

YES  NO

**EXHIBITS**

**CASE NO.** 2021 CH 1027

**DATE:** 3/3/2021

**CASE TYPE:** Class Action

**PAGE COUNT:** 22

**CASE NOTE**

---

---

---

**12-Person Jury**

Return Date: No return date scheduled  
Hearing Date: 7/1/2021 10:00 AM - 10:00 AM  
Courtroom Number: 2302  
Location: District 1 Court  
Cook County, IL

FILED  
3/3/2021 4:08 PM  
IRIS Y. MARTINEZ  
CIRCUIT CLERK  
COOK COUNTY, IL

**IN THE CIRCUIT COURT OF COOK COUNTY, ILLINOIS  
COUNTY DEPARTMENT, CHANCERY DIVISION**

JOHN DOE, individually and on behalf of all  
others similarly situated,

Plaintiff,

v.

DEPAUL UNIVERSITY,

Defendant.

Case No. 2021CH01027

12427900

CLASS ACTION

JURY TRIAL DEMANDED

**CLASS ACTION COMPLAINT**

Plaintiff John Doe (“Plaintiff”) brings this action on behalf of himself and all others similarly situated against Defendant DePaul University and its present, former, or future direct and indirect parent companies, subsidiaries, affiliates, agents, and/or other related entities (“DePaul” or “Defendant”) and alleges as follows:

**INTRODUCTION**

1. Defendant DePaul University is a private university located in Chicago, Illinois. DePaul offers undergraduate and graduate programs to more than 21,000 students both in person on its Chicago campuses and through distance and online learning programs.

2. In offering online courses to its students, DePaul requires that many student exams be conducted using an online remote proctoring tool called Respondus Monitor. Through the Respondus Monitor tool, DePaul unlawfully collects, uses, and discloses students’ biometric identifiers and biometric information without the students’ written and informed consent.

DePaul also lacks a legally-compliant written public policy establishing a retention schedule and guidelines for destroying biometric identifiers and biometric information and fails to comply with such policy.

FILED DATE: 3/3/2021 4:08 PM 2021CH01027

3. DePaul's chosen and exclusive remote proctoring tool, 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. DePaul owns, has access to, and possesses this data.

4. Through Respondus Monitor, DePaul 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. Using the Respondus Monitor tool, DePaul is able 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, Inc.'s 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/#c2d2e18638d8>. Relatedly, Duke University has decided not to allow virtual proctoring at this time, in part because of security concerns. *Id.*

5. All the while, students are left in the dark about the vast amount of information their university collects through the Respondus Monitor tool. DePaul does not disclose or obtain

written consent before collecting, capturing, storing, or disseminating users' biometric data.

DePaul also fails to disclose what it does with that biometric data after collection and does not comply with BIPA's retention and destruction requirements for private entities that possess biometric identifiers and biometric information.

6. 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.*

7. Plaintiff John Doe brings this action to enforce his legal rights under Illinois' Biometric Information Privacy Act, 470 ILCS 14/ (“BIPA”), and those of the proposed class of persons he represents.

8. 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.

9. 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).

10. 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).

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

12. 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.*

13. Plaintiff alleges DePaul violated BIPA by, among other things, collecting, capturing, using, storing, and sharing Plaintiff’s and class members’ biometric identifiers or biometric information obtained through the use of Respondus Monitor without informed written consent.

14. DePaul violated BIPA’s requirement that it maintain, disclose, and follow a retention policy that requires DePaul to permanently destroy students’ biometric data obtained through the use of Respondus Monitor once the purpose for collecting such data has been satisfied.

15. DePaul’s 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 Plaintiff’s personal rights and the rights of the class members he represents.

16. A class action is the best means of obtaining redress for DePaul’s wide-scale BIPA violations and is consistent with the fairness and efficiency goals of class actions.

## **JURISDICTION AND VENUE**

17. This Court has subject-matter jurisdiction over this putative class action lawsuit because it arises under Illinois law.

18. The Court has personal jurisdiction over DePaul pursuant to 735 ILCS 5/2-209 because Plaintiff's claims arise out of and relate to DePaul's conduct in the state of Illinois.

19. Venue is proper in this Court under 735 ILCS 5/2-101(2) because the transaction or some part thereof out of which the cause of action arose occurred in Cook County.

