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.

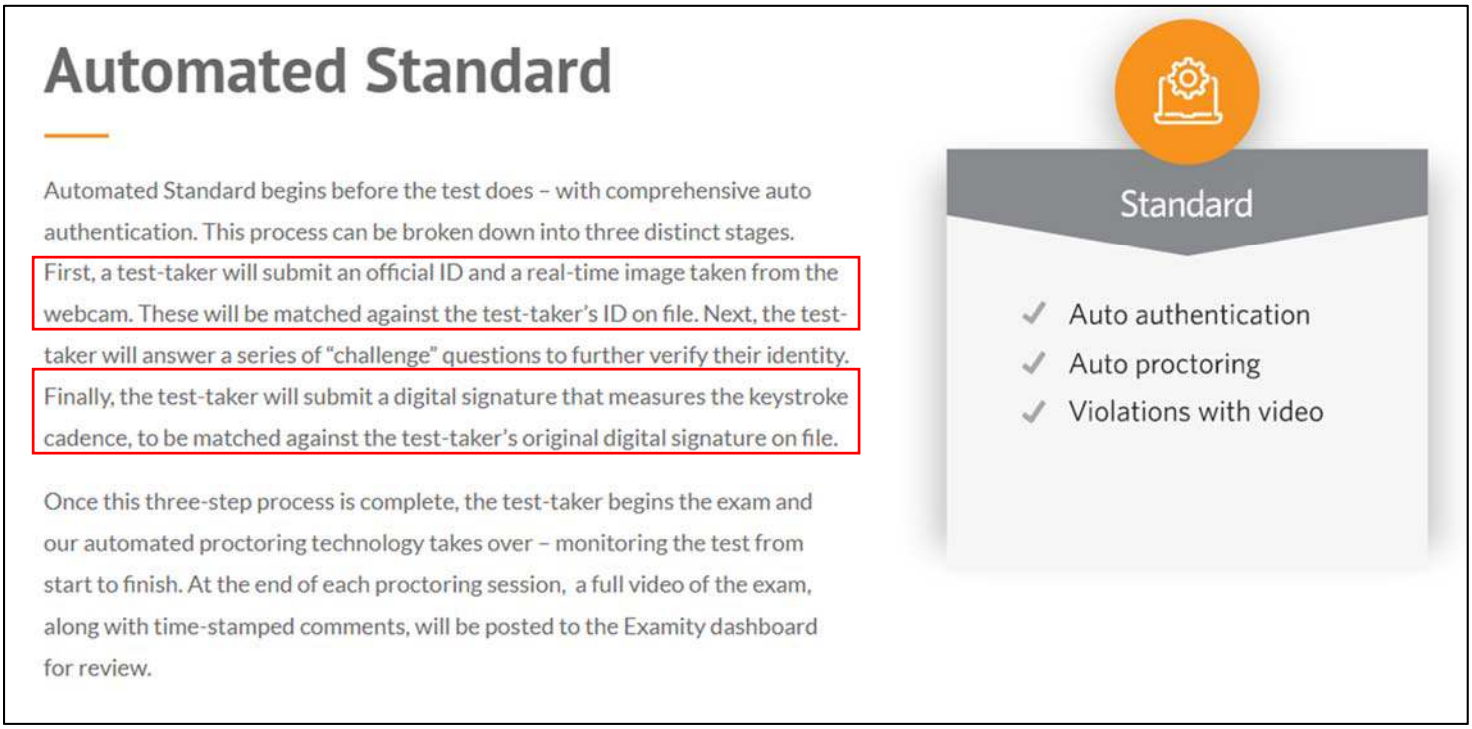
II. Defendant Violates Illinois' Biometric Information Privacy Act

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.

