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

PHILLIP BRIDGES and CHENG WU, individually and on behalf of all others similarly situated,	:	Case No. 1:21-cv-01785
Plaintiffs,	:	
v.	:	
RESPONDUS, INC.,	:	
Defendant.	:	

CLASS ACTION COMPLAINT

Plaintiffs Phillip Bridges ("Plaintiff Bridges") and Cheng Wu ("Plaintiff Wu") (collectively, "Plaintiffs") bring this action on behalf of themselves and all others similarly situated against Defendant Respondus, Inc. and its present, former, or future direct and indirect parent companies, subsidiaries, affiliates, agents, and/or other related entities ("Respondus") and allege as follows:

INTRODUCTION

1. Defendant Respondus, Inc. is a software company that develops "online proctoring software" to prevent cheating during online exams. Priding itself as a "pioneer of online testing applications for nearly two decades," Respondus touts itself as a provider of tools for "learning systems." *See* RESPONDUS, https://web.respondus.com (last visited Mar. 25, 2021).

2. In reality, Respondus provides sophisticated digital surveillance technologies to third parties, such as schools, that wish to monitor college and high school students during academic assessments.

3. One of Respondus' automatic proctoring tools, called Respondus Monitor, captures, uses, and stores vast amounts of data, including facial recognition data, facial detection

data, recorded patterns of keystrokes, eye monitoring data, gaze monitoring data, and camera and microphone recordings to effectively surveil students taking online exams.

4. Generally, students have no choice but to use Respondus Monitor if their educational institutions selected Respondus Monitor as the automatic proctoring solution for courses in which they are enrolled.

5. Additionally, virtually all students who are required to use Respondus' proctoring system download Respondus' software tools on their personal electronic devices while in their personal residences, further invading their privacy.

6. Respondus collects, captures, and stores everything from a student's facial features to their voice through a web portal accessed through the student's personal device. This means Respondus has the ability to collect and aggregate information on all aspects of a student's life. Indeed, as one director of academic testing told the *Washington Post*, software programs like Respondus' are akin to "spyware." *Mass School Closures in the Wake of the Coronavirus are Driving a New Wave of Student Surveillance*, Washington Post (Apr. 1, 2020), https://www.washingtonpost.com/technology/2020/04/01/online-proctoring-college-exams-coronavirus/. Likewise, an economics professor at Harvard University recently told *Forbes* that this type of technology involves an inappropriate "level of intrusion." Sean Lawson, *Are Schools Forcing Students to Install Spyware that Invades Their Privacy as a Result of the Coronavirus Lockdown?*, Forbes (Apr. 24, 2020 6:34 PM), https://www.forbes.com/sites/seanlawson/2020/04/24/are-schools-forcing-students-to-install-spyware-that-invades-their-privacy-as-a-result-of-the-coronavirus-lockdown/?sh=1fbe87cb638d. Relatedly, Duke University has decided not to allow virtual proctoring at this time, in part because of security concerns. *Id.*

7. All the while, students are left in the dark about the vast amount of information Respondus collects. Respondus does not disclose or obtain written consent before collecting, capturing, storing, or sharing users' biometric information or biometric identifiers. Respondus also fails to disclose what it does with that biometric data after collection and does not comply with Illinois' Biometric Information Privacy Act, 470 ILCS 14/ ("BIPA's") retention and destruction requirements for private entities that possess biometric identifiers or biometric information.

8. It is, therefore, no surprise that there is an outcry among students and faculty about the use of online proctoring software and services. Petitions have sprung up across college campuses nationwide demanding a ban on online proctoring. At major universities, such as the University of Texas at Dallas, California State University Fullerton, the University of Miami, Florida State University, Auburn University, the University of Wisconsin–Madison, and the City University of New York, petitions have gained tens of thousands of student and faculty signatures. At the University of California Santa Barbara, the Faculty Association published a letter demanding that university administration officials rescind its contracts with online-proctoring companies amid concerns these tools could turn the university into "a surveillance tool." *Id*.

