IN THE UNITED STATES DISTRICT COURT
FOR THE CENTRAL DISTRICT OF ILLINOIS
URBANA DIVISION

RUTVIK THAKKAR, WILLIAM GONIGAM, and ANDREA KOHLENBERG, individually and on behalf of all others similarly situated,

Plaintiffs,

v.

PROCTORU INC.,

Defendant.

Case No.

CLASS ACTION COMPLAINT

<u>JURY TRIAL DEMANDED</u>

Plaintiffs Rutvik Thakkar, William Gonigam, and Andrea Kohlenberg ("Plaintiffs"), individually and on behalf of all other persons similarly situated, by and through their attorneys, make the following allegations pursuant to the investigation of their counsel and based upon information and belief, except as to allegations specifically pertaining to themselves and their counsel, which are based on personal knowledge.

NATURE OF THE ACTION

1. This is a class action suit brought against Defendant ProctorU Inc. ("ProctorU" or "Defendant") for violations of the Illinois Biometric Information Privacy Act ("BIPA"), 740 ILCS 14/1 *et seq*. Defendant develops, owns, and operates an eponymous online proctoring software that collects biometric information.

2. Plaintiffs bring this action for damages and other legal and equitable remedies resulting from the illegal actions of Defendant in collecting, storing and using their and other

similarly situated individuals' biometric identifiers[1] and biometric information[2] (referred to collectively at times as "biometrics"). Defendant failed to provide the requisite data retention and destruction policies, and failed to properly "store, transmit, and protect from disclosure" these biometrics, in direct violation of BIPA.

3. 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.*

4. 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 that possesses biometrics must inform individuals in writing of the specific purpose and length of term for which such biometric identifiers or biometric information are being collected, stored and used. 740 ILCS 14/15(b).

5. Moreover, entities collecting biometrics must publish publicly available written retention schedules and guidelines for permanently destroying biometrics collected. *See* 740 ILCS 14/15(a).

6. Finally, entities collecting biometrics must:

> (1) store, transmit, and protect from disclosure all biometric identifiers and biometric information using the reasonable standard of care within the private entity's industry; and

[1] A "biometric identifier" is any personal feature that is unique to an individual, including fingerprints, iris scans, DNA and "face geometry", among others.

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

> (2) store, transmit, and protect from disclosure all biometric identifiers and biometric information in a manner that is the same as or more protective than the manner in which the private entity stores, transmits, and protects other confidential and sensitive information.

See 740 ILCS 14/15(e).

7. In direct violation of §§ 15(a) and 15(b) of BIPA, Defendant collected, stored and used—without first publishing sufficiently specific data retention and deletion policies—the biometrics of hundreds or thousands of students who used Defendant's software to take online exams.

8. In direct violation of the foregoing provisions of BIPA § 15(e), Defendant also failed to "store, transmit, and protect from disclosure all biometric identifiers using the reasonable standard of care within" its industry, "and in a manner that is the same as or more protective than the manner in which" it collected other sensitive information.

9. Plaintiffs are students who used ProctorU. During Plaintiffs' use of the software, ProctorU collected their biometrics, including eye movements and facial expressions (*i.e.*, face geometry) and keystroke biometrics.

10. Because Defendant did not take the proper steps to safeguard Plaintiffs' biometrics, Defendant was subject to a data breach. Further, Defendant does not sufficiently specify how long it will retain biometric information, or when it will delete such information. Accordingly, the only reasonable conclusion is that Defendant has not, and will not, destroy biometric data when the initial purpose for collecting or obtaining such data has been satisfied.

11. BIPA confers on Plaintiffs and all other similarly situated Illinois residents a right to know of such risks, which are inherently presented by the collection and storage of biometrics, and a right to have their biometrics stored using a reasonable standard of care and in a manner that

is as protective if not more than the manner in which entities store other confidential information, and a right to know how long such risks will persist after ceasing using Defendant's software.

12. Yet, Defendant failed to take such reasonable safeguards to protect the biometrics of Plaintiffs or the Class, and failed to provide sufficient data retention or destruction policies to Plaintiffs or the Class.

13. Plaintiffs bring this action to prevent Defendant from further violating the privacy rights of Illinois residents and to recover statutory damages for Defendant's improper and lackluster collection, storage, and protection of these individuals' biometrics in violation of BIPA.

JURISDICTION AND VENUE

14. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1332(d) because there are more than 100 class members and the aggregate amount in controversy exceeds $5,000,000, exclusive of interest, fees, and costs, and at least one Class member is a citizen of a state different from Defendant.

15. This Court has personal jurisdiction over Defendant because the biometrics that give rise to this lawsuit (1) belonged to Illinois residents, and (2) were collected by Defendant at Illinois schools or from students taking exams in Illinois.

16. Venue is proper in this District pursuant to 28 U.S.C. § 1391 because Defendant does substantial business in this District and a substantial part of the events giving rise to Plaintiffs' claims took place within this District because Plaintiff Thakkar's biometrics were collected in this District.

PARTIES

17. Plaintiff Rutvik Thakkar is, and has been at all relevant times, a resident of Champaign, Illinois and has an intent to remain there, and is therefore a domiciliary of Illinois.

18. Plaintiff William Gonigam is, and has been at all relevant times, a resident of Sleepy Hollow, Illinois and has an intent to remain there, and is therefore a domiciliary of Illinois.

19. Plaintiff Andrea Kohlenberg is, and has been at all relevant times, a resident of Wheaton, Illinois and has an intent to remain there, and is therefore a domiciliary of Illinois.

20. Defendant ProctorU Inc. is a Delaware corporation with its principal place of business at 2200 Riverchase Center Suite #600, Birmingham, Alabama 35244. Defendant develops, owns, and operates an online proctoring software of the same that is used throughout Illinois.

FACTUAL BACKGROUND

I. Illinois' Biometric Information Privacy Act

21. The use of a biometric scanning system entails serious risks. Unlike other methods of identification, facial geometry is a permanent, unique biometric identifier associated with an individual. This exposes individuals to serious and irreversible privacy risks. For example, if a device or database containing individuals' facial geometry data is hacked, breached, or otherwise exposed, individuals have no means by which to prevent identity theft and unauthorized tracking.

22. Recognizing the need to protect citizens from these risks, Illinois enacted the Biometric Information Privacy Act, 740 ILCS 14/1, *et seq.* ("BIPA") in 2008, to regulate companies that collect and store biometric information, such as facial geometry. *See* Illinois House Transcript, 2008 Reg. Sess. No. 276.

23. BIPA requires that a private entity in possession of biometrics:

> 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.

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.

WHAT WILL YOU BUILD? | sales@docketalarm.com | 1-866-77-FASTCASE

fastcase®
Smarter legal research.