

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

AKSHAT JAIN, *individually and on behalf of  
all others similarly situated,*

Plaintiff,

v.

BEREAL,

Defendant.

Case No. 2023CH06863

**CLASS ACTION COMPLAINT**

Plaintiff, Akshat Jain, individually and on behalf of all other persons similarly situated, by his undersigned attorneys, for his Class Action Complaint for violations of the Illinois Biometric Information Privacy Act (“BIPA”), 740 ILCS 14/1 *et seq.*, against Defendant, BeReal, (“Defendant”), alleges on personal knowledge, investigation of his counsel, and on information and belief as follows:

**NATURE OF THE ACTION**

1. Plaintiff brings this action for damages and other legal and equitable remedies resulting from the illegal actions of Defendant in collecting, capturing, otherwise obtaining, storing and using Plaintiff’s and other similarly situated individuals’ biometric identifiers and biometric information (referred to collectively at times as “biometrics”) without obtaining informed written consent or providing the requisite data retention and destruction policies, in direct violation of BIPA.

2. The Illinois Legislature has found that “[b]iometrics are unlike other unique identifiers that are used to access finances or other sensitive information.” 740 ILCS 14/5(c). “For 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. In recognition of these concerns over the security of individuals’ biometrics the Illinois Legislature enacted BIPA, which provides, *inter alia*, that a private entity like Defendant may not obtain and/or possess an individual’s biometrics unless it: (1) informs that person in writing that biometric identifiers or information will be collected, otherwise obtained, or stored, *see id.*; (2) informs that person in writing of the specific purpose and length of term for which such biometric identifiers or biometric information is being collected, otherwise obtained, stored and used, *see id.*; (3) receives a written release from the person for the obtaining of his or her biometric identifiers or information, *see id.*; and (4) publishes publicly available written retention schedules and guidelines for permanently destroying biometric identifiers and biometric information, *see* 740 ILCS 14/15(a). Further, the entity must store, transmit and protect an individual’s biometric identifiers and biometric information using the same standard of care in the industry and in a manner at least as protective as the means used to protect other confidential and sensitive information. *Id.* 14/15 (c). Finally, the entity is expressly prohibited from selling, leasing, trading or otherwise profiting from the individual’s biometrics. *Id.* 15/15(c).

4. In direct violation of each of the foregoing provisions of § 15(a) and § 15(b) of BIPA, Defendant possessed, collected, captured, otherwise obtained, and used – without first providing notice, obtaining informed written consent or publishing data retention policies – the face geometry and associated personally identifying information of millions of people, including, upon information and belief, at least thousands of people in Illinois.

5. Defendant developed a software application (the “App”) that it offered to Illinois users. In order to create an account under the App, users provided their names and phone numbers. Then, at least once per day, the App prompted users to take a picture of themselves to be shared with other users. In some instances, if a user did not take pictures of his or her face, the App responded with comments such as “who goes there?” or “Umm, anybody here?”, indicating that the App used facial detection software. In other instances, when a user smiled, the App responded with comments such as “aye what a smile” or “bonus point for the smile,” indicating that the App used facial expression recognition software. Both facial detection and facial expression recognition use face geometry, a biometric identifier.

6. If the biometrics obtained by Defendant were to fall into the wrong hands, by data breach or otherwise, the users to whom these sensitive biometric identifiers belong could have their identities stolen. BIPA confers on Plaintiff and all other similarly situated Illinois residents a right to know of such risks, which are inherently presented by the obtaining and storage of biometrics, and a right to know how long such risks will persist. Yet Defendant never informed Plaintiff or the Class (as defined below) of its biometrics obtaining practices, never obtained required written consent from Plaintiff or the Class regarding its biometric practices, and never provided any biometric data retention or destruction policies to Plaintiff or the Class.

7. Plaintiff brings this action to prevent Defendant from further violating the privacy rights of Illinois residents, and to recover statutory damages for Defendant’s unauthorized collection, otherwise obtaining, storage and use of these individuals’ biometrics in violation of BIPA.

## JURISDICTION AND VENUE

8. This Court has personal jurisdiction over the Defendant because the face geometry that gives rise to this lawsuit was collected, otherwise obtained, and used by Defendant through the App from users in Illinois when they used the App. Defendant directs its business to users in Illinois.

9. Consistent with the Due Process Clauses of the Fifth and Fourteenth Amendments, this Court has *in personam* jurisdiction over the Defendant because it conducts commerce in the State of Illinois, and is therefore present in the State of Illinois such that requiring an appearance does not offend traditional notions of fair play and substantial justice.