## **PARTIES**

20. Plaintiff John Doe is a natural person who resides in Cook County, Illinois.

21. Defendant DePaul University is an Illinois not-for-profit corporation with its principal place of business at 1 E. Jackson Boulevard, Chicago, Illinois 60604 and a registered agent of Kathryn Stieber, 55 E. Jackson Boulevard, Ste. 2200, Chicago, Illinois 60604.

## **FACTUAL BACKGROUND**

### **A. Online and Remote Proctoring**

22. 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 like DePaul have offered online coursework that requires students to take quizzes and exams online.

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

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

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

26. On information and belief, DePaul purchases a license from Respondus, Inc. to integrate Respondus Monitor into DePaul's LMS. *See* DEPAUL UNIVERSITY, <https://offices.depaul.edu/center-teaching-learning/instructional-technology/Pages/default.aspx> (last visited Feb. 26, 2021).

**B. The Respondus Monitor Tool**

27. This lawsuit arises from DePaul's use of the Respondus Monitor tool, a fully automated exam proctoring solution that enables students to take exams online in a *non-proctored* environment.

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

29. Respondus, Inc.'s 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 Dec. 6, 2020).

30. Respondus, Inc.'s 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.*

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

32. 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 Feb. 26, 2021).

33. However, prior to January 21, 2021, the terms of use that students must accept before using Respondus Monitor for DePaul exams say nothing about facial recognition, biometric identifiers, or biometric information, and do not disclose to student users that their biometric identifiers or biometric information will be captured, collected, analyzed, or disseminated to the student’s Institution.<sup>1</sup>

**C. Test-Taking with Respondus Monitor**

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

35. The student first logs into their Institution’s LMS platform and opens a browser.

36. 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**

37. The Monitor Student Terms include two components—terms applicable to (i) the student’s relationship with Respondus, Inc.; 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,

---

<sup>1</sup> On January 21, 2021, Respondus, Inc. 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.



2021, is attached hereto as **Exhibit A** and was previously publicly available on Respondus, Inc.'s website.

38. 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.” (*Id.*)

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

40. 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.

41. 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, Inc. on behalf of the Institution. (*See id.*)

42. These recordings, which the Institution controls, include students' biometric identifiers and biometric information, but, prior to January 21, 2021, that fact was not disclosed in the Monitor Student Terms.

43. The Monitor Student Terms state that Respondus, Inc. “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.*)

44. This “additional data” that Respondus, Inc. generates includes students’ biometric identifiers and biometric information, but, prior to January 21, 2021, that fact was not disclosed in the Monitor Student Terms.

45. 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.*)

46. 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.

47. The Monitor Student Terms additionally state Respondus, Inc. 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.*)

48. 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.

49. 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.*)

50. 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.

51. 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, Inc. or the Institution, whichever occurred first.

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

53. 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.

54. 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**

55. The Monitor Student Terms include two privacy policies—a Privacy and Security Policy (the "Monitor Privacy Policy"<sup>2</sup>), described in the Monitor Student Terms, and the "full Respondus Privacy Policy," incorporated by reference and publicly available on Respondus, Inc.'s website. *See* RESPONDUS, <https://web.respondus.com/privacy-policy/> (last visited Feb. 26, 2021) (the "Respondus Privacy Policy").

---

<sup>2</sup> 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.

**F. The Monitor Privacy Policy**

56. 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.)

57. 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.

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

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

60. 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, Inc. or the Institution, whichever occurred first.

**G. The Respondus Privacy Policy**

61. 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, Inc.’s website is attached hereto as **Exhibit B**. RESPONDUS, <https://web.respondus.com/privacy-policy/> (last visited Feb. 26, 2021).

62. The Respondus Privacy Policy does not disclose that Respondus, Inc. collects student biometric identifiers and biometric information through Respondus Monitor. (*See id.*)

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

#### **H. Other Relevant Monitor Student Terms**

64. 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.)

65. 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.*)

66. The Monitor Student Terms state that students using Respondus Monitor, and thus agreeing to these 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**

67. 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.

68. 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.

69. 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.

70. 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.

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

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

**J. The Monitor Institution Terms**

73. On information and belief, DePaul’s use of Respondus Monitor is subject to Terms of Use applicable to Institutions (the “Monitor Institution Terms”). A copy of these terms is attached hereto as **Exhibit C** and is publicly available on Respondus, Inc.’s website. *See* RESPONDUS, <https://web.respondus.com/tou-monitor-admin/> (last visited Feb. 26, 2021).

74. In the Monitor Institution Terms, Respondus, Inc. discloses to DePaul that “Respondus Monitor analyzes the recordings of student activity as part of an automated proprietary process.” (Ex. C.)

