

1 Michael Ram (SBN 104805)
mram@forthepeople.com
2 **MORGAN & MORGAN**
COMPLEX LITIGATION GROUP
3 711 Van Ness Ave, Suite 500
San Francisco, CA 94102
4 Tel: (415) 846-3862

5 Andrew R. Frisch (*Pro hac vice forthcoming*)
afrisch@forthepeople.com
6 **MORGAN & MORGAN, P.A.**
8151 Peters Road, 4th Floor
7 Plantation, Florida 33324
Tel: (954)327-5355

8 Jordan Richards (*Pro hac vice forthcoming*)
9 Jordan@jordanrichardspllc.com
JORDAN RICHARDS, PLLC
10 1800 SE 10th Ave. Suite 205
Fort Lauderdale, Florida 33316
11 Tel: (954) 871-0050

12 *Counsel for Plaintiff and the Proposed Class*

13 IN THE UNITED STATES DISTRICT COURT

14 NORTHERN DISTRICT OF CALIFORNIA

15 KEESHA STEPTOUR, individually, and on)
behalf of all others similarly situated,)

16 Plaintiff,)

17 v.)

18 ANVIZ GLOBAL, INC. a California)
corporation.,)

19 Defendant.)
20)
21)

CASE NO.

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

1 Plaintiff, Keesha Steptour (hereinafter “Plaintiff”), brings this class action under Rule 23
2 of the Federal Rules of Civil Procedure against ANVIZ GLOBAL, INC. (“Anviz Global” or
3 “Defendant”) for its violations of the Illinois Biometric Information Privacy Act, 740 ILCS § 14/1
4 (hereinafter “BIPA”). In support, Plaintiff alleges as follows:

5 **INTRODUCTION**

6 1. Plaintiff brings this class action for damages and other legal and equitable remedy
7 resulting from the illegal actions of Defendant in collecting, obtaining, storing and/or using
8 Plaintiff’s, and other similarly situated individuals’ biometric identifiers and biometric information
9 (referred to collectively as “biometrics”) without informed written consent in violation of the
10 Illinois Biometric Information Privacy Act (“BIPA”).

11 2. The Illinois Legislature has determined that “[b]iometrics are unlike any other
12 unique identifiers that are used to access finances or other sensitive information.” 740 ILCS 14/5L.
13 “For example, social security numbers, when compromised, can be changed. Biometrics,
14 however, are biologically unique to the individual; therefore, once compromised, the individual
15 has no recourse, is at heightened risk for identity theft, and is likely to withdraw from biometric-
16 facilitated transactions.” *Id.* In recognition of these concerns over the security of individuals’
17 biometrics, the Illinois Legislature enacted BIPA.

18 3. “Biometrics” refers to technologies used to identify an individual based on unique
19 physical characteristics. Common biometric identifiers include fingerprints, hand or face geometry
20 scans, retina or iris scans, or voice scans, which are all generally obtained by first acquiring an
21 image or photograph of the biometric identifier.

22 4. Unlike other identifiers like Social Security or credit card numbers, which can be
23 changed if compromised or stolen, biometric identifiers linked to a specific finger or hand cannot.
24 These unique and permanent biometric identifiers, once exposed, leave victims with no means to
25 prevent identify theft and unauthorized tracking.

26 5. As expressed herein, BIPA is the result of an expressed fundamental public policy
27 and legislative intent in Illinois to regulate the collection of biometric information. BIPA provides,
28 inter alia, that private entities like Defendant may not collect, capture, purchase, receive through

1 trade, or otherwise obtain an individual's biometrics unless it: (1) informs that person in writing
2 that biometric identifiers or information will be collected or stored; (2) informs that person in
3 writing of the specific purpose and length of term for which such biometric identifiers or biometric
4 information is being collected, stored and used; (3) receives a written release from the person for
5 the collection of his or her biometric identifiers or information; and (4) publishes publicly available
6 written retention schedules and guidelines for permanently destroying biometric identifiers and
7 biometric information, *see* 740 ILCS 14/15(a) and (b).

8 6. In direct violation of each of the foregoing provisions of Section 15(a) of BIPA,
9 Defendant failed to provide, publish, or otherwise make publicly available data retention policies.

10 7. In direct violation of the foregoing provisions of Section 15(b) of BIPA, Defendant
11 actively collected, stored, obtained, and used the biometrics of Illinois residents, including
12 Plaintiff, without providing notice, or obtaining informed written consent.

