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

BRIA RANDLE, VANESSA GUSMAN, KASIE SEDWICK, NICOLE DEMONTE, AINSLEY JACOBSON, and BRANDY LUKER, INDIVIDUALLY AND ON BEHALF OF ALL OTHERS SIMILARLY SITUATED, *Plaintiffs*, v. MATCH GROUP, INC., MATCH GROUP, LLC, and TINDER, INC. *Defendants*.	)	2022CH09803 Case No.: Judge:

CLASS ACTION COMPLAINT

Plaintiffs Bria Randle, Vanessa Gusman, Kasie Sedwick, Nicole DeMonte, Ainsley Jacobson, Brandy Luker (hereinafter "Plaintiffs"), brings this Class Action Complaint individually and on behalf of all others similarly situated against Defendants Match Group, Inc., Match Group LLC, and Tinder, Inc. (hereinafter "Defendants") to stop Defendants' unlawful collection, use, storage, and disclosure of Plaintiffs' and the proposed Class's sensitive, private, and personal biometric data. Plaintiffs allege as follows upon personal knowledge as to themselves and their own acts and experiences and, as to all other matters, upon information and belief including investigation conducted by their attorneys. Further, Plaintiffs allege as follows:

PARTIES, JURISDICTION, AND VENUE

1. Plaintiff Bria Randle is a natural person and citizen of Illinois.

2. Plaintiff Vanessa Gusman is a natural person and citizen of Illinois.

3. Plaintiff Kasie Sedwick is a natural person and citizen of Illinois.

4. Plaintiff Nicole DeMonte is a natural person and citizen of Illinois.

5. Plaintiff Ainsley Jacobson is a natural person and citizen of Illinois.

6. Plaintiff Brandy Luker is a natural person and citizen of Illinois.

7. Defendant Match Group, Inc. is a Delaware corporation with a principal place of business in Texas.

8. Defendant Match Group, Inc. may be served through its registered agent, The Corporation Trust Company, Corporation Trust Center, 1209 Orange Street, Wilmington, DE 19801.

9. Defendant Match Group, LLC is a Delaware limited liability corporation with a principal place of business in Texas.

10. Defendant Match Group, LLC may be served through its registered agent, The Corporation Trust Company, Corporation Trust Center, 1209 Orange Street, Wilmington, DE 19801.

11. Upon information and belief, Defendant Match Group, Inc. owns and controls Defendant Match Group, LLC.

12. Defendant Tinder, Inc. is a Delaware corporation with a principal place of business in Texas.

13. Defendant Tinder, Inc. may be served through its registered agent, The Corporation Trust Company, Corporation Trust Center, 1209 Orange Street, Wilmington, DE 19801.

14. Upon information and belief, Defendant Tinder, Inc. is the entity through which Defendant Match Group, LLC operates, owns, and/or does business as Tinder.

15. Jurisdiction is proper in this Court as Plaintiffs are citizens of Illinois and Defendants operates their business in Illinois, targets business activity in Illinois, and purposefully avails itself of the laws, protections, and advantages of doing business in Illinois, with Illinois consumers like Plaintiffs.

16. Venue is proper in this Court, as upon information and belief, a substantial part of the events giving rise to the claim occurred in this county.

INTRODUCTION

17. Defendant Match Group, Inc. is an American internet and technology company that owns and operates the largest global portfolio of popular online dating services including Tinder, Match.com, Meetic, OKCupid, Hinge, PlentyOfFish, Ship, and OurTime, totaling over 45 global dating companies. [1]

18. Tinder is a free app developed by Match Group, Inc. that is available both on Android and iOS.

19. Match Group, Inc. begin using selfie biometrics for identify verification in Tinder in early 2020. [2]

20. Tinder connects its users with profiles using location-based technology based on gender, distance and orientation filters you set. [3]

21. Tinder offers Photo Verification to make sure the person on the account matches their photos. Verified profiles will have a blue checkmark. [4]

22. Tinder's Photo Verification consists of one simple step of taking a video selfie. You will receive a "Photo Verified" status if the person in your video selfie passes both the Liveness Check and 3d Face Authentication steps. [5]

23. Tinder's Liveness Check scans the user's face in their video and helps Tinder confirm that the video was taken by a real, live person, and that it was not digitally altered or manipulated. 3D Face Authentication detects the user's face in their video selfie and their profile photos, and extracts facial geometries using facial recognition technology to generate a unique number or facial geometry "template." [6]

---

[1] Available at https://en.wikipedia.org/wiki/Match_Group (last accessed Sept. 23, 2022).
[2] Available at https://en.wikipedia.org/wiki/Match_Group (last accessed Sept. 23, 2022).
[3] Available at https://tinder.com/faq (last accessed Sept. 23, 2022).