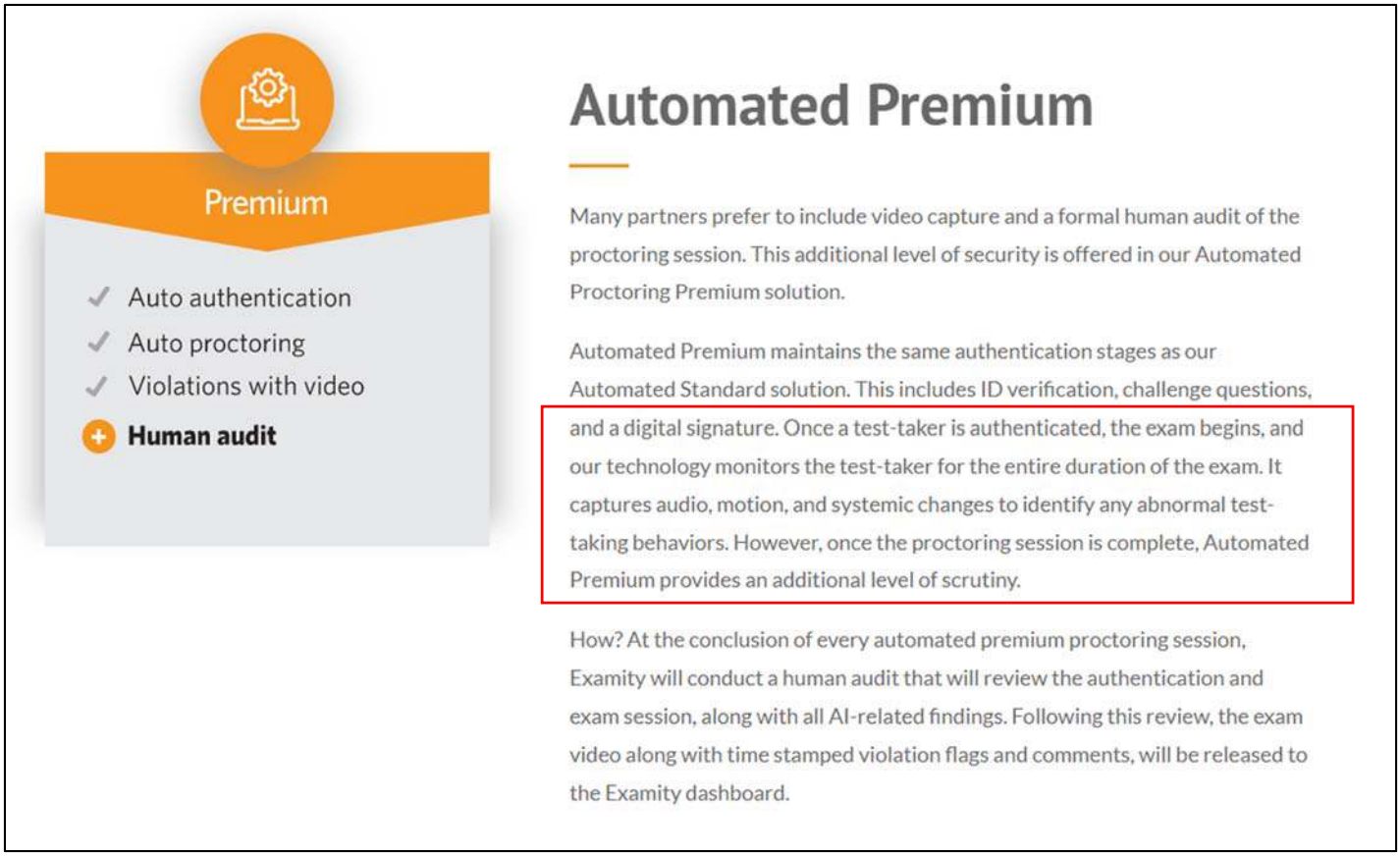
26. For the standard auto-proctoring, Examity begins with a "comprehensive auto authentication." The auto authentication begins with software that verifies and compares a "real-time image" with the "test-taker's ID on file." Auto authentication also collects a test-taker's "digital signature that measures the keystroke cadence, to be matched against the test-taker's original digital signature on file." During test administration, Examity's "automated proctoring technology takes over – monitoring the test from start to finish"[3]:



27. Examity advertises its "premium" auto-proctoring as even more invasive, stating that "Automated Premium maintains the same authentication stages as our Automated Standard solution," capturing "audio, motion, and systematic changes." Further, "once the proctoring session is complete, Automated Premium provides an additional level of scrutiny" with a human audit reviewing "all AI-related findings"[4]:

[3] https://web.archive.org/web/20200818091256/https://examity.com/auto-proctoring/

[4] *Id.*



28. For its live-proctoring services, Examity also provides "standard" and "premium" services.

//

//

//

//

//

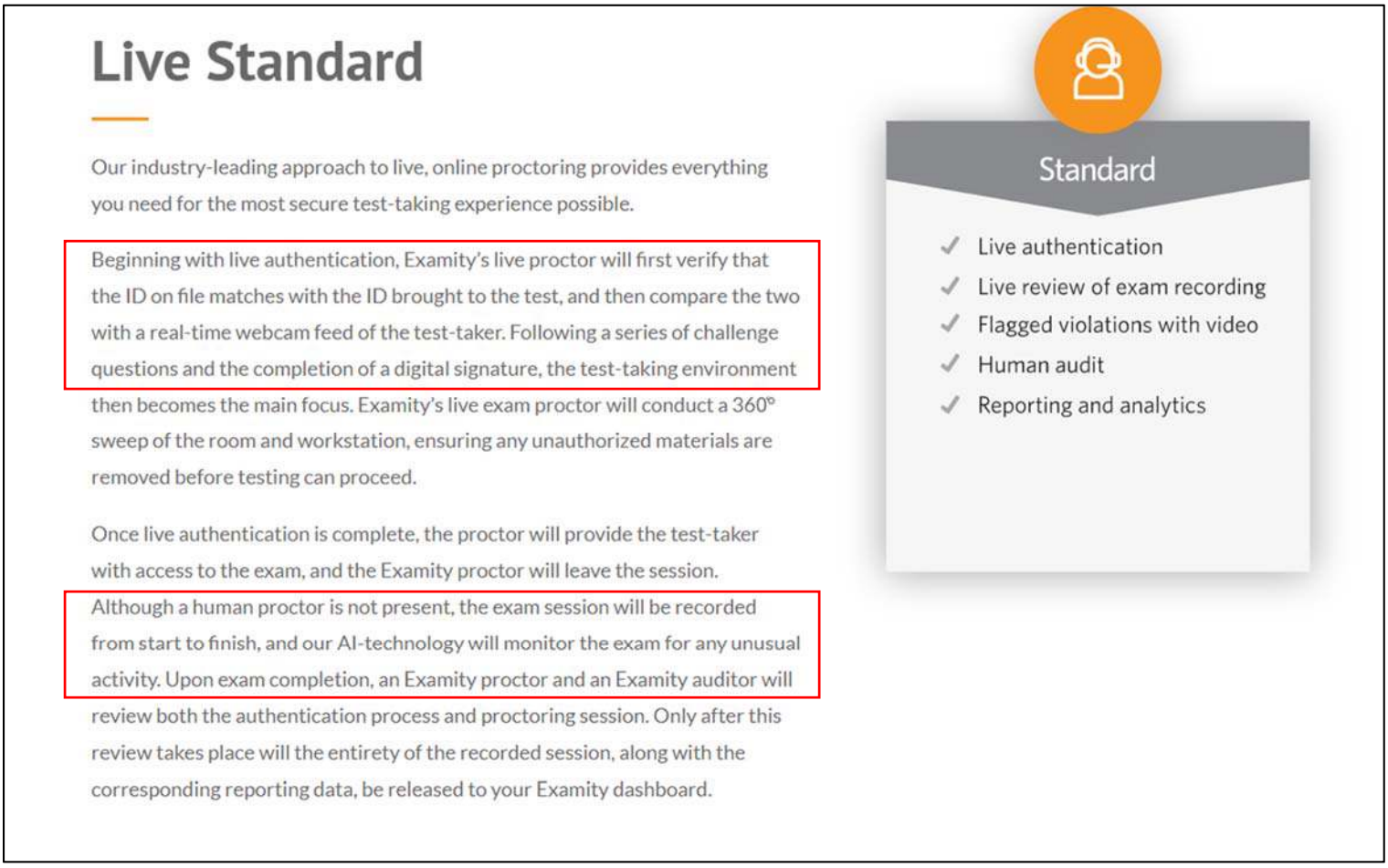
//

//

//

//

29. For its standard live-proctoring, as published in August 2020, Examity matches "the ID on file" and "the ID brought to the test" with "a real-time webcam feed of the test-taker." Further, Examity collects "a digital signature" and assures clients that "the session will be recorded from state to finish" and that Examity's "AI -technology will monitor the exam for any unusual activity"[5]:



Live Standard

Our industry-leading approach to live, online proctoring provides everything you need for the most secure test-taking experience possible.

Beginning with live authentication, Examity's live proctor will first verify that the ID on file matches with the ID brought to the test, and then compare the two with a real-time webcam feed of the test-taker. Following a series of challenge questions and the completion of a digital signature, the test-taking environment then becomes the main focus. Examity's live exam proctor will conduct a 360° sweep of the room and workstation, ensuring any unauthorized materials are removed before testing can proceed.

Once live authentication is complete, the proctor will provide the test-taker with access to the exam, and the Examity proctor will leave the session. Although a human proctor is not present, the exam session will be recorded from start to finish, and our AI-technology will monitor the exam for any unusual activity. Upon exam completion, an Examity proctor and an Examity auditor will review both the authentication process and proctoring session. Only after this review takes place will the entirety of the recorded session, along with the corresponding reporting data, be released to your Examity dashboard.

Standard

- ✓ Live authentication
- ✓ Live review of exam recording
- ✓ Flagged violations with video
- ✓ Human audit
- ✓ Reporting and analytics

