS 14/15(b)(3).

83. Defendant did not inform Plaintiff in writing that her biometric identifiers and/or biometric information were being collected, stored and used, nor did Defendant inform Plaintiff in writing of the specific purpose and length of term for which her biometric identifiers and/or biometric information were being collected, stored, and used as required by 740 ILCS 14/15(b)(1)-(2).

84. By collecting, storing, and using 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.

85. 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 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 willful and/or reckless violation of BIPA pursuant to 740 ILCS 14/20(2) or, in the alternative, statutory damages of $1,000 for each negligent violation of BIPA pursuant to 740 ILCS

14/20(1); and (4) reasonable attorneys' fees and costs and other litigation expenses pursuant to 740 ILCS 14/20(3).

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

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

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

88. Defendant fails to comply with this BIPA mandate.

89. Defendant EcoATM is a Delaware corporation that conducts business in Illinois and thus qualifies as a "private entity" under BIPA. *See* 740 ILCS § 14/10.

90. 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.

91. 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.

92. Defendant systematically and automatically disclosed, redisclosed, or otherwise disseminated Plaintiff'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 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 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 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 Brandy Acaley 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 Brandy Acaley 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* willful 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 or reckless;

E. Awarding injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and the Class, including an Order requiring Defendant to collect, store, use and disseminate biometric identifiers or biometric information in compliance with BIPA;

F. Awarding Plaintiff and the Class their reasonable attorneys' fees and costs and other litigation expenses pursuant to 740 ILCS 14/20(3);

G. Awarding Plaintiff and the Class pre- and post-judgment interest, to the extent allowable; and,

H. Awarding such other and further relief as equity and justice may require.

Date: January 5, 2021 Respectfully Submitted,

/s/ Catherine T. Mitchell
Ryan F. Stephan
James B. Zouras
Catherine T. Mitchell
STEPHAN ZOURAS, LLP
100 North Riverside Plaza
Suite 2150
Chicago, Illinois 60606
312.233.1550
312.233.1560 *f*
rstephan@stephanzouras.com
jzouras@stephanzouras.com
cmitchell@stephanzouras.com
Firm ID: 43734

ATTORNEYS FOR PLAINTIFF