IN THE CIRCUIT COURT OF GRUNDY COUNTY

Mark Yard, Plaintiff, v. OCR Labs Global (USA) Inc., Defendant.	2024LA4 CASE NUMBER **CLASS ACTION COMPLAINT**	JURY TRIAL DEMAND

Plaintiff, Mark Yard ("Plaintiff"), individually and on behalf of other similarly situated individuals, brings this Class Action Complaint and demand for jury trial against Defendant, OCR Labs Global (USA) Inc. ("OCR Labs" or "Defendant"), to put a stop to its unlawful collection, use, and storage of Plaintiff's and putative Class members' sensitive biometric data. Plaintiff, for this Class Action Complaint, alleges as follows upon his own knowledge as to himself and his own acts and experiences and, as to all other matters, upon information and belief.

I. NATURE OF THE ACTION

1. Defendant markets and sells biometric software that purports to help businesses quickly identify and register consumers through biometric identifiers[1] and biometric information[2] (collectively, "Biometric Data").

2. Defendant's software is becoming increasingly popular in the digital era, as online business often requires consumers to verify their identities by submitting photographs of their

[1] A "biometric identifier" includes a retina or iris scan, fingerprint, voiceprint, or scan of hand or "face geometry." 740 ILCS 14/10.

[2] "Biometric information" is any information captured, converted, stored, or shared based on a person's biometric identifier used to identify an individual. *See id.*

driver's licenses or identification cards along with "selfie" photographs of their faces. Defendant 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/or government databases.

3. Defendant's customers can integrate Defendant's software into their own websites or mobile applications so that the customer can verify a consumer's identity—for example, during a sign up or registration process--- without having to send the consumer to Defendant's webpage or another location or webpage for identity verification. Put another way, Defendant's software is designed in a way where consumers are entirely unaware that they are interacting with and providing their sensitive Biometric Data to Defendant. To the consumer, it appears that Defendant's customers are the ones collecting the Biometric Data, when it is actually Defendant. With this set up, Defendant can conceal its identity and business practices from Defendant's customer's consumers who provide their Biometric Data to Defendant under the guise of providing it to Defendant's customers.

4. One of Defendant's customers of such identity verification software is Coinmetro, a online, "app-based" platform wherein individuals can trade Bitcoin and 55 other cryptocurrencies. Coinmetro is not subject to Title V of the federal Gramm-Leach-Bliley Act of 1999.

5. When consumers apply or use Coinmetro, it requires its members or applicants to verify their identify in the manner described above---it looks like the consumer is verifying their identify with Coinmetro, but in reality, Defendant is capturing, converting, storing, and/or sharing

Plaintiff and Class Member's Biometric Data without them even knowing Defendant is involved in the identity verification process.

6. Utilizing biometric identification software, such that Defendant provides to Coinmetro, exposes consumers to serious and irreversible privacy risks, especially here where it is not clear to consumers that Defendant is collecting their biometric identifiers when they apply or use Coinmetro.

7. 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.

8. Despite this law, Defendant disregards consumers' statutorily protected privacy rights and unlawfully collects, stores, and uses, their biometric data in violation of the BIPA in regards to its services for Coinmetro and its other customers in Illinois. Specifically, Defendant has violated (and continues to violate) the BIPA because it did not:

A) Properly inform Plaintiff 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;

B) Provide and make known to Plaintiff and the Class members a publicly available retention schedule and guidelines for permanently destroying Plaintiff's and the Class's biometric data, as required by the BIPA; nor

C) Receive a written release from Plaintiff or the members of the Class to collect, capture, or otherwise obtain their biometric data, as required by the BIPA.

9. Accordingly, this Class Action 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 Plaintiff and the proposed Class.

JURISDICTION AND VENUE

10. This Court has jurisdiction over Defendant pursuant to 735 ILCS § 5/2-209 because Defendant conducts business transactions in Illinois, committed statutory violations in Illinois, and is registered to conduct business in Illinois.

11. Venue is proper in this county under is proper in this county under 735 ILCS 5/2-101 because the transaction or some part thereof out of which these causes of action arose occurred in Grundy County, Illinois.

PARTIES

12. Plaintiff is a natural person and citizen of Illinois.

13. Defendant OCR Labs Technologies, Inc. is a Delaware corporation that conducts business throughout Illinois, including in Grundy County, Illinois.