9. Plaintiffs bring this action to enforce their legal rights under BIPA, and those of the proposed class of persons they represent.

10. BIPA is designed to protect individuals against the threat of irreparable privacy harms, identity theft, and other economic injuries arising from private entities' increasing use of biometric identifiers and biometric information.

11. In enacting BIPA in 2008, the Illinois Legislature recognized that biometrics are unlike other unique identifiers because they are biologically unique to the individual and cannot be changed. Once compromised, the individual has no recourse. *See* 740 ILCS 14/5(c).

12. BIPA protects public welfare, security, and safety by regulating the collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and biometric information. *See* 740 ILCS 14/5(g).

13. BIPA defines a biometric identifier as "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry." 740 ILCS 14/10.

14. BIPA defines biometric information as "any information, regardless of how it is captured, converted, stored or shared, based on an individual's biometric identifier used to identify an individual." *Id*.

15. Plaintiffs allege Respondus violated BIPA by, among other things, collecting, capturing, using, storing, and sharing Plaintiffs' and class members' biometric identifiers or biometric information without informed written consent.

16. Respondus violated BIPA's requirement that it maintain, disclose, and follow a retention policy that requires Respondus to permanently destroy students' biometric data once the purpose for collecting such data has been satisfied.

17. Respondus' failure to follow BIPA's express disclosure and consent requirements and failure to comply with the destruction requirements for biometric identifiers and biometric information was an invasion of Plaintiffs' personal rights and the rights of the class members they represent.

18. Respondus illegally profits from possessing the biometric identifiers or biometric information of Plaintiffs and members of the class they represent.

19. A class action is the best means of obtaining redress for Respondus' wide-scale BIPA violations and is consistent with the fairness and efficiency goals of class actions.

JURISDICTION AND VENUE

20. This Court has subject-matter jurisdiction over this putative class action lawsuit under 28 U.S.C. § 1332(d).

21. The Court has personal jurisdiction over Respondus because Plaintiffs' claims arise out of and relate to Respondus' conduct in the state of Illinois.

22. Venue is proper in this Court under 28 U.S.C. § 1391(b) because Plaintiffs reside in this District and the transactions or some part thereof out of which the causes of action arose occurred in this District.

PARTIES

23. Plaintiff Bridges is a natural person who resides in Illinois.

24. Plaintiff Wu is a natural person who resides in Illinois.

25. Respondus is a Washington corporation with its principal place of business at 8201 164th Avenue NE, Suite 200, Redmond, Washington 98052, and whose registered agent for service of process is C T Corporation System, 711 Capitol Way, Suite 204, Olympia, Washington 98501-1267.

26. Respondus is a self-described education company with "a deep understanding of online testing." RESPONDUS, https://web.respondus.com/about/ (last visited Mar. 25, 2021). For 20 years, Respondus has partnered with universities and other institutions of learning to develop "world-class educational technologies." *Id*.

FACTUAL BACKGROUND

A. Online and Remote Proctoring

27. During the COVID-19 pandemic, schools, colleges, universities, and other educational institutions ("Institutions") have been forced to cease in-person instruction and move to remote learning. However, even prior to the pandemic, many Institutions have offered online coursework that requires students to take quizzes and exams online.

28. To facilitate remote test taking, Institutions contract with private companies that offer online exam monitoring and proctoring services.

29. One such company is Respondus, which offers several cloud-based software and service applications to assist Institutions in providing online content and exams to students.

30. Institutions that use Respondus' applications incorporate these tools into the Institution's learning management system ("LMS"). Well-known LMSs include Canvas, Blackboard Learn, Brightspace, and Moodle.

31. On its website, Respondus promotes its smooth integration of Respondus applications with these LMS platforms: "When we do everything right, users are unaware they're using a Respondus application because it looks and feels like a native tool of the LMS." RESPONDUS, https://web.respondus.com/partners/lms/ (last visited Mar. 25, 2021).

32. Respondus' servers, which house all data related to Respondus' applications (Respondus Monitor, LockDown Browser, StudyMate Campus, and Respondus 4.0), are controlled and operated by a third-party hosting provider—specifically, Amazon Web Services. *See* RESPONDUS, http://web.respondus.com/data-processing/ (last visited Mar. 25, 2021).