//

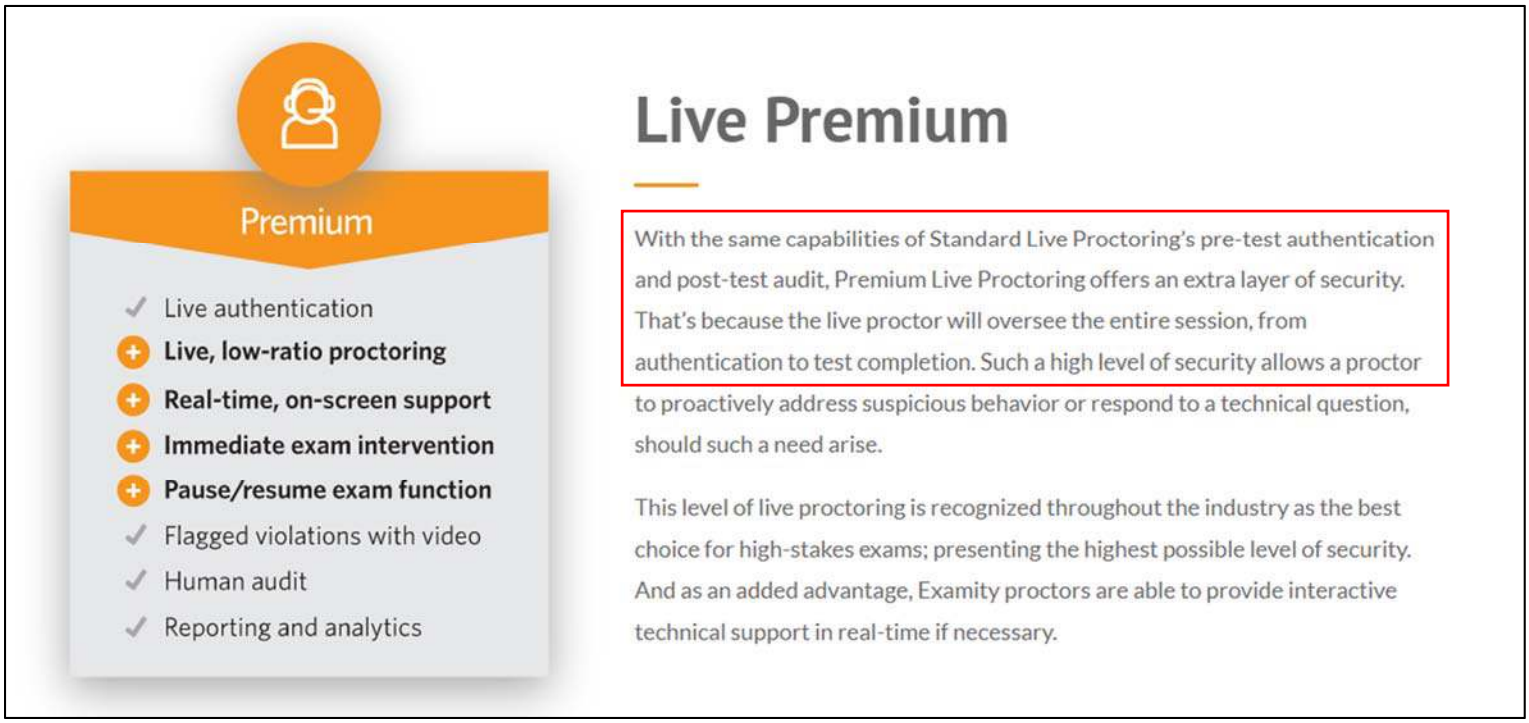
//

//

//

[5] https://web.archive.org/web/20200818101524/https://examity.com/live-proctoring/

30. Defendant's "premium" live-proctoring is just as intrusive, "[w]ith the same capabilities of Standard Live Proctoring's pre-test authentication and post-test audit" only a "live proctor will oversee the entire session, from authentication to test completion"[6]:



31. Put differently, all four proctoring services offered by Defendant actively collect biometric identifiers—including face scans and keystroke cadence—from the beginning of an exam until the end.

32. Indeed, Defendant's Product Privacy Policy, as published in August 2020, verifies as much, stating that "we have collected the following categories of personal information from our Users within the last twelve (12) months . . . E. Biometric information. Genetic, physiological, behavioral, and biological characteristics, or activity patterns used to extract a template or other identifier or identifying information, such as fingerprints, faceprints, and voiceprints, keystrokes."[7]

[6] *Id.*

[7] https://web.archive.org/web/20200817024924/https://examity.com/product-privacy-policy/.

In particular, we have collected the following categories of personal information from our Users within the last twelve (12) months:

Category	Examples	Collected
A. Identifiers.	A real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, driver's license number, passport number, or other similar identifiers.	YES
B. Personal information categories listed in the California Customer Records statute (Cal. Civ. Code § 1798.80(e)).	A name, signature, Social Security number, physical characteristics or description, address, telephone number, passport number, driver's license or state identification card number. Some personal information included in this category may overlap with other categories.	YES
C. Protected classification characteristics under California or federal law.	Age (40 years or older), race, color, citizenship, physical or mental disability, sex (including gender, gender identity, gender expression).	YES
D. Commercial information.	Records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.	NO
E. Biometric information.	Genetic, physiological, behavioral, and biological characteristics, or activity patterns used to extract a template or other identifier or identifying information, such as fingerprints, faceprints, and voiceprints, keystroke.	YES

33. Defendant's Product Privacy Policy is silent on if, when, or how it will delete or retain Plaintiff's biometric identifiers or biometric information.[8]

34. Online proctoring companies like Defendant have seen a significant uptick in light of the COVID-19 pandemic, which has caused institutions to move exams online. This has led to significant privacy implications for students.[9]

