IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS, EASTERN DIVISION

FREDY SOSA and ROHITH AMRUTHUR, individually and on behalf of all others similarly situated, *Plaintiffs*, v. ONFIDO, INC., a Delaware corporation, *Defendant*.	Case No.: 20-cv-04247 Honorable Marvin E. Aspen

FIRST AMENDED CLASS ACTION COMPLAINT AND DEMAND FOR JURY TRIAL

Plaintiffs Fredy Sosa and Rohith Amruthur ("Plaintiffs") bring this First Amended Class Action Complaint and Demand for Jury Trial against Defendant Onfido, Inc. ("Onfido") to put a stop to its unlawful collection, use, and storage of Plaintiffs' and putative Class members' sensitive biometric data. Plaintiffs, for this Class Action Complaint, 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.

NATURE OF THE ACTION

1. Defendant Onfido markets and sells biometric software that purports to help businesses identify and register consumers.

2. Onfido's software is becoming increasingly popular in the digital era, as online business often requires consumers to establish their identities by submitting photographs of their driver's licenses or identification cards along with photographs of their faces. Onfido developed proprietary facial recognition software that can be used to scan those uploaded photographs, locate consumers' faces, extract unique biometric identifiers associated with the consumers'

faces, and determine whether the photographs match uploaded identification cards, other photos in its database, the biometric data of known masks, or in some instances, on information and belief, third party and government databases.

3. Businesses can integrate Onfido's software into their own websites so that they can establish a consumer's identity—for example, during a sign up or registration process—without having to send the consumer to another location or webpage. In other words, Onfido's software is designed to be embedded into a business's website in such a way that that consumers will likely be entirely unaware they are interacting with and providing their sensitive information to an unknown, third-party company, Onfido.

4. Utilizing biometric identification software exposes consumers to serious and irreversible privacy risks, especially here where it is not clear to consumers that Onfido is collecting their biometric identifiers.

5. Recognizing the need to protect its citizens from situations like these, Illinois enacted the Biometric Information Privacy Act, 740 ILCS 14/1, *et seq.* ("BIPA"), specifically to regulate companies that collect and store Illinois citizens' biometrics.

6. Despite this law, Onfido disregards consumers' statutorily protected privacy rights and unlawfully collects, stores, and uses, their biometric data in violation of the BIPA. Specifically, Onfido has violated (and continues to violate) the BIPA because it did not:

- Properly inform Plaintiffs and the Class members in writing of the specific purpose and length of time for which their biometric data were being collected, stored, and used, as required by the BIPA;
- Provide and make known to Plaintiffs and the Class members a publicly available retention schedule and guidelines for permanently destroying Plaintiffs' and the Class's biometric data, as required by the BIPA; nor
- Receive a written release from Plaintiffs or the members of the Class to collect, capture, or otherwise obtain their biometric data, as required by the BIPA.

7. Accordingly, this Complaint seeks an Order: (i) declaring that Defendant's conduct violates the BIPA; (ii) requiring Defendant to cease the unlawful activities discussed herein; and (iii) awarding damages to Plaintiffs and the proposed Class.

PARTIES

8. Plaintiff Fredy Sosa is a natural person and citizen of Illinois.

9. Plaintiff Rohith Amruthur is a natural person and citizen of Illinois.

10. Defendant Onfido, Inc. is a Delaware corporation existing under the laws of the State of Delaware with its principal place of business located at 3 Finsbury Avenue, London EC2M 2PA. Onfido does business in this District, the State of Illinois, and across the country.

JURISDICTION AND VENUE

11. This matter was removed from the Circuit Court of Cook County, Illinois. (*See* Dkt. 1.)

12. As the removing party, Defendant Onfido asserted that jurisdiction and venue are proper under 28 U.S.C. §§ 1332 and 1441 (*See id.* at 3–9.)