33. Respondus' most widely-used LMS application is LockDown Browser, a custom browser that locks down a testing environment within an LMS. Respondus states that LockDown Browser is the "gold standard" for securing online exams in classroom settings or

proctored environments. RESPONDUS, https://web.respondus.com/he/lockdownbrowser/ (last visited Mar. 25, 2021).

34. Respondus also offers StudyMate Campus, a tool to create flash cards, self-assessments, and learning games within the LMS, and Respondus 4.0, a tool for creating exams that can be published directly to the LMS for online test taking. *See* RESPONDUS, https://web.respondus.com/he/studymate/ (last visited Mar. 25, 2021); *see also* RESPONDUS, https://web.respondus.com/he/respondus/ (last visited Mar. 25, 2021).

35. Each of Respondus' applications has unique Terms of Use that an Institution or student must accept prior to launching the software or service.

B. The Respondus Monitor Tool

36. This lawsuit arises from another of Respondus' applications—the "Respondus Monitor" tool, a fully-automated exam proctoring solution that enables students to take exams online in a *non-proctored* environment.

37. As of November 13, 2020, Respondus' website claimed that more than 1,000 higher educational institutions use Respondus for remote, un-proctored test taking and more than 20 million exams would be proctored that year using Respondus Monitor, far more than any other proctoring service in higher education. RESPONDUS, https://web.respondus.com/he/monitor/ (last visited Nov. 13, 2020).

38. Dozens of colleges and universities in Illinois use the Respondus Monitor tool.

39. Respondus' website explains that "[a]t the heart of [the] Respondus Monitor [tool] is a powerful artificial intelligence engine, Monitor AI™, that performs a second-by-second analysis of the exam session." Monitor AI uses "facial detection, motion, and lighting to analyze the student and examination environment." RESPONDUS, https://web.respondus.com/he/monitor/ (follow "Learn More" link in "Monitor AI is the most

advanced artificial intelligence system for automated proctoring" box) (last visited Nov. 13, 2020).

40. Respondus' website and marketing materials acknowledge that the Respondus Monitor tool uses facial recognition technology to determine, among other things, whether the person who started the exam switches to a different person along the way. *Id*.

41. Respondus' website explains this "data then flows into the 'Review Priority' system to help instructors quickly evaluate the proctoring results." *Id*.

42. Review Priority is a "patent-pending method for ranking proctoring results according to the risk that violations have occurred. … If wanted, instructors can view the data contributing to the Review Priority result on a video timeline, such as flagged events and key milestones." RESPONDUS, https://web.respondus.com/he/monitor/ (follow "Learn More" link in "Review Priority ranks results by risk, helping instructors know which sessions warrant deeper scrutiny" box) (last visited Nov. 13, 2020).

43. However, the Respondus Monitor Terms of Use for Students say nothing about facial recognition, biometric identifiers, or biometric information and do not disclose to student users that their biometric identifiers or information will be captured, collected, analyzed, or disseminated to the student's Institution or shared with Amazon Web Services.[1]

C. Test Taking with Respondus Monitor

44. To take an exam using Respondus Monitor, a student must have a webcam.

45. The student first logs into their Institution's LMS platform and opens the LockDown Browser.

[1] On January 21, 2021, Respondus updated the Respondus Monitor Terms of Use for Students. All references to the Respondus Monitor Terms of Use for Students (the "Monitor Student Terms") refer to the Monitor Student Terms in effect prior to January 21, 2021.

46. Next, the student is required to accept the Respondus Monitor Terms of Use for Students (the "Monitor Student Terms") by clicking, "I accept." Accepting the Monitor Student Terms is a condition of proceeding with the exam through Respondus Monitor.

D. The Monitor Student Terms

47. The Monitor Student Terms include two components—terms applicable to (i) the student's relationship with Respondus; and (ii) the student's relationship with the Institution. A true and correct copy of the Monitor Student Terms in effect prior to January 21, 2021 is attached hereto as **Exhibit A** and was previously publicly available on Respondus' website.