[8] *Id.*

[9] *See, e.g.*, Drew Harwell, *Mass School Closures In The Wake Of The Coronavirus Are Driving A New Wave Of Student Surveillance*, WASH. POST, Apr. 1, 2020, https://www.washingtonpost.com/technology/2020/04/01/online-proctoring-college-exams-coronavirus/ ("'Students are asked to agree to these decisions, but they have no meaningful power not to consent,' said Guy McHendry, an associate professor at Creighton University, which has used Examity for some

35. For instance, some students taking the Bar Exam were forced to urinate while being monitored, because if they "broke eye contact," their exams would be terminated.[10]

36. Other students have broken down in tears during exams, recorded on video by online proctoring companies such as Examity.[11]

37. Students have also published numerous petitions across the country to ask school administrators to cease using online proctoring tools.[12]

38. In direct violation of BIPA § 15(b)(2), from at least approximately March 2020 through present, Defendant never informed Illinois students who had their facial geometry or keystroke signature collected of the length of time for which their biometric identifiers or information would be collected, stored and used.

39. In direct violation of § 15(a) of BIPA, from at least approximately March 2020 through present, Defendant did not have written, publicly available policies identifying its retention schedules or guidelines, and has continued to retain the biometrics beyond the intended purpose for collection.

---

proctored exams. 'And because we're doing this with such urgency, we don't really have time to ingest all the implications of what these companies will do.'").

[10] Staci Zaretskym *Law Students Forced To Urinate While Being Watched By Proctors During Remote Ethics Exam*, ABOVE THE LAW, Aug. 18, 2020, https://abovethelaw.com/2020/08/law-students-forced-to-urinate-while-being-watched-by-proctors-during-remote-ethics-exam/.

[11] Thomas Germain, *Poor Security at Online Proctoring Company May Have Put Student Data at Risk*, CONSUMER REPORTS, Dec. 10, 2020, https://www.consumerreports.org/digital-security/poor-security-at-online-proctoring-company-proctortrack-may-have-put-student-data-at-risk/.

[12] Jason Kelley, *Students Are Pushing Back Against Proctoring Surveillance Apps*, ELECTRONIC FRONTIER FOUNDATION, Sept. 25, 2020, https://www.eff.org/deeplinks/2020/09/students-are-pushing-back-against-proctoring-surveillance-apps.

III. Experience of Plaintiff Paul Clarke

40. Plaintiff Clarke is an Illinois domiciliary. Plaintiff Clarke used Examity to take to take online exams while enrolled at Western Governors University.

41. When Plaintiff Clarke used Examity, his facial geometry, including his eye movements and facial expressions, was collected by Defendant.

42. When Plaintiff Clarke logged onto Examity, his facial geometry would be matched up to the biometrics he provided to Defendant to ensure he was the individual who was supposed to be taking an exam.

43. Defendant did not inform Plaintiff Clarke of the specific length of time that it intended to collect, store, and use his biometrics, nor did Defendant provide Plaintiff Clarke with a retention schedule and guidelines for permanently destroying his biometrics.

44. Upon information and belief, Examity continues to retain Plaintiff Clarke's biometrics beyond the intend purpose for collection.

45. Thus, when Plaintiff Clarke provided his biometrics to Defendant, Defendant collected said biometrics in violation of BIPA §§ 15(a) and 15(b).

CLASS ALLEGATIONS

46. **Class Definition:** Plaintiff seeks to represent a class of similarly situated individuals defined as all Illinois residents who used Examity from March 2020 through present to take an exam online and who had their facial geometry collected, captured, received, or otherwise obtained and/or stored by Defendant (the "Class").

47. Plaintiff Clarke seeks to represent a subclass of similarly situated individuals, defined as follows (the "WGU Subclass"):

> All Illinois residents who took online exams at Western Governors University from March 2020 through present and who had their facial

geometry collected, captured, received, or otherwise obtained and/or stored by Defendant.

48. Collectively, the Class and the WGU Subclass shall be known as the "Classes."

49. Subject to additional information obtained through further investigation and discovery, the above-described Classes may be modified or narrowed as appropriate, including through the use of multi-state subclasses.