13. This Court has personal jurisdiction over Defendant because, on information and belief, Defendant has contracted with Illinois-based businesses to provide its biometric identification software with the intention and purpose that it would be used to collect biometric data from Illinois residents. Defendant is and has been aware that it is collecting biometric data from Illinois residents, without complying with BIPA, throughout the class period. Additionally, this Court has jurisdiction over Plaintiffs because they are residents of the State of Illinois.

FACTUAL BACKGROUND

I. The Biometric Information Privacy Act.

14. In the early 2000s, major national corporations started using Chicago and other locations in Illinois to test "new [consumer] 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.

15. In late 2007, a biometrics company called Pay By Touch—which provided major retailers throughout the State of Illinois with fingerprint scanners to facilitate consumer transactions—filed for bankruptcy. That bankruptcy was alarming to the Illinois Legislature because suddenly there was a serious risk that millions of fingerprint records—which, are unique biometric identifiers, can be linked to people's sensitive financial and personal data—could now be sold, distributed, or otherwise shared through the bankruptcy proceedings without adequate protections for Illinois citizens. The bankruptcy also highlighted the fact that most consumers who had used that company's biometric scanners were completely unaware that the scanners were not actually transmitting 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.

16. Recognizing the "very serious need [for] protections for the citizens of Illinois when it [came to their] biometric information," Illinois enacted the BIPA in 2008. *See* Illinois House Transcript, 2008 Reg. Sess. No. 276; 740 ILCS 14/5.

17. The 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*:

> (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).

18. Biometric identifiers include retina and iris scans, voiceprints, scans of hand and fingerprints, and—most importantly here—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. *See id*.

19. The BIPA also establishes standards for how companies in possession of biometric identifiers and biometric information must handle them. *See* 740 ILCS 14/15(c)–(d). For instance, the BIPA 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).

20. Ultimately, the BIPA is simply an informed consent statute. Its narrowly tailored provisions place no absolute bar on the collection, sending, transmitting or communicating of biometric data. For example, the BIPA does not limit what kinds of biometric data may be collected, sent, transmitted, or stored. Nor does the BIPA limit to whom biometric data may be collected, sent, transmitted, or stored. The BIPA simply mandates that entities wishing to engage

in that conduct must make proper disclosures and implement certain reasonable safeguards.

II. Onfido Violates the Biometric Information Privacy Act.

21. By the time the BIPA passed through the Illinois Legislature in mid-2008, many companies who had experimented with using biometric data as an authentication method stopped doing so, at least for a time. That is because Pay By Touch's bankruptcy, described in Section I above, was widely publicized and brought attention to consumers' discomfort with the use of their biometric data.

22. Unfortunately, Onfido failed to address these concerns and it continues to collect, store, and use consumers' biometric data in violation of the BIPA by using facial recognition technology.

23. Onfido provides biometric identification software intended to be seamlessly incorporated into its customers' products and mobile apps, without clear notice to consumers that Onfido is even involved in the process (or how it is involved). According to Onfido's representations to businesses, "[i]dentity verification technology helps establish the legitimate online identity of the people accessing your product or service." Onfido claims that use of its software will "create trust and integrity" in its customer's online communities, and, for businesses first requiring user identification, Onfido's software will "make onboarding a breeze." Indeed, various businesses have partnered with Onfido for this purpose.

24. A consumer establishing his or her identity through Onfido must upload a copy of his or her identification (such as a driver's license, state identification, or a passport) and a photo of his or her face.

25. Onfido uses biometric facial recognition to establish consumers' identities. According to Onfido, "we take a new approach to identity—combining a person's ID with their

physical biometrics … Using advanced facial scanning, Onfido then compares their facial biometrics to the photo on the ID, and generates a score based on the similarity of the faces."

26. Onfido states that its biometric software "extract[s] and compare[s] numerical biometric data from facial images to understand whether two faces are likely to be a match."

27. Onfido also checks whether uploaded facial images show signs of fraud by, for example, comparing a person's numerical biometric data to the biometric data of known masks.