24. Defendants unlawfully store the biometric facial scans of its customers without their consent.

25. Defendants have failed – and continue to fail – to follow Illinois' Biometric Information Privacy Act, 740 ILCS 14/1, *et seq*. This failure is of great concern to Plaintiffs because it exposes Plaintiffs to serious and irreversible privacy risks.

26. The State of Illinois takes the privacy of biometric data seriously. The State's approach is not particularly surprising in light of recent events related to biometric identifiers.

27. If a biometric database is hacked, breached, or otherwise exposed – such as in the recent Equifax, and Marriott data breaches or misused such as the recent SolarWinds hack by Russian agents that exposed hundreds of companies' data – employees 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] Available at https://tinder.com/faq (last accessed Sept. 23, 2022).

[5,6]Available at https://www.help.tinder.com/hc/en-us/articles/4422771431309-How-Does-Selfie-Verification-Work- (last accessed Sept. 23, 2022).

28. Hackers regularly target biometric databases. 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.[7]

29. Moreover, an illegal market already exists for biometric data. For example, hackers and identity thieves have targeted Aadhaar, the largest biometric database in the world. That database contains the personal and biometric data – including fingerprints, iris scans, and a facial photograph – of over a billion Indian citizens.[2] In January 2018, an Indian newspaper reported that the

[7] U.S. Off. of Personnel Mgmt., *Cybersecurity Incidents* (2018), available at www.opm.gov/cybersecurity/cybersecurity-incidents.

[8]*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-inindiahas-left-a-billion-people-at-risk-of-identity-theft/?utm_term=.b3c70259f138.

information housed in Aadhaar was available for purchase for less than $8 and could be obtained in as little as 10 minutes.[8]

30. Unlike written passwords or social security numbers – which can be changed or replaced if stolen or compromised – biometrics are unique, permanent biometric identifiers associated with each individual.

31. There is no realistic way, absent surgery, to reassign someone's biometric data. A person can obtain a new social security number, but not a new face, which makes the protection of, and control over, biometric identifiers and biometric information particularly important.

32. 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 and store Illinois citizens' biometrics.

33. Defendants capture biometric facial scans, one of the specifically enumerated forms of biometric identifiers set forth in BIPA, both directly and indirectly, from any and all individuals whose facial scans are collected using Tinder. Defendants collect and retains these facial scans in a database.

34. Notwithstanding the clear and unequivocal requirements of Illinois law, Defendants violated Illinois individuals' statutorily protected privacy rights and unlawfully collected, stored, and used those individuals' biometric data in violation of BIPA. In particular, Defendants have violated and continues to violate BIPA because it did not, upon information and belief:

a. Properly inform Plaintiffs and others similarly situated in writing of the specific purpose and length of time for which their biometric facial scan(s) were being collected, stored, disseminated and used, as required by BIPA;

b. Provide a publicly available retention schedule and guidelines for permanently destroying Plaintiffs' and other similarly-situated individuals' biometric facial scan(s), as required by BIPA;

c. Receive a written release from Plaintiffs and others similarly situated to collect, store, disseminate or otherwise use their biometric facial scan(s), as required by BIPA; and

d. Obtain a written release from Plaintiffs and others similarly situated to disclose, redisclose, or otherwise disseminate their biometric identifiers and/or biometric information to a third party as required by BIPA.

35. Plaintiffs and the putative Class are aggrieved by Defendants' failure to destroy their biometric data when the initial purpose for collecting or obtaining such data has been satisfied or within three years of individual's last interactions with the entity.

ILLINOIS'S STRONG STANCE ON PROTECTION OF BIOMETRIC INFORMATION

36. BIPA provides valuable privacy rights, protections, and benefits to citizens of Illinois.

37. In passing BIPA, the Illinois General Assembly found that major national corporations started using Chicago and other locations in Illinois in the early 2000s 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(b). Given its relative infancy, an overwhelming portion of the public became weary of this then- growing yet unregulated technology. See 740 ILCS 14/5.