13 8. Specifically, during the relevant time period, Plaintiff and other similarly situated
14 individuals in Illinois were required to scan their faces on Defendant's biometric facial imaging
15 devices to keep track of the amount of time Plaintiffs were working for Defendant's customers.

16 9. Plaintiff brings this action on behalf of herself and a class of similarly situated
17 individuals to prevent Defendant from further violating privacy rights and to recover statutory
18 damages for Defendant's unauthorized collection, storage and use of Plaintiff's biometrics in
19 violation of BIPA.

20 **PARTIES, JURISDICTION & VENUE**

21 10. Plaintiff is and has been at all relevant times, a resident and citizen of the State of
22 Illinois. Plaintiff was employed by a third-party, All Fleet, who utilized Defendant's biometric
23 timekeeping devices during one or more workweeks when she worked as a dispatcher for her
24 employer. Plaintiff worked for third-party, All Fleet, in Zion, Illinois, from approximately
25 February 2022 to January 2023. Plaintiff was required to use her facial images to clock-in and
26 clock-out of work to perform her duties daily within the five (5) year period prior to the filing of
27 this Complaint. Plaintiff never consented, agreed or gave permission – written or otherwise – to
28 this Defendant for the collection or storage of the biometric identifiers or biometric information

1 associated with her facial images. Further, this Defendant never provided Plaintiff, nor did she
2 ever sign a written release allowing this Defendant to collect or store the biometric identifiers or
3 biometric information associated with their facial images. Plaintiff consents to the Court's
4 jurisdiction.

5 11. Defendant is a California corporation, with its registered agent, Lingling Qian,
6 located at 32920 Alvarado-Niles Road #220 in Union City, California 94587. Defendant, while
7 headquartered in California, engages in continuous business in Illinois and operates with Illinois
8 companies by storing Illinois residents' biometric information in its database, and sends its
9 biometric devices into the State of Illinois, and is subject to the laws of Illinois, including BIPA.
10 Defendant owns, operates, and/or controls several biometric devices which it has delivered to the
11 State of Illinois which collected the biometric information of hundreds (if not thousands) of
12 individuals in the State of Illinois within the past 5 years. Defendant may be served through its
13 registered agent, Lingling Qian at 32920 Alvarado-Niles Road #220 in Union City, California
14 94587.

15 12. This Court has subject matter jurisdiction over this matter pursuant to 28 U.S.C. §
16 1332(a) because there is complete diversity of citizenship between Plaintiff and Defendant and the
17 amount in controversy exceeds \$75,000.00.

18 13. This Court also has subject matter jurisdiction over this matter pursuant to the Class
19 Action Fairness Act ("CAFA"), 28 U.S.C. § 1332(d)(2), because this is a class action in which the
20 Defendant is a citizen of a state different than Plaintiff and the other class members, and because
21 the amount in controversy exceeds \$5,000,000.00.

22 14. No applicable statutory exception to jurisdiction exists.

23 15. This Court has personal jurisdiction over Defendant named in this action because
24 Defendant is a California corporation operating in California and Defendant maintains a place of
25 business in California. Defendant collected the biometric information of Illinois residents in
26 Illinois, and stored this information in a database over which it asserts and maintains control.
27 Defendant engages in continuous and systematic business operations or activities within California
28 and maintains a location in the State, including within Union City, within this judicial circuit.

1 16. Venue is proper in this Court because Defendant maintains its place of business
2 within this County, transacts substantial business within this County, and the events giving rise to
3 this lawsuit occurred in substantial part within this County.

4 **ANVIZ GLOBAL'S BIOMETRIC DEVICES**

5 17. Defendant advertises itself as a world leading provider of biometrics, video
6 surveillance, intelligent smart homes, and smart building solutions. See www.anviz.com (last
7 visited April 19, 2024).

8 18. To help make employee time and attendance tracking more accurate, Defendant
9 advertises on its website to encourage its customers to use its biometric-based time clocks, which
10 use an employee's biometric identifiers and biometric information to punch in and out of work,
11 instead of key fobs, identification numbers, or swipe cards.

12 19. One of Defendant's biometric timekeeping products that it offers to clients is the
13 Face Deep Series.

14 20. Defendant designed its Face Deep Series with a "Smart Face Recognition
15 Terminal" so that employers could utilize its biometric verification function for time and
16 attendance tracking which integrates with cloud software for reduced management costs.

17 21. More specifically, Defendant has created a unique BioNANO algorithm which
18 relies upon facial geometric characteristics from users to create a database template of a known
19 user and then compares subsequent information scanned with the database to find a match.