28. Consumers establishing their identities through a mobile app, website, or other software using Onfido's identity software are not made aware that the process relies on biometric technology rather than, for example, a real person conducting the identification process or any other confirmation method.

29. What's worse, Onfido has also created numerous, potentially massive databases of biometric identifiers obtained from consumers. Onfido calls these databases "Known Faces." The Known Faces database allows Onfido's customers to compare a consumer's identity against an individual already in its database and flag consumers who have already been identified:

> The Known Faces report compares a specific applicant's likeness in their most recent live photo to live photos from all applicants in your Onfido account database. It alerts you to faces which have already been through your identity verification flow, so you can catch repeat identity fraud attempts, and help confused users who may have forgotten they already registered with you to recover their accounts.

30. As such, the biometric templates obtained by Onfido may be compared against hundreds or even thousands of other templates as part of the identification process.

31. Although Onfido is well aware of Illinois consumers' privacy rights under BIPA—stating on its website that "[c]onsent and transparency must be paramount concerns" when collecting consumers' biometric identifiers—it failed to inform consumers of the complete purposes for which it collects their sensitive biometric data or to whom the data is disclosed, if at

all.

32. Onfido similarly failed to provide consumers with a written, publicly available policy identifying its retention schedule, and guidelines for permanently destroying consumers' facial geometries when the initial purpose for collecting or obtaining their facial geometries is no longer relevant, as required by the BIPA. A consumer who established his or her identity through Onfido does so without any knowledge of when his or her biometric identifiers will be removed from Onfido's databases—or if they ever will be.

33. The Pay By Touch bankruptcy that catalyzed the passage of the BIPA highlights why conduct such as Onfido's—where the consumers upload their photos but are not aware of the full extent of the reasons they are doing so, nor are they informed who else is receiving this data—is so dangerous. That bankruptcy spurred Illinois citizens and legislators to reach a critical conclusion: it is crucial for people to understand that (1) they are providing biometric data in the first place; (2) who exactly is collecting it; (3) who it will be transmitted to; (4) for what purposes; and (5) for how long it will be kept. But Onfido disregards these obligations, and instead unlawfully collects, stores, and uses consumer's biometric identifiers and information without proper consent.

34. Ultimately, Onfido's conduct disregards consumers' statutorily protected privacy rights in violation of the BIPA.

FACTS SPECIFIC TO PLAINTIFF SOSA

35. Plaintiff Fredy Sosa is a member of an online marketplace where consumers buy and sell goods. In order to increase one's reputation and trustworthiness in the online marketplace, consumers are strongly encouraged to register their identities.

36. For this purpose, the online marketplace partnered up with Onfido to establish its

users' identities.

37. On or around April 2020, Plaintiff Sosa established his identity through the online marketplace's mobile application by uploading a photograph of his driver's license and a photograph of his face. Onfido subsequently used biometric identification technology to extract his biometric identifiers and compare the two photographs.

38. Onfido did not inform Plaintiff Sosa that it would collect, store, or use his biometric identifiers derived from his face. In fact, there was almost no notice whatsoever that Onfido is even involved in the process.

39. In addition, Onfido never informed Plaintiff Sosa of any biometric data retention policy it developed, nor whether it will ever permanently delete the biometric identifiers derived from his face.

40. Plaintiff Sosa never signed a written release allowing Onfido to collect, use, or store his biometric identifiers derived from his face.

41. Plaintiff Sosa has, therefore, been exposed to the risks and harmful conditions created by Onfido's violations of the BIPA alleged herein.

42. Plaintiff Sosa seeks damages under BIPA as compensation for the injuries Onfido has caused.

FACTS SPECIFIC TO PLAINTIFF AMRUTHUR

43. Plaintiff Rohith Amruthur downloaded to his smartphone and used a financial services app operated by a customer of Onfido. Specifically, Onfido provides identity verification software to the customer's app so that the customer can establish its users' identities.