48. The Monitor Student Terms inform the students that "your Institution is requiring students to use Respondus Monitor for certain, or all, courses. In order to use Respondus Monitor, you must agree to these Terms in full, including this section under REQUIREMENTS OF YOUR INSTITUTION, regarding your relationship with your Institution." (Ex. A.)

49. Next, in relevant part, the Monitor Student Terms disclose that Respondus Monitor will record student activity, both audibly and visually, during exams. (*See id*.)

50. However, prior to January 21, 2021, the Monitor Student Terms did *not* disclose that Respondus Monitor would use facial recognition technology to collect, capture, analyze, and disseminate a student's biometric identifiers or biometric information.

51. Instead, the Monitor Student Terms cryptically stated that "other data" related to student activity during an assessment may be recorded by Respondus Monitor. The Terms stated that "[t]he recordings are controlled by your Institution" and will be processed by Respondus on behalf of the Institution. (*See id.*)

52. This "other data" includes students' biometric identifiers and biometric information, but that fact is not disclosed in the Monitor Student Terms.

53. The Monitor Student Terms state that Respondus "may analyze the recordings through automated processes to generate additional data derived from the recordings, with the additional data being associated with individual students for use by your Institution in evaluating the recordings." (*Id.*)

54. This "additional data" that Respondus generates includes students' biometric identifiers and biometric information, but, prior to January 21, 2021, that fact was not disclosed in the Monitor Student Terms.

55. The Monitor Student Terms say this additional data and the original exam recordings "may be evaluated by agents of your Institution, including your instructors, to review, assess, and analyze student performance and conduct … for the purpose of improving educational processes for students, including investigating student conduct violations." (*Id.*)

56. This "additional data" that may be evaluated by an Institution includes students' biometric identifiers and biometric information, but, prior to January 21, 2021, that fact was not disclosed in the Monitor Student Terms.

57. Furthermore, the Monitor Student Terms do not disclose that Respondus shares biometric identifiers and biometric information with Amazon Web Services.

58. The Monitor Student Terms additionally state Respondus works with the Institution to ensure the student's privacy regarding the recording and to comply with applicable law as to any information or data. (*See id.*)

59. This "data" that is subject to privacy laws includes students' biometric identifiers and biometric information, but, prior to January 21, 2021, that fact was not disclosed in the Monitor Student Terms.

60. The Monitor Student Terms state Respondus Monitor will save all recordings of students for one (1) year, but that Institutions have the ability to retain data for up to an additional four (4) years. (*See id.*)

61. The "data" an Institution can retain for up to four (4) years includes students' biometric identifiers and biometric information, but, prior to January 21, 2021, that fact was not disclosed in the Monitor Student Terms.

62. Prior to January 21, 2021, the Monitor Student Terms did not establish a retention schedule or guidelines for permanently destroying students' biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information had been satisfied or within three (3) years of the student's last interaction with Respondus or the Institution, whichever occurred first.

63. To the contrary, the Monitor Student Terms state Respondus does not guarantee removal of "all traces of any information or data (including recordings) from the Respondus Monitor Services after deletion." (*See id*.)

64. This trace "information and data" includes students' biometric identifiers and biometric information, but, prior to January 21, 2021, that fact was not disclosed in the Monitor Student Terms.

65. Brazenly, in the Monitor Student Terms, the Institution unlawfully purports to disclaim any liability to the student for the "legality" or "availability of information or data in the Respondus Monitor Service or Software." The Monitor Student Terms also purport to disclaim any liability of the Institution to the student for harm resulting from "downloading or accessing any information or data through Respondus Monitor." (*See id*.)

E. Privacy Policies in the Monitor Student Terms

66. The Monitor Student Terms include two privacy policies—a Privacy and Security Policy (the "Monitor Privacy Policy"[2]), described in the Monitor Student Terms, and the "full Respondus Privacy Policy," incorporated by reference and publicly available on Respondus' website. *See* RESPONDUS, https://web.respondus.com/privacy-policy (last visited Mar. 25, 2021) (the "Respondus Privacy Policy").