38. 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. The bankruptcy was alarming to the Illinois General Assembly because there was suddenly a serious risk that millions of fingerprint records – which, similar to 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 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.

39. 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.

40. The Illinois General Assembly explicitly acknowledged that Biometrics "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." 740 ILCS 14/5(c)

41. BIPA provides individuals with a private right of action, protecting their right to privacy regarding their biometrics as well as protecting their rights to know the precise nature for which their biometrics are used and how they are being stored and ultimately destroyed. Unlike other statutes that only create a right of action if there is a qualifying data breach, BIPA strictly regulates the manner in which entities may collect, store, use, and disseminate biometrics and creates a private right of action for lack of statutory compliance.

42. To ensure such 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.

43. 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).

44. Biometric identifiers include "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face 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*.

45. 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 that disclosure. *See*, 740 ILCS 14/15(d)(1).

46. 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).

47. Plaintiffs, like the Illinois General Assembly, recognizes how imperative it is to keep biometric information secure. Biometric information, unlike other personal identifiers such as a social security number, cannot be changed or replaced if hacked or stolen.

PLAINTIFFS SPECIFIC ALLEGATIONS

48. Plaintiffs are customers of Match Group, Inc., Match Group LLC and/or Tinder, Inc. ("Defendants"), who, upon information and belief, utilizes Defendants' Photo Verification and Liveness Check for its identification verification through biometric authentication.

49. Defendants offer their customers "Photo Verification" and "Liveness Check" which allows its customers to authenticate themselves in their video selfies to pass through the Liveness Check and 3d Face Authentication.

50. Defendants utilize the biometric facial scans by scanning the customer's face in their video and uses that to confirm that the video was taken by a real, live person, and was not digitally altered or manipulated.

51. Defendants' 3D Face Authentication detects the customer's face in the video selfie and their profile photos, and extracts facial geometries using facial recognition technology to generated a unique number or facial geometry "template."

52. These biometric facial scans are used by Defendants to verify if the customer in their video self is the same person that is in their profile photos.

53. Defendants state that they will only use the facial recognition information for the purpose of Photo Verification.

54. Upon information and belief, Plaintiffs have been utilizing Defendants' Photo Verification between approximately 2020 to current.

55. Upon information and belief, Defendants, either directly or indirectly, collected, utilized and stored the Plaintiffs' facial biometric identifiers in its database(s).

56. Storing Plaintiffs' biometric facial scans has value to Defendants because the larger the database, the more accurate and useful the database becomes.

57. Plaintiffs were never informed of the specific limited purposes or length of time for which Defendant collected, stored, or used their biometrics.

58. Plaintiffs were never informed of any biometric data retention policy developed by Defendant, nor have they ever been informed of whether Defendants will ever permanently delete their biometrics.

59. Plaintiffs were never provided with nor ever signed a written release allowing Defendants to collect, capture, store, or otherwise obtain their biometric facial scan or other biometrics.

60. Plaintiffs have continuously and repeatedly been exposed to the risks and harmful conditions created by Defendants' violations of BIPA alleged herein.

61. BIPA protects individuals like Plaintiffs and the putative Class from this precise conduct, and Defendants had no right to secure this data.

62. Through BIPA, the Illinois General Assembly has created a right – a right to receive certain information prior to an entity securing their highly personal, private and proprietary biometric data – and an injury – not receiving this extremely critical information.

63. Pursuant to 740 ILCS 14/15(b), Plaintiffs and the putative Class were entitled to receive certain information prior to Defendants securing their biometric data; namely, information advising them of the specific limited purpose(s) and length of time for which it/they collect(s), store(s), and use(s) their biometric facial scan(s) and any biometrics derived therefrom; information regarding Defendants' biometric retention policy; and, a written release allowing Defendants to collect and store their private biometric data.

64. No amount of time or money can compensate Plaintiffs if their biometric data is compromised by the lax procedures through which Defendants captured, stored, used, and disseminated Plaintiffs' and other similarly-situated individuals' biometrics, and Plaintiffs would not have provided their biometric data to Defendants if they had known that Defendants would retain such information for an indefinite period of time without their consent.

65. A showing of actual damages is not necessary in order to state a claim under BIPA. *See Rosenbach v. Six Flags Ent. Corp.*, 2019 IL 123186, ¶ 40 ("[A]n individual need not allege some actual injury or adverse effect, beyond violation of his or her rights under the Act, in order to qualify as "aggrieved" person and be entitled to seek liquidated damages and injunctive relief pursuant to the Act").