44. In or around 2019, Plaintiff Amruthur established his identity through the financial services mobile app by uploading a photograph of his driver's license and a photograph

of his face. Onfido subsequently used biometric identification technology to extract his biometric identifiers and compare the two photographs.

45. Onfido did not inform Plaintiff Amruthur that it would collect, store, or use his biometric identifiers derived from his face. In fact, there was almost no notice whatsoever that Onfido is even involved in the process.

46. In addition, Onfido never informed Plaintiff Amruthur of any biometric data retention policy it developed, nor whether it will ever permanently delete the biometric identifiers derived from his face.

47. Plaintiff Amruthur never signed a written release allowing Onfido to collect, use, or store his biometric identifiers derived from his face.

48. Plaintiff Amruthur has, therefore, been exposed to the risks and harmful conditions created by Onfido's violations of the BIPA alleged herein.

49. Plaintiff Amruthur seeks damages under BIPA as compensation for the injuries Onfido has caused.

CLASS ALLEGATIONS

50. **Class Definitions**: Plaintiffs Fredy Sosa and Rohith Amruthur bring this action pursuant to Federal Rule of Civil Procedure 23 on behalf of themselves and two classes of similarly situated individuals (collectively, the "Classes").

51. Plaintiff Amruthur seeks to represent a class defined as: All persons who, while within the State of Illinois, uploaded their photograph(s) and an ID to any application, software, or website operated by an Onfido customer that is a financial institution, and subsequently to Onfido, between June 12, 2015 and the present (the "Financial Institution Class").

52. Plaintiff Sosa seeks to represent a class defined as: All persons who, while within

the State of Illinois, uploaded their photograph(s) and an ID to any application, software, or website operated by a Onfido customer that is not a financial institution, and subsequently to Onfido, between June 12, 2015 and the present (the "Non-Financial Institution Class").

53. The following people are excluded from the Classes: (1) any Judge or Magistrate presiding over this action and members of their families; (2) Defendant, Defendant's subsidiaries, parents, successors, predecessors, and any entity in which the Defendant or its parents have a controlling interest and its current or former officers and directors; (3) persons who properly execute and file a timely request for exclusion from the Classes; (4) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; (5) Plaintiffs' counsel and Defendant's counsel; and (6) the legal representatives, successors, and assigns of any such excluded persons.

54. **Numerosity**: Defendant has collected, captured, received, or otherwise obtained biometric identifiers or biometric information from hundreds of thousands of consumers who fall into the Financial Institution Class and Non-Financial Institution Class, making individual joinder impracticable. Ultimately, the members of the Classes will be easily identified through Defendant's or its customers' records.

55. **Commonality and Predominance**: Common questions of law and fact exist as to all members of the Financial Institution Class and as to all members of the Non-Financial Institution Class, and those questions predominate over questions affecting only individual members of the respective Classes. Common legal and factual questions include, but are not necessarily limited to the following:

a) whether Defendant collected, captured, or otherwise obtained Plaintiffs' and the Classes' biometric identifiers or biometric information;

b) whether Defendant properly informed Plaintiffs and the Classes of its

purposes for collecting, using, and storing their biometric identifiers or biometric information;

c) whether Defendant obtained a written release (as defined in 740 ILCS 14/10) to collect, use, and store Plaintiffs' and the Classes' biometric identifiers or biometric information;

d) whether Defendant has sold, leased, traded, or otherwise profited from Plaintiffs' and the Classes' biometric identifiers or biometric information;

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

f) whether Defendant complies with any such written policy (if one exists); and

g) whether Defendant used Plaintiffs' and the Classes' faceprints or facial geometry to identify them.

56. **Adequate Representation**: Plaintiffs will fairly and adequately represent and protect the interests of their respective Classes and have retained counsel competent and experienced in complex litigation and class actions. Plaintiffs have no interests antagonistic to those of their respective Classes, and Defendant has no defenses unique to either Plaintiff. Plaintiffs and their counsel are committed to vigorously prosecuting this action on behalf of the members of the Classes, and have the financial resources to do so. Neither Plaintiffs nor their counsel have any interest adverse to those of the other members of the Classes.

