IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS

PAUL CLARKE, individually and on behalf of all others similarly situated, Plaintiff, v. EXAMITY, INC., Defendant.	Case No. **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Paul Clarke ("Plaintiff"), individually and on behalf of all other persons similarly situated, by and through his attorneys, makes the following allegations pursuant to the investigation of his counsel and based upon information and belief, except as to allegations specifically pertaining to himself and his counsel, which are based on personal knowledge.

NATURE OF THE ACTION

1. This is a class action suit brought against Defendant Examity Inc. ("Examity" 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. Plaintiff brings this action for damages and other legal and equitable remedies resulting from the illegal actions of Defendant in collecting, storing and using his 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

[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.

destruction policies, and failed to provide Plaintiff the specific purpose and length of term for which a biometric identifier or biometric information was being collected, stored, and used.

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. 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.

7. Plaintiff is a student who used Examity. During Plaintiff's use of the software, Examity collected his biometrics, including eye movements and facial expressions (*i.e.*, face geometry).

8. 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.

9. BIPA confers on Plaintiff and all other similarly situated Illinois residents a right to know of the risks that are inherently presented by the collection and storage of biometrics, and a right to know how long such risks will persist after ceasing using Defendant's software.

10. Yet, Defendant failed to provide sufficient data retention or destruction policies to Plaintiff or the Classes.

11. Plaintiff brings 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

12. 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.

13. 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.

14. 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 Plaintiff's claims took place within this District because Plaintiff Clarke's biometrics were collected in this District.

PARTIES

15. Plaintiff Paul Clarke is, and has been at all relevant times, a resident of Aurora, Illinois and has an intent to remain there, and is therefore a domiciliary of Illinois.

16. Defendant Examity, Inc. is a Delaware corporation with its principal place of business at 135 Needham Street, Newton, Massachusetts 02464. 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

17. 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.

18. 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.

19. 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.

740 ILCS 14/15(a).

20. Moreover, entities collecting biometrics must inform individuals "in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used." 740 ILCS 14/15(b)(2).

21. As alleged below, Defendant violated BIPA §§ 15(a) and 15(b) by failing to specify the length of time that it would retain biometrics, or provide a deletion schedule for biometric information.

22. Moreover, and upon information and belief, because Defendant has failed to specify the length of time it retains biometrics, 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.

II. Defendant Violates Illinois' Biometric Information Privacy Act

23. Defendant develops, owns, and operates an eponymous online proctoring software.

24. One of the ways in which Examity monitors students is by collecting and monitoring their facial geometry and "keystroke cadence." According to Examity's website, as published in August 2020, Examity offers both auto and live proctoring.

25. For auto proctoring, Examity offers both a "standard" and "premium" version.

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.