10. The application of the law of France, rather than Illinois, would be contrary to a fundamental policy of Illinois which has a materially greater interest in protecting people in Illinois than France's interest in the determination of whether BIPA violations occurred in Illinois.

11. Litigation in France concerning Illinois resident's rights in Illinois under an Illinois statute, BIPA, when France does not have BIPA litigation or a history of class action litigation, would contravene the strong public policy of Illinois. Moreover, litigation and trial in France would be seriously inconvenient for Plaintiff, putative Class members, and the seemingly many potential witness employees of Defendant located in the United States.

12. Plaintiff had his biometric identifiers captured, collected, otherwise obtained, stored, or used by Defendant in Cook County, Illinois. Accordingly, venue is proper under 735 ILCS 5/1-108 and 2-101 of the Illinois Code of Civil Procedure.

## PARTIES

13. Plaintiff is a resident and citizen of New York, New York that took pictures using the BeReal app, on multiple occasions, within the state of Illinois.

14. Defendant BeReal is a French company with its headquarters at 30/32 Boulevard Sébastopol, 75004 Paris, France.

**FACTUAL BACKGROUND**

**I. Illinois’s Biometric Information Privacy Act**

15. In 2008, Illinois enacted BIPA due to the “very serious need [for] protections for the citizens of Illinois when it [comes to their] biometric information.” Illinois House Transcript, 2008 Reg. Sess. No. 276. BIPA makes it unlawful for a company to, *inter alia*, “collect, capture, purchase, receive through trade, or otherwise obtain a person’s or a customer’s biometric identifiers and/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 or the subject’s legally authorized representative.”

740 ILCS 14/15 (b).

16. 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).

17. A “biometric identifier” is a personal feature that is unique to an individual, including fingerprints, iris scans, DNA and “face geometry”, among others. 740 ILCS 14/10.

18. Merriam-Webster defines geometry as, among other things, a “configuration” and “an arrangement of objects or parts that suggests geometric figures.”<sup>1</sup>

19. “Biometric information” is any information captured, converted, stored, or shared based on a person’s biometric identifier used to identify an individual. 740 ILCS 14/10.

20. As alleged below, Defendant’s practices of collecting, otherwise obtaining, and using individuals’ biometric identifiers (specifically, face geometry) and associated biometric information without informed written consent violated all three prongs of § 15(b) of BIPA. Defendant’s failure to provide a publicly available written policy regarding their schedule and guidelines for the retention and permanent destruction of individuals’ biometric identifiers and biometric information also violated § 15(a) of BIPA.

**II. The App is a Social Media Application Used to Take and Send Photographs to Other of Defendant’s Users.**

21. The App “is the simplest photo sharing app to share once a day your real life in photo with friends. Every day at a different time, everyone captures a photo within 2 minutes.”<sup>2</sup> The App accesses the user’s camera and “[t]he special BeReal camera is designed to take both a selfie and a frontal photo simultaneously.”<sup>3</sup>

22. The photos are shared with other users. However, if a user shares the content globally, then they purportedly agree to grant Defendant “a worldwide, non-exclusive, royalty-free, sublicensable license to use, copy, reproduce, process, adapt, modify, publish, transmit, display and distribute the content you share with a Globally Shared Content in any and all media or distribution methods.” (See BeReal Terms attached as Exhibit A.)

---

<sup>1</sup> <https://www.merriam-webster.com/dictionary/geometry>

<sup>2</sup> <https://apps.apple.com/us/app/bereal-your-friends-for-real/id1459645446>

<sup>3</sup> Id.

23. Defendant asserts that it collects all sorts of different data, but it does not mention collecting biometric identifiers or information anywhere in its Terms or Privacy Policy. (See BeReal Privacy Policy attached as Exhibit B.)

24. The App encourages users to smile for the camera as they take a picture.

25. If the user smiles while taking the picture, the App will sometimes flash a message stating: “Bonus point for the smile!” or “Keep smiling and don’t change a thing.” or “Aye what a smile.” The App uses facial expression recognition software to determine whether users are smiling and to send these messages. Otherwise, the App would have no ability to determine whether the user was smiling or not smiling.

26. Facial expression recognition (“FER”) software takes facial recognition to another level, by recognizing the emotion expressed by a person’s face. As explained in the Abstract to an article surveying FER methods: “FER is to detect human emotional state related to biometric traits.”<sup>4</sup> Just like facial recognition, FER generally involves comparing features, points, or segments of certain parts of a person’s face in reference to the arrangement or configuration of other features, points, or segments of the person’s face.<sup>5</sup> Regardless of whether the information is reduced to ones and zeros, pixels, histograms, or to a lower dimension vector through principal component analysis, the starting point FER is the configuration or arrangement of certain facial characteristics – i.e., the person’s face geometry.