20 22. Defendant's own advertising brochures available for download on its website state
21 that the Anviz Global Face Deep Series is powered by Anviz Facial Biometric Technology which
22 utilizes the BioNANO algorithm:

23 //

24 //

25 //

26 //

27 //

28 //

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

Features



High-Speed CPU

A High-performance Linux CPU implementing a face-capturing of fewer than 0.3 seconds provide an efficient workplace.

BioNANO®

Anviz Facial Biometric Technology

Powered by Anviz the facial biometric BioNANO® algorithm and AI deep learning technology, FaceDeep 3 Series offers the best matching speed, accuracy, and level of security, even while wearing a mask.



Intuitive UI

Its 5-inch TFT, 720*1280 high-resolution touch screen provides a dynamic user experience. The easy-to-use, graphics-based navigation allows users to exploit the maximal capabilities of the FaceDeep 3 Series.



Extensive Interfaces

It allows flexible system design with extensive communication interfaces such as WiFi, TCP/IP and RS485. In addition, it provides Exit Button, Wiegand Output & Input, and Relay Outputs to offer any applications flexibility.



Confidence in All Environments

Anviz's Dual Camera technology enables IR and visual face recognition, and automatically adapts LED lights based on ambient lighting conditions for enhanced capturing in different environments, even in complete darkness.



Employee Health Screening

FaceDeep 3 Series IRT version supports temperature measuring and cost advantages with the most economical temperature detection option to fit any budget of a business.

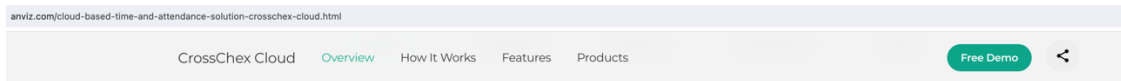
See anziv.com/download/2697.html (last visited April 23, 2024).

23. When the Face Deep Series captures a user's biometric information from facial scans in Illinois, it stores the template on the CrossChex Cloud system which is controlled by Defendant and used to identify the individuals who are clocking in and clocking out.

24. Anviz Global operates and controls its proprietary CrossChex Cloud system which is compatible and used with all Anviz Global time and attendance devices.

25. According to Anviz Global's own website, one of the features provided by the CrossChex Cloud system is "biometrics":

//
//
//
//
//
//
//
//
//
//
//
//
//
//
//
//
//
//
//
//
//



Innovative Features

		Current Version	Next-Gen
System	Multi-Location	✓	✓
	Multi-level Administrator & Supervisor	✓	✓
	Activity Dashboard	✓	✓
	Attendance Management	✓	✓
	Shift Scheduling	✓	✓
	Group Scheduling	-	✓
	Time Tracking	✓	✓
	Approval Process Control	-	✓
	Biometrics	✓	✓
	Body Temperature & Mask Detection	✓	✓

See anviz.com/cloud-based-time-and-attendance-solution-crosschex-cloud.html (last visited April 23, 2024).

26. In light of the biometric features provided on its devices, Defendant markets its biometric devices to employers in Illinois as superior options to traditional time clocks. By marketing its biometric devices in this manner, Anviz Global obtains competitive advantage over other time clock companies and secures profits from its use of biometric data, all while failing to comply with the minimum requirements for handling employees’ biometric data established by BIPA to protect Illinois residents.

27. Unlike key fobs, identification numbers, or swipe cards – which can be changed or replaced if stolen or compromised – facial imaging biometrics are unique, permanent biometric identifiers associated with each employee. This exposes employees who are required to use an Anviz Global device as a condition of their employment to serious and irreversible privacy risks.

28. In fact, Defendant advertises the Face Deep Series biometric devices it sells and/or leases to Illinois businesses as each being capable of storing biometric information from up to 50,000 different users.

1 29. During the relevant time period, Anviz Global sent one or more biometric devices
2 into the State of Illinois with the knowledge that its device would be capturing, obtaining, using,
3 and/or collecting biometric information from Illinois residents.

4 30. For example, Anviz Global sent a Face Deep Series device to All Fleet in Illinois
5 within the past 5 years with the knowledge that the Face Deep Series would collect and maintain
6 biometric information from its users' facial scans.

7 31. When an employee first begins work at an Illinois company that uses one of Anviz
8 Global's biometric devices, the employee is required to have their face scanned into the Anviz
9 Global biometric device in order to create a template and enroll them in the Anviz Global database.

10 32. Defendant then stores the biometric information and/or identifiers of Illinois
11 residents in its database so that Illinois employers can access the biometric information to use this
12 information for timekeeping, payroll, and attendance confirmation.