66. Plaintiffs are not required to allege or prove actual damages in order to state a claim under BIPA, and they seek statutory damages under BIPA as compensation for the injuries caused by Defendants. *Rosenbach*, 2019 IL 123186, ¶ 40.

DEFENDANTS' BIOMETRIC FACIAL-SCANNING OF ILLINOIS CITIZENS

67. Defendants have the means to achieve identity verification of their customers through biometric authentication.

68. Defendants have caused these biometrics to be associated with certain individuals' identities, along with other personal, private information for each individual.

69. However, on information and belief, Defendants do not acknowledge that Defendants are capturing and storing this sensitive biometric information when a customer uses one of Defendants' products their websites. To the contrary, an individual using Defendants' facial recognition software through a subsidiary, for example a customer like Plaintiffs here, likely will have no idea that Defendants are collecting this information or even that Defendants are connected in any way to the their facial recognition software.

70. Nor, on information and belief, Defendants link to their privacy statement such that any disclosures made there are known to their customers. Thus, a customer who does not know that his/her facial scan is being stored by Defendants has no means or reason to review Defendants' privacy statement.

71. As a result of the foregoing, on information and belief, despite capturing, collecting and retaining these biometrics, from their customers, Defendants do not adequately:

a. Inform their customers in writing that Defendants are capturing, obtaining, collecting, or storing biometric information or biometric identifiers;

b. Inform its subsidiaries' customers in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored,

and used; or

c. Receive a written release executed by its subsidiaries' customers consenting to collection, capture, obtainment, purchase, storage, or retention of biometric information or biometric identifiers.

72. Furthermore, on information and belief, Defendants' website, at relevant times hereto, did not have a written, publicly available policy identifying its biometrics retention schedule, nor did Defendants provide such information to their customers from whom Defendants were collecting their biometric facial scans.

73. Defendants, on information and belief, did not inform Plaintiffs in writing (or otherwise) that Defendants were obtaining, capturing, collecting and/or storing their biometric identifier, or of the specific purposes and length of term for which it would collect, capture, store, and/or use their biometric identifier or biometric information. Defendants did not obtain from Plaintiffs consent required by BIPA to capture, collect, store, obtain, and/or use Plaintiffs' biometric facial scan or associated biometrics.

74. Nor did Plaintiffs know or fully understand that Defendants were collecting, capturing, and/or storing biometrics when Plaintiffs was utilizing the biometric facial scan identity verification; nor did Plaintiffs know or could Plaintiffs know all of the uses or purposes for which Plaintiffs' biometrics were taken.

75. The Pay by Touch bankruptcy that catalyzed the passage of BIPA highlights why conduct such as Defendants' – where individuals are aware that they are providing a biometric but not aware of to whom or for what purposes they are doing so – is dangerous.

76. That bankruptcy spurred Illinois citizens and legislators into realizing that it is crucial for individuals to understand when providing biometric identifiers or information such as a finger

scan, and/or data derived therefrom, who exactly is collecting their biometric data, where it will be transmitted and for what purposes, and for how long.

77. Thus, BIPA is the Illinois General Assembly's expression that Illinois citizens have biometric privacy rights, as created by BIPA.

78. Defendants disregarded these obligations and instead unlawfully captured, collected, stored, and used individual's biometric identifiers and information, without ever receiving those individual's informed written consent as required by BIPA.

79. Because Defendants neither published a BIPA-mandated data retention policy nor disclosed the purposes for their collection of biometric data, their customers have no idea whether Defendants sell, disclose, re-disclose, or otherwise disseminate their biometric data.

80. Nor are Plaintiffs and the putative Class told to whom Defendants currently disclose their biometric data, or what might happen to their biometric data in the event of a buyout, merger, or a bankruptcy.

81. By and through the actions detailed above, Defendants have not only disregarded the Class' privacy rights, but it has also violated BIPA.

CLASS ALLEGATIONS

82. Plaintiffs bring this action on behalf of themselves and pursuant to 735 ILCS 5/2-801 on behalf of a class (hereinafter the "Class") defined as follows:

> All Illinois residents who directly or indirectly used Defendants' biometric authentication products and subsequently had his or her biometric facial scan captured, collected, stored, or otherwise obtained by Defendants during the applicable statutory period.

Excluded from the class are Defendants' officers and directors, Plaintiffs' counsel, and any member of the judiciary presiding over this action.