27. In some instances, when the user’s face is not fully visible while taking the picture, the App will flash a message on the screen stating: “who goes there?” or “Umm, anybody here?”

---

<sup>4</sup> <https://ietresearch.onlinelibrary.wiley.com/doi/10.1049/iet-ipr.2018.6647>

<sup>5</sup> *Id.*

<https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3715259/#:~:text=Geometry%2Dbased%20features%20describe%20the,the%20face%2C%20caused%20by%20expression.>

or “Your friends will definitely prefer to see your face!” These messages show that the App uses facial detection software, which can be the first step of FER.<sup>6</sup> Otherwise, the App would have no ability to determine whether a user was present or absent from the picture.

28. There are various methods for facial detection. All those methods also compare features, points, the shape, or segments of a person’s face in reference to the arrangement or configuration of other features, points, shapes, or segments to a person’s face – i.e., the person’s face geometry.

29. Defendant contends that the App uses software that collects the biometric face geometry scans on each user’s device and that the biometric information is not sent back to BeReal’s own server. However, even if that contention is true, BeReal completely controls the biometric information it obtains from Plaintiff and other users because the users are not informed that their biometrics are being collected.

30. Whether or not the biometric information remains solely on a user’s phone, no user has any knowledge that this sensitive information has been obtained and sits on their phone. Since they have no knowledge that their phone now obtains their biometrics, users cannot delete the App due to such a concern.

31. If a user’s phone is hacked or lost, then the biometric information surreptitiously collected on the phone puts the Plaintiff at risk. If a user, believing nothing important is stored on the phone, allows someone else to hold their phone or to use it, then the biometrics surreptitiously obtained on the phone puts the Plaintiff at risk.

32. Just like a person carrying a copy of their social security card in their wallet is at risk of theft or loss of such important personal information, users of the App are carrying around

---

<sup>6</sup> *Id.*



their biometrics in their phones and are at risk. One key difference is that a person can choose not to carry around their social security card. Defendant's users don't even know that they are exposing themselves.

33. Without the disclosure, only Defendant controls Plaintiff's and other users' biometric information.

34. Moreover, Defendant's contention that the App uses software that collects the biometric face geometry on each user's device without sharing the information with the BeReal server was only supported by a reference and a description of a certain program available for developers of apps for Apple products. Defendant contends that the App uses the program. While Defendant has control of the biometrics, as the only entity that is informed of their collection in the first place, the use of the program does not show that Defendant does not receive the biometrics on its own servers.

35. The program merely allows a device to recognize facial characteristics, but says nothing about whether the biometric information collected remains on the device subsequent to its collection. The BeReal Terms state that Defendant receives photos, geolocation, data about the number of times a photo is taken, and "event logs." This information is also initially obtained by a user's phone and then apparently sent to BeReal. It is not clear whether Defendant treats the biometric facial geometry data collected by the App as part of the photo itself, saved as a jpeg file, or as part of the other data Defendant receives. It is also not clear whether the App uses the similar program on its Android phones to keep biometric information processing on the device. Finally, even if Defendant is not currently transmitting the biometric information from users' devices to its own servers, it has the ability to make such transmission happen.

### **III. Defendant Violates Illinois' Biometric Information Privacy Act**

36. Unbeknown to the average person, and in direct violation of § 15(b)(1) of BIPA, Defendant collects, captures, or otherwise obtains people's biometric identifiers – all without ever informing anyone of this practice in writing.

37. In direct violation of §§ 15(b)(2) and 15(b)(3) of BIPA, from 2022 or earlier to at least the present, Defendant never informed Illinois users who had their face geometry obtained of the specific purpose and length of term for which their biometric identifiers or information would be obtained and used, nor did Defendant obtain a written release from these individuals.

38. In direct violation of § 15(a) of BIPA, from 2022 or earlier to at least the present, Defendant did not have written, publicly available policies identifying their retention schedules, or guidelines for permanently destroying any of these biometric identifiers or biometric information.

### **III. Plaintiff Jain's Experience**

39. Plaintiff started using the App in or about July 2022.

40. During the course of Plaintiff's registration in the App, the App instructed Plaintiff to provide his name, birthdate, and phone number. Plaintiff provided this information.

41. During the course of Plaintiff's use of the App, he took multiple pictures of his face. In some instances, when he smiled, the App flashed him messages stating: "Bonus point for the smile!" or "Keep smiling and don't change a thing." or "Aye what a smile." In some instances, when he was not fully positioned in the picture, the App stated: "who goes there?" or "Umm, anybody here?" or "Your friends will definitely prefer to see your face!"