13 33. When an Illinois resident employed by a company in Illinois scans its biometric
14 information into an Anviz Global biometric device the Defendant becomes aware that it is in the
15 possession of Illinois residents' biometric information.

16 34. Anviz Global maintains control over the biometric information it collects from
17 individuals who use the Face Deep Series device and other biometric devices.

18 **PLAINTIFF'S BIOMETRIC INFORMATION**

19 35. Plaintiff was employed by All Fleet in Zion, Illinois from approximately February
20 2022, through January 11, 2023.

21 36. As a condition of her employment Plaintiff was required to scan her face on an
22 Anviz Global Face Deep Series biometric device to clock-in and clock-out of work.

23 37. Plaintiff was first required to scan her face on the Anviz Global biometric device
24 so that her biometric information could be kept in Defendant's database and thereafter use the
25 device's BioNANO algorithm to identify Plaintiff each and every time she scanned on the device
26 to clock-in and clock-out.

27 38. Plaintiff scanned her face on the Anviz Global biometric device while she was
28 physically present and working in the State of Illinois.

39. Defendant’s Quick Guide for the Face Deep 3 Smart Face Recognition Terminal provides an overview on User Enrollment for how users are to scan their faces on the device, which includes instructions to: (a) keep the face in the center of the detection frame, according to the device request; (b) slightly move head left and right, up and down during the registration; (c) remove glasses if the detection frame is triggered by the eyewear:

User Enrollment

The diagram illustrates the 'Quick Face Registration' process. It starts with a 'Main' menu containing 'Enroll', 'User', 'Data', 'Network', 'Setting', and 'Advance'. An arrow points to a 'Register Face' screen where an ID is entered. This leads to a sequence of three face registration screens: 1. 'Face in the circle' (Step 1), 2. 'Enrolled' (Step 2), and 3. 'Already exist' (indicating a failed attempt). A list of instructions is provided below the registration steps.

Quick Face Registration

1. Register Face (ID input screen)

2. Face in the circle

3. Enrolled

4. Already exist

Main Menu: Enroll, User, Data, Network, Setting, Advance

Instructions:

- Keep face in the center of the detection frame, according to the device request.
- Slightly move head left and right, up and down during the registration.
- If the registration process takes too long or fails, please change the registration position.
- In some cases, the detection frame might move to the top, it might be triggered by glasses. Take the glasses off, and try one again.

40. Defendant thereafter collected and stored Plaintiff’s biometric data in its CrossChex Cloud database(s) immediately after it was captured in the State of Illinois.

41. After registering on the device, Plaintiff was required to scan her face on the Anviz Global device each time she clocked in and out for work including each time she clocked out for a meal break and then clocked back in when returning from a meal break.

42. During her employment period Plaintiff scanned her face on Defendant’s biometric device at least 4 times per day.

1 of a class of similarly situated individuals, defined as follows (hereinafter “the Class”):

2 **All individuals who resided in Illinois within the past 5 years**
3 **who had their biometric identifiers, including “facial images”**
4 **collected, captured, received, used, or otherwise obtained by**
5 **Defendant in the State of Illinois on an Anviz Global biometric**
6 **device.**

7 53. The following are excluded from the Class: (1) any Judge presiding over this action
8 and members of his or her family; (2) persons who properly executed and file a timely request for
9 exclusion from the Class; (3) persons whose claims in this matter have been finally adjudicated on
10 the merits or otherwise released; (4) Plaintiff’s counsel and Defendant’s counsel; and (6) legal
11 representatives, successors, and assigns of any such excluded persons.

12 54. **Numerosity:** The number of persons within the Class is substantial and is believed
13 to amount to hundreds of people. It is, therefore, impractical to join each member of the Class as
14 a named Plaintiff. Further, the size and relatively modest value of the claims of the individual
15 members of the Class renders joinder impractical. Accordingly, utilization of the class action
16 mechanism is the most economically feasible means of determining and adjudicating the merits of
17 this litigation.