F. The Monitor Privacy Policy

67. The Monitor Privacy Policy states that "Instructors, administrators and other agents of Institution" may access the *recordings and data* related to their students through Respondus Monitor. (Ex. A.)

68. The "recordings and data" that may be accessed by agents of the Institution include students' biometric identifiers and biometric information, but, prior to January 21, 2021, that fact was not disclosed in the Monitor Privacy Policy.

69. The Monitor Privacy Policy states that samples of de-identified student video recordings may be shared with researchers, including biometric experts. (*See id*.)

70. However, prior to January 21, 2021, the Monitor Privacy Policy did not disclose that, prior to sending student video recordings to experts for research purposes, Respondus already captured the students' biometric information or biometric identifiers from these recordings.

71. The Monitor Privacy Policy does not disclose that Respondus shares biometric identifiers and biometric information with Amazon Web Services.

[2] On January 21, 2021, Respondus, Inc. updated the Monitor Privacy Policy. All references to the Monitor Privacy Policy refer to the Monitor Privacy Policy in effect prior to January 21, 2021.

72. Prior to January 21, 2021, the Monitor Privacy Policy did not establish a retention schedule or guidelines for permanently destroying students' biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information had been satisfied or within three (3) years of the students' last interaction with Respondus or the Institution, whichever occurred first.

G. The Respondus Privacy Policy

73. The Respondus Privacy Policy is incorporated by reference into the Monitor Student Terms. A true and correct copy of the Respondus Privacy Policy obtained from Respondus' website is attached hereto as **Exhibit B.** RESPONDUS, https://web.respondus.com/privacy-policy/ (last visited Mar. 25, 2021).

74. The Respondus Privacy Policy does not disclose that Respondus collects student biometric identifiers and biometric information through Respondus Monitor. (*See* Ex. B.)

75. The Respondus Privacy Policy does not disclose that Respondus shares biometric identifiers and biometric information with Amazon Web Services.

76. The Respondus Privacy Policy does not establish a retention schedule and guidelines for permanently destroying students' biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within three (3) years of the student's last interaction with Respondus or the Institution, whichever occurs first. (*See id.*)

H. Other Relevant Monitor Student Terms

77. The Monitor Student Terms state that if the student does not agree to the Monitor Student Terms, "[the student] will not be permitted to use this Service." (Ex. A.)

78. The Monitor Student Terms have an integration clause that states, "the Terms constitute the entire agreement between the parties with respect to the subject contained herein

and supersede any other agreements between Respondus and you regarding Respondus Monitor." (*Id*.)

79. The Monitor Student Terms also provide that "[a]ll legal issues arising from or related to the use of Respondus Monitor between you and your Institution shall be construed in accordance with the laws of the state in which your Institution resides …." (*Id*.)

80. The Monitor Student Terms state that students using Respondus Monitor, and thus agreeing to these Monitor Student Terms, "consent to personal jurisdiction and venue in the state and federal courts located in and serving the county in which your Institution resides." (*Id.*)

I. The Capture of Student Biometric Identifiers and Information

81. After a student clicks to accept the Monitor Student Terms in their browser, Respondus Monitor conducts a webcam check to confirm the webcam's audio and video are working properly. In this step, Respondus Monitor requires that a student's face be centered in the camera and that the student speak into the microphone.

82. Next, Respondus Monitor's portal instructs the student to look into the webcam so it can capture an image of the student so the student's identity can be confirmed.

83. The Respondus Monitor portal may require the student to show photo identification so the software can take a picture of the photo identification before proceeding.

84. Next, the Respondus Monitor portal instructs the student to use the webcam to record a 360-degree "environment check" of the student's test-taking surroundings. This recording is captured by the Respondus Monitor system.

85. Lastly, Respondus Monitor conducts a "facial detection check" of the student taking the exam and requires the student to look directly into the webcam.

86. During these pre-exam steps, unbeknownst to the student, Respondus Monitor captures the student's facial geometry and other biometric identifiers.