42. The App's messages described above demonstrate that the App was capturing Plaintiff's biometric identifier through its use of FER and face detection.

43. Plaintiff never consented, agreed, or gave permission – written or otherwise – to Defendant for the obtaining or storage of his unique biometric identifiers or biometric information.

44. Further, Defendant never provided Plaintiff with, nor did he ever sign, a written release allowing Defendant to obtain or store his unique biometric identifiers or biometric information.

45. Likewise, Defendant never provided Plaintiff with the requisite statutory disclosures nor an opportunity to prohibit or prevent the collection, obtaining, storage or use of his unique biometric identifiers or biometric information.

46. By obtaining Plaintiff's unique biometric identifiers or biometric information without his consent, written or otherwise, Defendant invaded Plaintiff's statutorily protected right to privacy in his biometrics.

47. Finally, Defendant never provided Plaintiff with a retention schedule and/or guideline for permanently destroying his biometric identifiers and biometric information.

### **CLASS ALLEGATIONS**

48. **Class Definition:** Plaintiff brings this action pursuant to 735 ILCS 5/2-801 on behalf of a class of similarly situated individuals, defined as follows (the "Class"):

All individuals who, while residing in the State of Illinois, had their face geometry collected, captured, received, or otherwise obtained, and/or stored, by Defendant.

49. **Numerosity:** Pursuant to 735 ILCS 5/2-801 (1), the number of persons within the Class is substantial, believed to amount to at least thousands of persons. It is, therefore, impractical to join each member of the Class as a named Plaintiff. 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.

50. **Commonality and Predominance:** Pursuant to 735 ILCS 5/2-801(2), there are well-defined common questions of fact and law that exist as to all members of the Class and that predominate over any questions affecting only individual members of the Class. These common legal and factual questions, which do not vary from Class member to Class member, and which may be determined without reference to the individual circumstances of any Class member, include, but are not limited to, the following:

- (a) whether Defendant collected or otherwise obtained Plaintiff's and the Class' biometric identifiers or biometric information;
- (b) whether Defendant properly informed Plaintiff and the Class that it collected, used, otherwise obtained, and stored their biometric identifiers or biometric information;
- (c) whether Defendant obtained a written release (as defined in 740 ILCS 1410) to collect, use, otherwise obtain, and store Plaintiff's and the Class' biometric identifiers or biometric information;
- (d) 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 3 years of their last interaction, whichever occurs first;
- (e) whether Defendant used Plaintiff's and the Class' biometric identifiers or biometric information to identify them; and
- (f) whether Defendant's violations of BIPA were committed intentionally, recklessly, or negligently.

51. **Adequate Representation:** Pursuant to 735 ILCS 5/2-801 (3), Plaintiff has retained and is represented by qualified and competent counsel who are highly experienced in complex consumer class action litigation, including class action litigation under BIPA. Plaintiff

and his counsel are committed to vigorously prosecuting this class action. Moreover, Plaintiff is able to fairly and adequately represent and protect the interests of the Class. Neither Plaintiff nor his counsel has any interest adverse to, or in conflict with, the interests of the absent members of the Class. Plaintiff has raised viable statutory claims or the type reasonably expected to be raised by members of the Class, and will vigorously pursue those claims. If necessary, Plaintiff 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, or to amend the Class definition to address any steps that Defendant took in 2018.

52. **Superiority:** Pursuant to 735 ILCS 5/2-801(4), 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. Even if every member of the Class could afford to pursue individual litigation, the Court system could not. It would be unduly burdensome to the courts in which individual litigation of numerous cases would proceed. Individualized litigation would also present the potential for varying, inconsistent or contradictory judgments, and 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. Plaintiff anticipates no difficulty in the management of this action as a class action. Class-wide relief is essential to compliance with BIPA.

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

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

54. 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).

55. Defendant failed to comply with these BIPA mandates.

56. Defendant is a private company and thus qualifies as a “private entity” under BIPA. See 740 ILCS 14/10.

57. Plaintiff is an individual who had his “biometric identifiers” captured, collected, and/or otherwise obtained by Defendant, as explained in detail above. See 740 ILCS 14/10.

58. Plaintiff’s biometric identifiers are connected with his name and phone number and, therefore, could also constitute “biometric information” as defined by BIPA. See 740 ILCS 14/10.

59. 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).

60. Upon information and belief, Defendant lacked retention schedules and guidelines for permanently destroying Plaintiff’s and the Class’s biometric data and have 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.

61. On behalf of himself 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 each Defendant to comply with BIPA's requirements for the collection, capture, storage, otherwise obtaining, 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).