18 55. **Commonality and Predominance:** There are well-defined common questions of
19 facts and law that exist as to all members of the Class and that predominate over any questions
20 affecting only individual members of the Class. These common legal and factual questions, which
21 do not vary from Class member to Class member, and which may be determined without reference
22 to the individual circumstances of any class member include, but are not limited to, the following:

23 (a) whether Defendant collected or otherwise obtained Plaintiffs’ and the Class’s
24 biometric identifiers or biometric information;

25 (b) whether Defendant properly informed Plaintiffs and the Class that it collected, used,
26 and stored their biometric identifiers or biometric information;

27 (c) whether Defendant obtained a written release (as defined in 740 ILCS 1410) to
28 collect, use, and store Plaintiffs’ and the Class’s biometric identifiers or biometric information;

1 (d) whether Defendant developed a written policy, made available to the public,
2 establishing a retention schedule and guidelines for permanently destroying biometric identifiers
3 and biometrics information when the initial purpose for collecting or obtaining such identifiers or
4 information has been satisfied or within 3 years of their last interaction, whichever occurs first;

5 (e) whether Defendant used Plaintiffs' and the Class's biometric identifiers or
6 biometric information to identify them; and

7 (f) whether Defendant's violations of the BIPA were committed intentionally,
8 reckless, or negligently.

9 56. **Adequate Representation:** Plaintiff has retained and are represented by qualified
10 and competent counsel who are highly experienced in complex employment class action litigation.
11 Plaintiff and her counsel are committed to vigorously prosecuting this class action. Neither
12 Plaintiff nor her counsel have any interest adverse to, or in conflict with, the interests of the absent
13 members of the Class. Plaintiff is able to fairly and adequately represent and protect the interests
14 of such a Class. Plaintiff has raised viable statutory claims of the type reasonably expected to be
15 raised by members of the Class, and will vigorously pursue those claims. If necessary, Plaintiffs
16 may seek leave of this Court to amend this Class Action Complaint to include additional Class
17 representatives to represent the Class or additional claims as may be appropriate.

18 57. **Superiority:** A class action is superior to other available methods for the fair and
19 efficient adjudication of this controversy because individual litigation of the claims of all Class
20 members is impracticable. Even if every member of the Class could afford to pursue individual
21 litigation, the Court system could not. It would be unduly burdensome to the courts in which
22 individual litigation of numerous cases would proceed. Individualized litigation would also present
23 the potential for varying, inconsistent or contradictory judgments, and would magnify the delay
24 and expense to all parties and to the court system resulting from multiple trials of the same factual
25 issues. By contrast, the maintenance of this action as a class action, with respect to some or all of
26 the issues presented herein, presents few management difficulties, conserves the resources of the
27 parties and of the court system and protects the rights of each member of the Class. Plaintiffs
28

1 anticipate no difficulty in the management of his action as a class action. Class wide relief is
2 essential to compel compliance with the BIPA.

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

5 **(On Behalf of Plaintiff and the Class)**

6
7 58. Plaintiff hereby incorporates the allegations within paragraphs 1-49 as though fully
8 set forth herein.

9 59. Defendant is a California corporation that engages in business in Illinois and sends
10 its biometric devices into Illinois to collect biometric information from Illinois residents, and thus
11 qualifies as a “private entity” under BIPA. *See* 740 ILCS 14/10.

12 60. BIPA mandates that companies in possession of biometric data establish and
13 maintain a satisfactory biometric data retention – and, importantly, deletion – policy. Specifically,
14 those companies must: (i) make publicly available a written policy establishing a retention
15 schedule and guidelines for permanent deletion of biometric data (at most three years after the
16 company’s last interaction with the individual); and (ii) actually adhere to that retention schedule
17 and actually delete the biometric information. *See* 740 ILCS 14/15(a).

18 61. As a private entity covered under BIPA, Defendant failed and continues to fail to
19 comply with these BIPA mandates.

20 62. Plaintiff and members of the putative class are individuals who had their “biometric
21 identifiers” collected by Defendant, as explained in detail above. *See* 740 ILCS 14/10.

22 63. Plaintiff’s and putative class members’ biometric identifiers were used to identify
23 Plaintiffs and, therefore, constitute “biometric information” as defined by BIPA. *See* ILCS 14/10.

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

27 65. Defendant likewise failed to comply or adhere to any such retention schedule or
28 otherwise delete the biometric information it collected as required under BIPA.

1 66. Defendant lacks retention schedules and guidelines for permanently destroying
2 Plaintiffs’ and the Class’s biometric data and have not and will not destroy Plaintiffs’ and the
3 Class’s biometric data when the initial purpose for collecting or obtaining such data has been
4 satisfied or within three years of the individual’s last interaction with the company.