83. **Numerosity:** The exact number of class members is unknown and is not available to Plaintiffs at this time, but upon information and belief, there are in excess of forty potential class

members, and individual joinder in this case is impracticable. Class members can easily be identified through Defendants' records and allowing this matter to proceed on a class basis will prevent any retaliation by Defendants against individuals who are currently having their BIPA rights violated.

84. **Common Questions:** There are several questions of law and fact common to the claims of Plaintiffs and the Class members, and those questions predominate over any questions that may affect individual Class members. Common questions include, but are not limited to, the following:

a. whether Defendants collected, captured, received, or otherwise obtained Plaintiffs' and the Class' biometric identifiers;

b. whether Defendants properly informed Plaintiffs and the Class that it collected, used, and stored their biometric identifiers;

c. whether Defendants developed a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within three years of the individual's last interaction with Defendants, whichever occurs first;

d. whether Defendants obtained an executed written release (as defined in 740 ILCS 14/10) from Plaintiff and the Class to collect, capture, or otherwise obtain their biometric identifiers;;

e. whether Defendants obtained an executed written release (as defined in 740 ILCS 14/10) from Plaintiffs and the Class before capturing, collecting, converting, sharing, storing or using individuals' biometrics;

f. whether Defendants provided a writing disclosing to Plaintiffs and the Class the specific purposes for which the biometrics are being collected, stored, and used;

g. whether Defendants provided a writing disclosing to Plaintiffs and the Class the length of time for which the biometrics are being collected, stored, and used;

h. whether Defendants' conduct violates BIPA;

i. whether Defendants' conduct was negligent, reckless, or willful;

j. whether Plaintiffs and Class members are entitled to damages, and what is the proper measure of damages;

85. **Adequacy of Representation:** Plaintiffs will fairly and adequately represent and protect the interest of the class and has retained competent counsel experienced in complex litigation

and class action litigation. Plaintiffs have no interests antagonistic to those of the class, and Defendants have no defenses unique to Plaintiffs.

86. **Appropriateness:** Class proceedings are also superior to all other available methods for the fair and efficient adjudication of this controversy because joinder of all parties is impracticable. Further, it would be virtually impossible for the individual members of the Class to obtain effective relief because of the fear and likelihood of retaliation by Defendants against individuals bringing a civil action as an individual. Even if Class members were able or willing to pursue such individual litigation, a class action would still be preferable due to the fact that a multiplicity of individual actions would likely increase the expense and time of litigation given the complex legal and factual controversies presented in this Class Action Complaint. A class action, on the other hand, provides the benefits of fewer management difficulties, single adjudication, economy of scale, and comprehensive supervision before a single Court, and would result in reduced time, effort and expense for all parties and the Court, and ultimately, the uniformity of decisions.

COUNT I – FOR DAMAGES AGAINST DEFENDANTS
VIOLATION OF 740 ILCS 14/15(a) – FAILURE TO INSTITUTE, MAINTAIN, AND ADHERE TO PUBLICLY AVAILABLE RETENTION SCHEDULE

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

88. 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).

89. Defendants fail to comply with these BIPA mandates.

90. Plaintiffs and the Class are individuals who have had their "biometric identifiers" collected by Defendants, as explained in detail in above. See 740 ILCS 14/10.

91. Plaintiffs' biometric identifiers were used to identify Plaintiffs and, therefore, constitute "biometric information" as defined by BIPA. See 740 ILCS 14/10.

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

93. Upon information and belief, Defendants lack retention schedules and guidelines for permanently destroying Plaintiffs' and the Class' biometric data and have not and will not destroy Plaintiffs' and the Class' 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.

94. On behalf of themselves and the Class, Plaintiffs seek: (1) declaratory relief; (2) injunctive and equitable relief as is necessary to protect the interests of Plaintiffs and the Class by requiring the Defendants to comply with BIPA's requirements for the collection, storage, and use of biometric identifiers and biometric information as described herein; (3) statutory damages of $5,000 for each intentional and/or reckless violation of BIPA pursuant to 740 ILCS 14/20(2) or, in the alternative, statutory damages of $1,000 for each negligent violation of BIPA pursuant to 740 ILCS 14/20(1); and (4) reasonable attorneys' fees and costs and other litigation expenses pursuant to 740 ILCS 14/20(3).