J. Plaintiff Bridges' Experience with Respondus Monitor

87. Plaintiff Bridges is currently a student at Resurrection University in Chicago, Illinois.

88. Plaintiff Bridges enrolled in courses at Resurrection University that required the use of Respondus Monitor for exams. Plaintiff Bridges recalls using Respondus Monitor to take exams on at least twenty (20) occasions.

89. Since January 1, 2021, Plaintiff Bridges has used Respondus Monitor take exams on approximately ten (10) occasions.

90. Plaintiff Bridges recalls that, in using Respondus Monitor for test taking, he was required to take video footage of his surroundings and of his face prior to starting each exam.

91. When agreeing to use Respondus Monitor for the exams, Plaintiff Bridges did not know Respondus Monitor would collect and analyze his biometric identifiers or biometric information prior to and during the exams.

92. When agreeing to use Respondus Monitor for his exams, Plaintiff Bridges did not give informed written consent for his biometric identifiers or information to be collected, stored, used, or disseminated.

93. When agreeing to use Respondus Monitor, Plaintiff Bridges was unaware of any collection and retention policy that Respondus has regarding his biometric identifiers and biometric information collected through Respondus Monitor.

94. The context in which Plaintiff Bridges was asked to accept the Monitor Student Terms—as a requirement to successfully complete a college course examination—did not give him a meaningful choice.

K. Plaintiff Wu's Experience with Respondus Monitor

95. Plaintiff Wu is a former student of Illinois Institute of Technology in Chicago, Illinois.

96. Prior to his graduation from Illinois Institute of Technology in the fall of 2020, Plaintiff Wu enrolled in courses at Illinois Institute of Technology that required the use of Respondus Monitor for exams.

97. Plaintiff Wu recalls using Respondus Monitor to take exams on at least six (6) occasions.

98. Since March 25, 2020, Plaintiff Wu has used Respondus Monitor to take exams on approximately three occasions.

99. Plaintiff Wu has not used Respondus Monitor since he graduated from Illinois Institute of Technology in the fall of 2020.

100. Plaintiff Wu recalls that, in using Respondus Monitor for test taking, he was required to take video footage of his surroundings and of his face prior to starting each exam.

101. When agreeing to use Respondus Monitor for the exams, Plaintiff Wu did not know Respondus Monitor would collect and analyze his biometric identifiers or biometric information prior to and during the exams.

102. When agreeing to use Respondus Monitor for his exams, Plaintiff Wu did not give informed written consent for his biometric identifiers or information to be collected, stored, used, or disseminated.

103. When agreeing to use Respondus Monitor, Plaintiff Wu was unaware of any collection and retention policy that Respondus has regarding his biometric identifiers and biometric information collected through Respondus Monitor.

104. The context in which Plaintiff Wu was asked to accept the Monitor Student Terms—as a requirement to successfully complete a college course examination—did not give him a meaningful choice.

CLASS ALLEGATIONS

105. Plaintiffs bring this action on behalf of a Class of all other persons or entities similarly situated in the state of Illinois (the "Class").

106. The Class of persons Plaintiffs propose to represent is tentatively defined as:

> All persons who took an assessment using Respondus Monitor in Illinois at any time during the five years prior to the filing of this Complaint through January 20, 2021.

107. Excluded from the Class are counsel, Defendant, any entities in which Defendant has a controlling interest, Defendant's agents and employees, any judge to whom this action is assigned, and any member of such judge's staff and immediate family.