5 67. On behalf of herself and the Class, Plaintiff seeks: (1) declaratory relief; (2)
6 injunctive relief and equitable relief as is necessary to protect the interests of Plaintiff and the Class
7 by requiring Defendant to comply BIPA’s requirements for the collection, storage, and use of
8 biometric identifiers and biometric information as described herein; (3) statutory damages of
9 \$5,000 for each intentional and/or reckless violation of BIPA pursuant to 740 ILCS 14/20(2), or,
10 in the alternative, statutory damages of \$1,000 for each negligent violation of BIPA pursuant to
11 740 ILCS 14/20(1); and (4) reasonable attorney’s fees and costs and other litigation expenses
12 pursuant to 740 ILCS 14/20(3).

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

16 **(On Behalf of Plaintiff and the Class)**

17 68. Plaintiff incorporates the allegations within paragraphs 1-49 as though fully set
18 forth herein.

19 69. Defendant is a California corporation that engages in business in Illinois and sends
20 its biometric devices into Illinois to collect biometric information from Illinois residents, and thus
21 qualifies as a “private entity” under BIPA. *See* 740 ILCS 14/10.

22 70. BIPA requires companies to obtain informed written consent from employees
23 before acquiring their biometric data. Specifically, BIPA makes it unlawful for any private entity
24 to “collect, capture, purchase, receive through trade, or otherwise obtain a person’s or a customer’s
25 biometric identifiers or biometric information unless [the entity] first: (1) informs the subject... in
26 writing that a biometric identifier or biometric information is being collected or stored; (2) informs
27 the subject... in writing of the specific purpose and length of term for which a biometric identifier
28 or biometric information is being collected, stored, and used; and (3) receives a written release

1 executed by the subject of the biometric identifier or biometric information...” *See* 740 ILCS
2 14/15(b).

3 71. Defendant failed and still fails to comply with these BIPA mandates.

4 72. Plaintiff and members of the putative class are individuals who have had their
5 “biometric identifiers” collected by Defendant, as explained in detail above. *See* 740 ILCS 14/10.

6 73. Plaintiff’s and the Class’s biometric identifiers were used to identify them and,
7 therefore, constitutes “biometric information” as defined by BIPA. *See* 740 ILCS 14/10.

8 74. Defendant systematically and automatically collected, used, stored, and
9 disseminated Plaintiff’s and the Class’s biometric identifiers and/or biometric information without
10 first obtaining the written release required by 740 ILCS 14/15(b)(3).

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

16 76. By collecting, storing, using and disseminating Plaintiffs’ and the Class’s biometric
17 identifiers and biometric information as described herein, Defendant violated Plaintiffs’ and the
18 Class’s rights to privacy in their biometric identifiers and/or biometric information as set forth in
19 BIPA. *See* 740 ILCS 14/1, et. seq.

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

28

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, KEESHA STEPTOUR, on behalf of herself and the proposed Class, respectfully requests that this Court enter an Order:

(A) Certifying this case as a class action on behalf of the Class above pursuant to Fed. R. Civ. P. 23, appointing Plaintiff as representative of the class, and appointing Plaintiff’s 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 reckless violation of the BIPA pursuant to 740 ILCS 14/20(2), or alternatively, statutory damages of \$1,000.00 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, and use biometric identifiers or biometric information in compliance with the BIPA;

(E) Awarding Plaintiffs and the Class their reasonable litigation expenses and attorney’s fees;

(F) Awarding Plaintiffs and the Class pre- and post-judgment interest, to the extent allowable; and

(G) Awarding such other and further relief as equity and justice may require.

JURY TRIAL DEMAND

Plaintiff, KEESHA STEPTOUR, demands a trial by jury on all issues so triable on behalf of herself and similarly situated individuals.

DATED: May 1, 2024.

MORGAN & MORGAN, P.A.

By: /s/ Michael Ram

Michael F. Ram (SBN 104805)
MORGAN & MORGAN
COMPLEX LITIGATION GROUP

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

711 Van Ness Ave, Suite 500
San Francisco, CA 94102
mram@forthepeople.com
Tel: (415) 846-3862

Andrew R. Frisch (*Pro hac vice forthcoming*)
MORGAN & MORGAN, P.A.
8151 Peters Road, 4th Floor
Plantation, Florida 33324
afrisch@forthepeople.com
Tel: (954)327-5355

Jordan Richards (*Pro hac vice forthcoming*)
JORDAN RICHARDS, PLLC
1800 SE 10th Ave. Suite 205
Fort Lauderdale, Florida 33316
Jordan@jordanrichardspllc.com
Tel: (954) 871-0050

Counsel for 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: [Anviz Global Illegally Captured Illinois Workers' Facial Scans, Class Action Lawsuit Claims](#)