**PRAYER FOR RELIEF**

WHEREFORE, Plaintiff Jain, on behalf of himself and the proposed Class, with respect to this Count, 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 as representative of the Class, and appointing his counsel as Class Counsel;

B. Declaring that Defendant's actions, as set out above, violate BIPA, 740 ILCS 14/1, *et seq.*;

C. Awarding statutory damages of \$5,000.00 for each and every intentional and/or reckless violation of BIPA pursuant to 740 ILCS 14/20(2), or alternatively, statutory damages of \$1,000.00 for each and every violation pursuant to 740 ILCS 14/20(1) if the Court finds that Defendant's violations were negligent;

D. Awarding injunctive and other equitable relief as is necessary to protect the interests of the Class, including, *inter alia*, an Order requiring Defendant to collect, store, otherwise obtain, and use biometric identifiers and/or biometric information in compliance with BIPA;

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

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

G. Entering judgment in favor of Plaintiff and the Class and against Defendant, awarding the relief set forth in this Prayer for Relief; and

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

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

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

63. BIPA requires companies to obtain informed written consent from users 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).

64. Defendant failed to comply with these BIPA mandates.

65. Defendant is a private company and thus qualifies as a “private entity” under BIPA. *See* 740 ILCS 14/10.

66. Plaintiff and the Class are individuals who have had their “biometric identifiers” collected, captured, and/or otherwise obtained by Defendant, as explained in detail above. *See* 740 ILCS 14/10.



67. Plaintiff's and the Class's biometric identifiers are connected with their names and phone numbers and therefore could also constitute "biometric information" as defined by BIPA. *See* 740 ILCS 14/10.

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

69. Defendant never informed Plaintiff, and never informed any member of the Class at least prior to February 2018, in writing that their biometric identifiers and/or biometric information were being collected, captured, otherwise obtained, stored, and/or used, nor did Defendant inform Plaintiff and the Class in writing of the specific purpose(s) and length of term for which their biometric identifiers and/or biometric information were being collected, captured, otherwise obtained, stored, used and disseminated as required by 740 ILCS 14/15(b)(1)-(2).

70. By collecting, capturing, storing, otherwise obtaining, and/or 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 and/or biometric information as set forth in BIPA. *See* 740 ILCS 14/1, *et seq.*

71. On behalf of himself 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, captures, storage, use, otherwise obtaining, and dissemination of biometric identifiers and biometric information as described herein; (3) statutory damages of \$5,000 for each intentional and/or reckless violation of BIPA pursuant to 740 ILCS 14/20(2) or, in the alternative, statutory damages of \$1,000 for each

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

**PRAYER FOR RELIEF**

WHEREFORE, Plaintiff Jain, on behalf of himself and the proposed Class, with respect to this Court, 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 as representative of the Class, and appointing his counsel as Class Counsel;

B. Declaring that Defendant's actions, as set out above, violate BIPA, 740 ILCS 14/1, *et seq.*;

C. Awarding statutory damages of \$5,000.00 for each and every intentional and/or reckless violation of BIPA pursuant to 740 ILCS 14/20(2), or alternatively, statutory damages of \$1,000.00 for each and every violation pursuant to 740 ILCS 14/20(1) if the Court finds that Defendant's violations were negligent;

D. Awarding injunctive and other equitable relief as is necessary to protect the interests of the Class, including, *inter alia*, an Order requiring Defendant to collect, store, otherwise obtain, and use biometric identifiers and/or biometric information in compliance with BIPA;

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

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

G. Entering judgment in favor of Plaintiff and the Class and against Defendant, awarding the relief set forth in this Prayer for Relief; and

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

Dated: July 26, 2023

Respectfully submitted,

/s/ Gary M. Klinger

Gary M. Klinger (ARDC# 6303726)  
**MILBERG COLEMAN BRYSON  
PHILLIPS GROSSMAN PLLC**  
227 West Monroe Street, Suite 2100  
Chicago, IL 60606  
Telephone: 866.252.0878  
gklinger@milberg.com

Daniel R. Johnson (ARDC# 6283164)  
Adam Waskowski (#6284221)  
**WASKOWSKI JOHNSON  
YOHALEM LLP**  
954 W. Washington Blvd., Suite 322  
Chicago, Illinois 60607  
(312) 278-3153  
djohnson@wjylegal.com  
awaskowski@wjylegal.com

*Attorneys for the Plaintiff and the  
Proposed Class*

# ClassAction.org

This complaint is part of ClassAction.org's searchable class action lawsuit database and can be found in this post: [BeReal App Collected Illinois Users' Biometric Data Without Consent, Class Action Says](#)

---