108. The Class defined above is identifiable through Defendant's business records.

109. The potential members of the Class number, at least, in the thousands.

110. Individual joinder of these persons is impracticable.

111. Plaintiffs Bridges and Wu are members of the Class.

112. There are questions of law and fact common to Plaintiffs and to the proposed Class, including but not limited to the following:

a. Whether Defendant developed a written policy, 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 have been satisfied or within three (3) years of the individual's last interaction with Defendant, whichever occurs first, and whether Defendant complied with such written policy;

b. Whether Defendant collects, captures, or otherwise obtains Plaintiffs' and Class members' biometric identifiers or information without:

(i) informing them in writing that a biometric identifier or biometric information is being collected and stored;

(ii) informing them in writing of the specific purpose and length of term for which biometric identifier or biometric information is being collected, stored, and used; or

(iii) obtaining their written release;

c. Whether Defendant profits from Plaintiffs' and Class members' biometric identifiers or information;

d. Whether Defendant discloses or disseminates Plaintiffs' and Class members' biometric identifiers or biometric information without Plaintiffs' and Class members' consent;

e. Whether Defendant's conduct was negligent;

f. Whether Defendant's conduct was knowing or reckless; and

g. Whether Plaintiffs and Class members are entitled to damages for violation of their privacy rights.

113. Plaintiffs' claims are typical of the claims of Class members.

114. Plaintiffs are adequate representatives of the Class because their interests do not conflict with the interests of the Class, they will fairly and adequately protect the interests of the Class, and they are represented by counsel skilled and experienced in class actions.

115. Common questions of law and fact predominate over questions affecting only individual Class members, and a class action is the superior method for fair and efficient

adjudication of the controversy. The only individual question concerns identification of Class members, which will be ascertainable from records maintained by Defendant.

116. The likelihood that individual members of the Class will prosecute separate actions is remote due to the time and expense necessary to prosecute an individual case.

FIRST CLAIM FOR RELIEF
Violation of 740 ILCS 14/15(a)

117. Plaintiffs repeat the prior allegations of this Complaint and incorporate them by reference herein.

118. Respondus is a "private entity" for purposes of BIPA.

119. Respondus is in possession of biometric identifiers or biometric information from students who use Respondus Monitor.

120. Respondus does not have 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 (3) years of the individual's last interaction with the private entity, whichever occurs first, in violation of 740 ILCS 14/15(a).

121. Respondus' failure to maintain and comply with such a written policy is negligent and reckless because BIPA has governed the collection and use of biometric identifiers and biometric information since 2008, and Respondus is presumed to know these legal requirements. Respondus' selective disclosure on its website and for marketing purposes that it is collecting and using biometric data, but not disclosing this same information in the Monitor Student Terms, shows that Respondus' conduct is willful or reckless. Respondus' conduct is all the more egregious given the current and public discourse among Respondus' customers and users about how online proctoring systems violate students' privacy rights.

122. Respondus' unlawful conduct caused injury to Plaintiffs and the proposed Class.

123. Plaintiffs and the Class seek damages, attorney's fees, and costs.

SECOND CLAIM FOR RELIEF
Violation of 740 ILCS 14/15(b)

124. Plaintiffs repeat the prior allegations of this Complaint and incorporate them by reference herein.

125. Respondus collects, captures, and obtains biometric identifiers or biometric information from students who use Respondus Monitor in violation of 740 ILCS 14/15.

126. Respondus collects, captures, and obtains such biometric identifiers or biometric information without informing the students in writing that biometric identifiers or biometric information is being collected or stored in violation of 740 ILCS 14/15(b)(1).

127. Respondus collects, captures, and obtains such biometric identifiers or biometric information without informing the students in writing of the specified purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used in violation of 740 ILCS 14/15(b)(2).

128. Respondus collects, captures, and obtains such biometric identifiers or biometric information without receiving a written release executed by the students in violation of 740 ILCS 14/15(b)(3).

129. Respondus' unlawful conduct is negligent and reckless because BIPA has governed the collection and use of biometric identifiers and biometric information since 2008, and Respondus is presumed to know these legal requirements. Respondus' selective disclosure on its website and for marketing purposes that it is collecting and using biometric data, but not disclosing this same information in the Monitor Student Terms, shows Respondus' conduct is willful or reckless. Respondus' conduct is all the more egregious given the current and public

discourse among Respondus' customers and users about how online proctoring systems violate students' privacy rights.