FACTUAL BACKGROUND

I. Illinois' 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 biometric 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. 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. To protect this highly sensitive biometric information, BIPA imposes several requirements on companies relating to biometrics.

17. The BIPA is an informed consent statute, and under BIPA, before obtaining an individual's Biometric Data, a private entity must comply with the statute's notice and consent provisions. Specifically, BIPA makes it unlawful for a private entity to "collect, capture, purchase, receive through trade, or otherwise obtain a person's or a consumer'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."

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. Defendant Violates the Biometric Information Privacy Act With Applicants and Users of Coinmetro and Other Customers

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, Defendant failed to address these concerns for a company it provides services for—Coinmetro--and it continues to collect, store, and use consumers' biometric data in violation of the BIPA by using facial recognition technology.

23. Defendant provides biometric identification software intended to be seamlessly incorporated into Coinmetro's products and mobile apps, without clear notice to Coinmetro's consumers that Defendant is even involved in the process (or how it is involved).

24. A consumer establishing his or her identity through Defendant 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 via a "selfie."

25. Defendant uses biometric facial recognition to verify Coinmetro's consumers' identities. Defendant's website explains how it does this.

26. Coinmetro's consumers or applicants are never informed by Defendant or Coinmetro that Defendant is involved in the Biometric Data verification process at all.

27. Upon information and belief, Defendant's BIPA violations are not limited to just applicants and users of Coinmetro, it occurs for all applicants and users of Defendant's customers.

28. There are several companies that properly disclose their involvement in the biometric verification of identities in the exact same scenario that Defendant provides for Coinmetro.

29. Although Defendant is well aware of Illinois consumers' privacy rights under BIPA—the truth is that it simply failed to inform its consumers of the complete purpose for which it collects their sensitive biometric data or to whom the data is disclosed, if at all.

30. Defendant similarly failed to provide Coinmetro's 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 BIPA. A Coinmetro consumer (which includes applicants) who established his or her identity through Defendant does so without any knowledge of when his or her biometric identifiers will be removed from Defendant's databases—or if they ever will be.

31. The Pay By Touch bankruptcy that catalyzed the passage of the BIPA highlights why conduct such as Defendant's—where Coinmetro's 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 Defendant disregards these obligations, and instead unlawfully collects, stores, and uses consumer's biometric identifiers and information without proper consent.

32. Ultimately, Defendant's conduct disregards Coinmetro's consumers' statutorily protected privacy rights in violation of the BIPA.

III. Facts Specific to Plaintiff

33. Plaintiff signed up to join Coinmetro in Illinois, and in an effort to eliminate fraudulent or spoofed accounts, Coinmetro partnered up with Defendant to verify its users' identities.

34. In or around January 2024, while Plaintiff was physically in Illinois, Plaintiff established his identity through Coinmetro's mobile application by uploading a photograph of his driver's license and a "selfie" photograph of his face. Defendant subsequently used biometric

identification technology to extract Plaintiff's biometric identifiers and compare the two photographs, which Plaintiff had no idea that Defendant was involved in this.

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

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

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

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

39. Plaintiff seeks damages under BIPA as compensation for the injuries Defendant has caused.

40. Plaintiff did not enter into an arbitration agreement with Defendant.

41. Coinmetro's Terms of Use and Privacy Notice does not contain a hyperlink to Defendant's own terms of use or privacy policy.

42. Coinmetro's Privacy Notice does not disclose that Defendant is involved in the collection of Plaintiff's Biometric Data.

IV. Class Action Allegations

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

> All persons who, while within the State of Illinois, uploaded their photograph(s) and an ID to any application, software, or website, and subsequently to OCR Labs, from January 17, 2019 to the present.
>
> Excluded from the Class are: (i) any judge or magistrate judge presiding over this action and members of their staff, as well as members of their families; (ii) OCR Labs, OCR Labs's predecessors, parents, successors, heirs, assigns, subsidiaries, and any entity in which any OCR Labs has a controlling interest, as well as OCR Labs's current or former employees, agents, officers, and directors; (iii) persons who properly execute and file a timely request for exclusion from the Class; (iv) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; (v) counsel for OCR Labs; and (vi) the legal representatives, successors, and assigns of any such excluded persons.