57. **Superiority**: This class action is appropriate for certification because class proceedings are superior to all other available methods for the fair and efficient adjudication of this controversy and joinder of all members of the Classes is impracticable. The damages suffered by the individual members of the Classes are likely to have been small relative to the burden and expense of individual prosecution of the complex litigation necessitated by Defendant's wrongful conduct. Thus, it would be virtually impossible for the individual

members of the Classes to obtain effective relief from Defendant's misconduct. Even if members of the Classes could sustain such individual litigation, it would not be preferable to a class action because individual litigation would increase the delay and expense to all parties due to the complex legal and factual controversies presented in their Complaint. By contrast, a class action presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court. Economies of time, effort, and expense will be fostered and uniformity of decisions will be ensured.

CAUSE OF ACTION
Violation of 740 ILCS 14/1, *et seq.*
(On Behalf of Plaintiffs and the Classes)

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

59. The BIPA requires companies to obtain informed written consent from individuals before acquiring their biometric data. Specifically, the 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).

60. The BIPA also 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 (*i.e.*, when the

business relationship ends); and (ii) actually adhere to that retention schedule and actually delete the biometric information. *See* 740 ILCS 14/15(a).

61. Unfortunately, Onfido fails to comply with these BIPA mandates.

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

63. Plaintiffs and the Classes are individuals who had their "biometric identifiers" collected by Onfido (in the form of their facial scans), as explained in detail in Section II. *See* 740 ILCS 14/10.

64. Plaintiffs' and the Classes' biometric identifiers or information based on those biometric identifiers were used to identify them, constituting "biometric information" as defined by the BIPA. *See* 740 ILCS 14/10.

65. Onfido violated 740 ILCS 14/15(b)(3) by failing to obtain written releases from Plaintiffs and the Classes before it collected, used, and stored their biometric identifiers and biometric information.

66. Onfido violated 740 ILCS 14/15(b)(1) by failing to inform Plaintiffs and the Classes in writing that their biometric identifiers and biometric information were being collected and stored.

67. Onfido violated 740 ILCS 14/15(b)(2) by failing to inform Plaintiffs and the Classes in writing of the specific purpose and length of term for which their biometric identifiers or biometric information was being collected, stored, and used.

68. Onfido violated 740 ILCS 14/15(a) by failing to establish a publicly-available retention schedule or guideline for permanently destroying consumers' biometric identifiers and biometric information.

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

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

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and the Classes, respectfully request that the Court enter an Order:

A. Certifying this case as a class action on behalf of the Classes defined above, appointing Plaintiff Rohith Amruthur as class representative of the Financial Institution Class, appointing Plaintiff Fredy Sosa as class representative of the Non-Financial Institution Class, and appointing Plaintiffs' counsel as Class Counsel;

B. Declaring that Defendant's actions, as set out above, violate the BIPA;

C. Awarding statutory damages of $5,000 for *each* willful and/or reckless violation of BIPA pursuant to 740 ILCS 14/20(2) or, in the alternative, statutory damages of $1,000 for *each* negligent violation of BIPA pursuant to 740 ILCS 14/20(1);

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

E. Awarding Plaintiffs and the Classes their reasonable litigation expenses and attorneys' fees;

F. Awarding Plaintiffs and the Classes 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

Plaintiffs demand a trial by jury for all issues so triable.

Respectfully submitted,

FREDY SOSA and **ROHITH AMRUTHUR**, individually and on behalf of all others similarly situated,

Dated: March 2, 2023

By: /s/ Schuyler Ufkes
One of Plaintiffs' Attorneys

J. Eli Wade-Scott
ewadescott@edelson.com
Schuyler Ufkes
sufkes@edelson.com
EDELSON PC
350 North LaSalle Street, 14th Floor
Chicago, Illinois 60654
Tel: 312.589.6370
Fax: 312.589.6378