75. Under the Monitor Institution Terms, DePaul is made aware that video recordings DePaul students make and send through Respondus Monitor are accessible to DePaul, its instructors, administrators, and other agents of DePaul. (*Id.*)

76. In the Monitor Institution Terms, DePaul agrees its students’ recordings made while using Respondus Monitor may be used by Respondus, Inc. and may “be shared with researchers (research institutions and/or biometric experts) under contract with Respondus to assist in such research ....” (*Id.*)

77. The Monitor Institution Terms make clear that if DePaul authorizes Respondus, Inc. to share student recordings or personally identifying information of any student with a third party, Respondus, Inc. will do so under the Institution's direction and control. (*Id.*)

78. The Monitor Institution Terms inform DePaul that Respondus Monitor saves all recordings of students for a period of one (1) year but that DePaul has the ability to retain the data for up to an additional four (4) years. (*Id.*)

79. The Monitor Institution Terms inform DePaul that Respondus, Inc. "does not guarantee removal of all traces of any information or data (including recordings) from the Respondus Monitor Services after deletion." (*Id.*)

**K. DePaul's Data Policy**

80. DePaul maintains a publicly-available policy governing "Access to and Responsible Use of Data" on its website. *See* DEPAUL UNIVERSITY, <https://offices.depaul.edu/secretary/policies-procedures/policies/Pages/default.aspx> (follow "Access to and Responsible Use of Data" link) (last accessed Feb. 26, 2021) (the "DePaul Data Policy").

81. The DePaul Data Policy does not disclose that it collects biometric identifiers or biometric information. *Id.*

82. The DePaul Data Policy does not include a retention or destruction policy for biometric identifiers or biometric information that DePaul collects and controls. *Id.*

**L. Plaintiff's Experience with Respondus Monitor**

83. Plaintiff is currently a student at DePaul.

84. Plaintiff pays tuition and other fees to DePaul to take courses and receive credits toward a college degree.

85. Plaintiff is enrolled in a course at DePaul that requires the use of Respondus Monitor for exams.

86. Plaintiff has used Respondus Monitor to take exams for this course.

87. Plaintiff has used Respondus Monitor twice in the past twelve months.

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

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

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

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

92. The context in which Plaintiff 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**

93. Plaintiff brings this action on behalf of a class of all other persons or entities similarly situated (the “Class”).

94. The Class of persons Plaintiff proposes to represent is tentatively defined as:

All persons who took an assessment using Respondus Monitor, as a student of DePaul University in Illinois, at any time during the



five years prior to the filing of this Complaint through January 20, 2021.

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

96. The Class defined above is identifiable through DePaul's business records.

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

98. Individual joinder of these persons is impracticable.

99. Plaintiff is a member of the Class.

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

a. Whether DePaul developed a written policy, available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information collected through Respondus Monitor, when the initial purpose for collecting such identifiers or information has been satisfied or within three (3) years of the individual's last interaction with DePaul, whichever occurs first, and whether DePaul complied with such written policy;

b. Whether DePaul collects, captures, or otherwise obtains Plaintiff's and Class members' biometric identifiers or biometric 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 DePaul discloses or disseminates Plaintiff's and Class members' biometric identifiers or biometric information without Plaintiff's and Class members' consent;

d. Whether DePaul's conduct was negligent;

e. Whether DePaul's conduct was knowing or reckless; and

f. Whether Plaintiff and Class members are entitled to damages for violation of their privacy rights.

101. Plaintiff's claims are typical of the claims of Class members.

102. Plaintiff is an adequate representative of the Class because his interests do not conflict with the interests of the Class, he will fairly and adequately protect the interests of the Class, and he is represented by counsel skilled and experienced in class actions.

103. 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 DePaul.

104. 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.

105. Plaintiff is not aware of any litigation concerning this controversy already commenced by others who meet the criteria for class membership described above.

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

106. Plaintiff repeats the prior allegations of this Complaint and incorporates them by reference herein.

107. DePaul is a "private entity" for purposes of BIPA.

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

109. DePaul 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).

110. DePaul does not comply with any established retention schedule or destruction guideline.

111. DePaul's 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 DePaul is presumed to know these legal requirements. DePaul's conduct is all the more egregious given the current and public discourse in higher education about how online proctoring systems violate students' privacy rights.