44. **Numerosity:** The number of persons within the Class is substantial, believed to amount to at least 25 people. 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 OCR Labs's or its customer's records.

45. **Typicality:** Plaintiff's claims are typical of the claims of the Class members because Plaintiff and the Class had their Biometric Data collected or otherwise obtained as part of OCR Labs's identity verification, and therefore, Plaintiff's claims arise from the same common course of conduct giving rise to the claims of the members of the Class and the relief sought is common to the Class.

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

(a) Whether Defendant collected, captured, or otherwise obtained Plaintiff's and the Class's biometric identifiers or biometric information;

(b) Whether Defendant properly informed Plaintiff and the Class 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 Plaintiff's and the Classes' biometric identifiers or biometric information;

(d) Whether Defendant has sold, leased, traded, or otherwise profited from Plaintiff and the Class's 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 Plaintiff and the Class's faceprints or facial geometry to identify them.

47. **Adequate Representation:** Plaintiff has retained and is represented by qualified and competent counsel who is highly experienced in complex consumer class action litigation. Plaintiff and his counsel are committed to vigorously prosecute this class action. Moreover, Plaintiff can fairly and adequately represent and protect the interests of such a 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 of 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 complaint to include additional class representatives to represent the Class, additional claims as may be appropriate, or to amend the Class definition to address any steps that OCR Labs took.

48. **Superiority.** 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 anticipate no difficulty in the management of this action as a class action. Class-wide relief is essential to compliance with BIPA.

V. CAUSE OF ACTION

Violation of 740 ILCS 14/1, et seq.
(On Behalf of Plaintiff and the Class)

49. Plaintiff repeats and re-alleges each and every allegation contained in paragraphs 1 through 48 above as if fully set forth herein.

50. BIPA requires companies to obtain informed written consent from individuals before acquiring their Biometric Data. Specifically, BIPA makes it unlawful for any private entity to "collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's

biometric identifiers or biometric information unless [the entity] first: (1) informs the subject . . .in writing that a biometric identifier or biometric information is being collected or stored; (2) informs the subject . . . in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; and (3) receives a written release executed by the subject of the biometric identifier or biometric information . . . .” 740 ILCS 14/15(b). OCR Labs failed to comply with these BIPA mandates.

51. 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). Unfortunately, Defendant fails to comply with these BIPA mandates too.

52. Defendant is a “private entity” under BIPA 740 ILCS 14/10 because it is a Delaware corporation.

53. Plaintiff and the Class are individuals who had their “biometric identifiers” collected by Defendant (in the form of their facial scans), as explained in detail in Section II. *See* 740 ILCS 14/10.

54. Plaintiff and the Class’s 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.

55. Defendant violated 740 ILCS 14/15(b)(3) by failing to obtain written releases from Plaintiff and the Class before it collected, used, and stored their biometric identifiers and biometric information.

56. Defendant violated 740 ILCS 14/15(b)(1) by failing to inform Plaintiff and the Class in writing that their biometric identifiers and biometric information were being collected and stored.

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

58. Defendant 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.

59. By collecting, storing, and using Plaintiff's and the Class's biometric identifiers and biometric information as described herein, Defendant violated Plaintiff's and the Class's rights to privacy in their biometric identifiers or biometric information as set forth in the BIPA, 740 ILCS 14/1, *et seq*.

60. On behalf of himself and the Class, Plaintiff seeks: (1) injunctive and equitable relief as is necessary to protect the interests of Plaintiff and the Class 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, Plaintiff, on behalf of himself and the putative Class, respectfully requests that this Court enter an Order:

A. Certifying this case as a class action on behalf of the Class defined above, and 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 willful 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, among other things, an Order requiring Defendant to collect, store, and use Biometric Data in compliance with BIPA;

E. Awarding Plaintiff and the Class their reasonable attorneys' fees and costs and other litigation expenses;

F. Awarding Plaintiff 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

Plaintiff demands a trial by jury for all issues so triable.

Dated: January 17, 2024 **CONSUMER LAW ADVOCATE, PLLC.**

By: /s/ Matthew T. Peterson

230 E. Ohio St., Suite 410
Chicago, IL 60611
Telephone: (815) 999-9130
mtp@lawsforconsumers.com
ARDC# 6321290

Attorney for Plaintiff