50. **Numerosity:** At this time, Plaintiff does not know the exact number of members of the aforementioned Classes. However, given the size of Defendant's business and the number of students who attended Western Governors University, the number of persons within the Classes is believed to be so numerous that joinder of all members is impractical.

51. **Commonality and Predominance:** There is a well-defined community of interest in the questions of law and fact involved in this case. Questions of law and fact common to the members of the Classes that predominate over questions that may affect individual members of the Classes include:

(a) whether Defendant collected or otherwise obtained Plaintiff's and the Classes' biometric identifiers and/or biometric information;

(b) 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 3 years of their last interaction, whichever occurs first;

(c) whether Defendant destroyed Plaintiff's and the Classes' biometric identifiers and/or biometric information once that information was no longer needed for the purpose for which it was originally collected; and

(d) whether Defendant used a reasonable standard of care when collecting, storing, and protecting from disclosure the biometrics of Plaintiff's and the Classes;

(e) whether Defendant collected, stored, and protecting from disclosure the biometrics of Plaintiff's and the Classes in a manner that that is as protective if not more than the manner in which Defendant collects other biometric information;

(f) whether Defendant's violations of BIPA were committed intentionally, recklessly, or negligently.

52. **Typicality:** Plaintiff's claims are typical of those of the Classes because Plaintiff, like all members of the Classes, used Examity to take an online exam, and had his biometrics recorded and improperly stored by Defendant in violation of BIPA.

53. **Adequate Representation:** Plaintiff has retained and is represented by qualified and competent counsel who are highly experienced in complex consumer class action litigation. Plaintiff and his counsel are committed to vigorously prosecuting this class action. Moreover, Plaintiff is able to fairly and adequately represent and protect the interests of the Classes. Neither Plaintiff nor his counsel have any interest adverse to, or in conflict with, the interests of the absent members of the Classes. Plaintiff has raised viable statutory claims or the type reasonably expected to be raised by members of the Classes, and will vigorously pursue those claims. If necessary, Plaintiff may seek leave of this Court to amend this Class Action Complaint to include additional representatives to represent the Classes, additional claims as may be appropriate, or to amend the definition of the Classes to address any steps that Defendant took.

54. **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 members of the Classes is impracticable. Even if every member of the Classes 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 Classes. Plaintiff anticipates no difficulty in the management of this action as a class action. Class-wide relief is essential to compliance with BIPA.

COUNT I – FOR DAMAGES AGAINST DEFENDANT
VIOLATION OF 740 ILCS 14/15(A)

55. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

56. Plaintiff brings this claim individually and on behalf of the members of the proposed Classes against Defendant.

57. BIPA 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 (at most three years after the company's last interaction with the individual); and (ii) actually adhere to that retention schedule and actually delete the biometric information. *See* 740 ILCS 14/15(a).

58. Defendant failed to comply with these BIPA mandates.

59. Defendant is a corporation and does business in Illinois and thus qualifies as a "private entity" under BIPA. *See* 740 ILCS 14/10.

60. Plaintiff is an individual who had his "biometric identifiers" captured and/or collected by Defendant, as explained in detail in above. *See* 740 ILCS 14/10.

61. Plaintiff's biometric identifiers were used to identify Plaintiff and, therefore, constitute "biometric information" as defined by BIPA. *See* 740 ILCS 14/10.

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

63. Defendant lacked retention schedules and guidelines for permanently destroying Plaintiff's and the Classes' biometric data. As such, the only reasonable conclusion is that Defendant has not, and will not, destroy Plaintiff's and the Classes' biometric data when the initial purpose for collecting or obtaining such data has been satisfied.

64. On behalf of himself and the Classes, Plaintiff seeks: (1) declaratory relief; (2) injunctive and equitable relief as is necessary to protect the interests of Plaintiff and the Classes by requiring Defendant to comply with BIPA's requirements for the collection, capture, storage, and use of biometric identifiers and biometric information as described herein; (3) statutory damages of $5,000 for each intentional 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); and (4) reasonable attorneys' fees and costs and other litigation expenses pursuant to 740 ILCS 14/20(3).