112. DePaul's unlawful conduct caused injury to Plaintiff and the proposed Class.

113. Plaintiff and the Class seek damages, attorney's fees, and costs.

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

114. Plaintiff repeats the prior allegations of this Complaint and incorporates them by reference herein.

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

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

117. DePaul 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).

118. DePaul 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).

119. DePaul's unlawful conduct is negligent and reckless because BIPA has governed the collection and use of biometric identifiers and biometric information since 2008, and DePaul is presumed to know these legal requirements. DePaul's conduct is all the more egregious given the current and public discourse in higher education about how online proctoring systems violate students' privacy rights.

120. DePaul's unlawful conduct caused injury to Plaintiff and the proposed Class.

121. Plaintiff and the Class seek damages, attorney's fees, and costs.

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

122. Plaintiff repeats the prior allegations of this Complaint and incorporates them by reference herein.

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

124. DePaul charges students tuition and other fees for academic courses DePaul offers. To complete required course examinations, students are required to use the Respondus Monitor tool.

125. DePaul profits from requiring students to use Respondus Monitor as it allows DePaul to offer online coursework and thereby receive tuition dollars from students.

126. DePaul's unlawful conduct is negligent and reckless because BIPA has governed the collection and use of biometric identifiers and biometric information since 2008, and DePaul is presumed to know these legal requirements. DePaul's conduct is all the more egregious given the current and public discourse in higher education about how online proctoring systems violate students' privacy rights.

127. DePaul's unlawful conduct caused injury to Plaintiff and the proposed Class.

128. Plaintiff and the Class seek damages, attorney's fees, and costs.

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

129. Plaintiff repeats the prior allegations of this Complaint and incorporates them by reference herein.

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

131. DePaul discloses or disseminates students' biometric identifiers or biometric information to its instructors and other agents without the student's consent to the disclosure in violation of 740 ILCS 14/15(d).

132. DePaul's unlawful conduct is negligent and reckless because BIPA has governed the collection and use of biometric identifiers and biometric information since 2008, and DePaul is presumed to know these legal requirements. DePaul's conduct is all the more egregious given

the current and public discourse in higher education about how online proctoring systems violate students' privacy rights.

133. DePaul's unlawful conduct caused injury to Plaintiff and the proposed Class.

134. Plaintiff and the Class seek damages, attorney's fees, and costs.

### **PRAYER FOR RELIEF**

**WHEREFORE**, Plaintiff, individually and on behalf of the Class, prays for the following relief:

- A. Certification of the proposed Class;
- B. Appointment of Plaintiff as representative of the Class;
- C. Appointment of the undersigned counsel as counsel for the Class;
- D. An award to Plaintiff and the Class of damages in excess of \$50,000, as allowed by law; and
- E. Orders granting such other and further relief as the Court deems necessary, just, and proper.

### **JURY TRIAL DEMANDED**

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

Dated: March 3, 2021

Respectfully submitted,

**/s/ Brian K. Murphy**

Brian K. Murphy (IL Atty. No. 6225697;

Cook County No. 37524)

Joseph F. Murray (*pro hac vice* to be filed)

Jonathan P. Misny (*pro hac vice* to be filed)

Murray Murphy Moul + Basil LLP

1114 Dublin Road

Columbus, OH 43215

Telephone: 614.488.0400

Facsimile: 614.488.0401

E-mail: [murphy@mmmb.com](mailto:murphy@mmmb.com)

[murray@mmmb.com](mailto:murray@mmmb.com)

[misny@mmmb.com](mailto:misny@mmmb.com)

Mary C. Turke (*pro hac vice* to be filed)

Samuel J. Strauss (*pro hac vice* to be filed)

Turke & Strauss, LLP

613 Williamson Street, Suite 201

Madison, WI 53703

Telephone: (608) 237-1775

Facsimile: (608) 509-4423

Email: [mary@turkestrauss.com](mailto:mary@turkestrauss.com)

Email: [sam@turkestrauss.com](mailto:sam@turkestrauss.com)

Anthony I. Paronich (*pro hac vice* to be  
filed)

Paronich Law, P.C.

350 Lincoln Street, Suite 2400

Hingham, MA 02043

Telephone: (508) 221-1510

Email: [anthony@paronichlaw.com](mailto:anthony@paronichlaw.com)

*Counsel for Plaintiff*

# ClassAction.org

This complaint is part of ClassAction.org's searchable class action lawsuit database and can be found in this post: [Lawsuit Claims DePaul's Respondus Remote Exam Proctoring Tool Infringed on Ill. Students' Privacy Rights](#)

---