130. Respondus' unlawful conduct caused injury to Plaintiffs and the proposed Class.

131. Plaintiffs and the Class seek damages, attorney's fees, and costs.

THIRD CLAIM FOR RELIEF
Violation of 740 ILCS 14/15(c)

132. Plaintiffs repeat the prior allegations of this Complaint and incorporate them by reference herein.

133. Respondus is in possession of biometric identifiers or biometric information it collects when students use Respondus Monitor.

134. Respondus contracts with Institutions to provide the Respondus Monitor tool to Institutions and receives a fee in exchange.

135. Respondus profits from students' biometric identifiers or biometric information through contracts it has with Institutions for the Respondus Monitor service.

136. Respondus' unlawful conduct is negligent and reckless because BIPA has governed the collection and use of biometric identifiers and biometric information since 2008, and Respondus is presumed to know these legal requirements. Respondus' selective disclosure on its website and for marketing purposes that it is collecting and using biometric data, but not disclosing this same information in the Monitor Student Terms, shows Respondus' conduct is willful or reckless. Respondus' conduct is all the more egregious given the current and public discourse among Respondus' customers and users about how online proctoring systems violate students' privacy rights.

137. Respoundus' unlawful conduct caused injury to Plaintiffs and the proposed Class.

138. Plaintiffs and the Class seek damages, attorney's fees, and costs.

FOURTH CLAIM FOR RELIEF
Violation of 740 ILCS 14/15(d)

139. Plaintiffs repeat the prior allegations of this Complaint and incorporate them by reference herein.

140. Respondus is in possession of biometric identifiers or biometric information it collects when students use Respondus Monitor.

141. Respondus discloses or disseminates students' biometric identifiers or biometric information to the student's Institution without the student's consent to the disclosure in violation of 740 ILCS 14/15(d).

142. Respondus further discloses or disseminates students' biometric identifiers or biometric information to Amazon Web Services without the student's consent to the disclosure in violation of 740 ILCS 14/15(d).

143. Respondus' unlawful conduct is negligent and reckless because BIPA has governed the collection and use of biometric identifiers and biometric information since 2008, and Respondus is presumed to know these legal requirements. Respondus' selective disclosure on its website and for marketing purposes that it is collecting and using biometric data, but not disclosing this same information in the Monitor Student Terms, shows Respondus' conduct is willful or reckless. Respondus' conduct is all the more egregious given the current and public discourse among Respondus' customers and users about how online proctoring systems violate students' privacy rights.

144. Respondus' unlawful conduct caused injury to Plaintiffs and the proposed Class.

145. Plaintiffs and the Class seek damages, attorney's fees, and costs.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of the Class, pray for the following

relief:

A. Certification of the proposed Class;

B. Appointment of Plaintiffs as representatives of the Class;

C. Appointment of the undersigned counsel as counsel for the Class;

D. An award to Plaintiffs and the Class of damages, as allowed by law; and

E. Orders granting such other and further relief as the Court deems necessary, just, and proper.

JURY TRIAL DEMANDED

Plaintiffs, on behalf of themselves and all others similarly situated, hereby demand trial by jury on all issues in this Complaint that are triable as a matter of right.

Dated: April 2, 2021

Respectfully submitted,

/s/ Brian K. Murphy
Brian K. Murphy (6225697)
Jonathan P. Misny
Murray Murphy Moul + Basil LLP
1114 Dublin Road
Columbus, OH 43215
Telephone: 614.488.0400
Facsimile: 614.488.0401
Email: murphy@mmmb.com
misny@mmmb.com

Samuel J. Strauss
Mary C. Turke
Turke & Strauss LLP
613 Williamson Street #201
Madison, WI 53703
Telephone: 608.237.1775
Facsimile: 608.509.4423
Email: sam@turkestrauss.com
Email: mary@turkestrauss.com

Anthony I. Paronich
Paronich Law, P.C.
350 Lincoln Street, Suite 2400
Hingham, MA 02043
Telephone: 508.221.1510
Email: anthony@paronichlaw.com

Lauren E. Urban (6293832)
1424 N. Hoyne Ave.
Chicago, IL 60622
(419) 344-1146
lauren.elizabeth.urban@gmail.com

Counsel for Plaintiffs