COUNT II – FOR DAMAGES AGAINST DEFENDANT
VIOLATION OF 740 ILCS 14/15(B)(2)

65. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

66. Plaintiff brings this claim individually and on behalf of the members of the proposed Classes against Defendant.

67. BIPA requires companies to obtain informed written consent from employees 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 … (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." 740 ILCS 14/15(b)(2).

68. Defendant failed to comply with these BIPA mandates.

69. Defendant is a corporation and does business in Illinois and thus qualifies as a "private entity" under BIPA. *See* 740 ILCS 14/10.

70. Plaintiff and the Classes are individuals who have had their "biometric identifiers" collected and/or captured by Defendant, as explained in detail above. *See* 740 ILCS 14/10.

71. Plaintiff's and the Classes' biometric identifiers were used to identify them and, therefore, constitute "biometric information" as defined by BIPA. *See* 740 ILCS 14/10.

72. Defendant systematically and automatically collected, captured, used, and stored Plaintiff's and the Classes' biometric identifiers and/or biometric information without first obtaining the written release required by 740 ILCS 14/15(b)(3).

73. Defendant never informed Plaintiff, and never informed any member of the Classes, in writing of the specific length of term for which their biometric identifiers and/or biometric information were being collected, stored, used and disseminated as required by 740 ILCS 14/15(b)(1)-(2).

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

75. On behalf of himself and the Classes, Plaintiff's seek: (1) declaratory relief; (2) injunctive and equitable relief as is necessary to protect the interests of Plaintiff and the Classes by requiring Defendant to comply with BIPA's requirements for the collection, captures, storage,

use and dissemination of biometric identifiers and biometric information as described herein; (3) statutory damages of $5,000 for each intentional 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); and (4) reasonable attorneys' fees and costs and other litigation expenses pursuant to 740 ILCS 14/20(3).

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of all others similarly situated, seek judgment against Defendant as follows:

(a) For an order certifying the Classes under Rule 23 of the Federal Rules of Civil Procedure and naming Plaintiff as representative of the Classes and Plaintiff's attorneys as Class Counsel to represent the members of the Classes;

(b) For an order declaring the Defendant's conduct violates the statutes referenced herein;

(c) For an order finding in favor of Plaintiff and the Classes on all counts asserted herein;

(d) For compensatory and punitive damages in amounts to be determined by the Court and/or jury;

(e) An award of statutory penalties to the extent available;

(f) For pre-judgment interest on all amounts awarded;

(g) For an order of restitution and all other forms of monetary relief;

(h) For an order awarding Plaintiff and the Classes their reasonable attorneys' fees and expenses and costs of suit.

JURY DEMAND

Pursuant to Fed. R. Civ. P. 38(b)(1), Plaintiff demands a trial by jury of all issues so triable.

Dated: April 16, 2021

Respectfully submitted,

/s/ Carl V. Malmstrom
WOLF HALDENSTEIN ADLER FREEMAN & HERZ LLC
Carl V. Malmstrom
111 W. Jackson Blvd., Suite 1700
Chicago, IL 60604
Tel: (312) 984-0000
Fax: (212) 686-0114
E-mail: malmstrom@whafh.com
Local Counsel for Plaintiff and the Putative Classes

BURSOR & FISHER, P.A.
Alec M. Leslie*
Max S. Roberts*
888 Seventh Avenue, Third Floor
New York, NY 10019
Tel: (646) 837-7150
Fax: (212) 989-9163
Email: aleslie@bursor.com
mroberts@bursor.com

BURSOR & FISHER, P.A.
Christopher R. Reilly*
701 Brickell Avenue, Suite 1420
Miami, FL 33131
Telephone: (305) 330-5512
Facsimile: (305) 679-9006
Email: creilly@bursor.com

**Pro Hac Vice Application Forthcoming*

Attorneys for Plaintiff and the Putative Classes