COUNT II – FOR DAMAGES AGAINST DEFENDANTS
VIOLATION OF 740 ILCS 14/15(b) – FAILURE TO OBTAIN INFORMED WRITTEN CONSENT AND RELEASE BEFORE OBTAINING BIOMETRIC IDENTIFIERS OR INFORMATION

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

96. BIPA requires companies to obtain informed written consent from Illinois citizens 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).

97. Defendants fails to comply with these BIPA mandates.

98. Plaintiffs and the Class are individuals who have had their "biometric identifiers" collected by Defendants, as explained in detail above. *See* 740 ILCS 14/10.

99. Plaintiffs' and the Class' biometric identifiers were used to identify them and, therefore, constitute "biometric information" as defined by BIPA. *See* 740 ILCS 14/10.

100. Defendants systematically and automatically collected, used, stored and disseminated Plaintiffs' and the Class' biometric identifiers and/or biometric information without first obtaining the written release required by 740 ILCS 14/15(b)(3).

101. Defendants never informed Plaintiffs and the Class in writing that their biometric identifiers and/or biometric information were being collected, stored, used and disseminated, nor did Defendants inform Plaintiffs and the Class in writing of the specific purpose(s) and length of term for which their biometric identifiers and/or biometric information were being collected, stored, used and disseminated as required by 740 ILCS 14/15(b)(1)-(2).

102. By collecting, storing, using and disseminating Plaintiffs' and the Class' biometric identifiers and biometric information as described herein, Defendants violated Plaintiffs' and the Class' rights to privacy in their biometric identifiers and/or biometric information as set forth in BIPA. *See* 740 ILCS 14/1, *et seq*.

103. On behalf of themselves and the Class, Plaintiffs seeks: (1) declaratory relief; (2) injunctive and equitable relief as is necessary to protect the interests of Plaintiffs and the Class by requiring Defendants to comply with BIPA's requirements for the collection, storage, use and dissemination of biometric identifiers and biometric information as described herein; (3) statutory damages of $5,000 for each intentional and/or reckless violation of BIPA pursuant to 740 ILCS 14/20(2) or, in the alternative, statutory damages of $1,000 for each negligent violation of BIPA pursuant to 740 ILCS 14/20(1); and (4) reasonable attorneys' fees and costs and other litigation expenses pursuant to 740 ILCS 14/20(3).

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of the Class of similarly situated individuals, pray for an Order as follows:

A. Finding this action satisfies the prerequisites for maintenance as a class action set forth in 735 ILCS 5/2-801, *et seq*., and certifying the Class as defined herein;

B. Designating and appointing Plaintiffs as representative of the Class and Plaintiffs' undersigned counsel as Class Counsel;

C. Declaring that Defendants' actions, as set forth above, violate BIPA;

D. Awarding Plaintiffs and the Class members statutory damages of $5,000 for *each* intentional and/or reckless violation of BIPA pursuant to 740 ILCS 14/20(2); statutory damages of $1,000 per *each* negligent violation of BIPA pursuant to 740 ILCS 14/20(1);

E. Declaring that Defendants' actions, as set forth above, were intentional or reckless;

F. Declaring that Defendants' actions, as set forth above, were negligent;

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

H. Awarding Plaintiffs and the Class members reasonable attorneys' fees and costs incurred in this litigation pursuant to 740 ILCS 14/20(3);

I. Awarding Plaintiffs and the Class pre- and post-judgment interest, to the extent allowable; and

J. Granting all such other and further relief as the Court deems just and appropriate.

Dated: October 3, 2022

Respectfully Submitted:

By: */s/ Brandon M. Wise*
Brandon M. Wise – IL Bar # 6319580
Paul A. Lesko – IL Bar # 6288806
Adam Florek – IL Bar # 6320615
PEIFFER WOLF CARR KANE CONWAY & WISE, LLP
818 Lafayette Ave., Floor 2
St. Louis, MO 63104
Ph: 314-833-4825
Email: bwise@peifferwolf.com
Email: plesko@peifferwolf.com
Email: aflorek@peifferwolf.com

Mason A. Barney, Esq.
(*pro hac vice to be filed*)
Sonal Jain, Esq.
(*pro hac vice to be filed*)
SIRI & GLIMSTAD LLP
745 Fifth Ave, Suite 500,
New York, NY 10151
Tel: (212) 532-1091
mbarney@sirillp.com
sjain@sirillp.com

COUNSEL FOR THE PLAINTIFFS AND THE PUTATIVE CLASS