ROB BONTA
Attorney General of California
NICKLAS A. AKERS
Senior Assistant Attorney General
STACEY D. SCHESSER
Supervising Deputy Attorney General
YEN P. NGUYEN (SBN 239095)
Deputy Attorney General
455 Golden Gate Avenue, Suite 11000
San Francisco, CA 94102-7004
Telephone: (415) 510-3497
E-mail: TiTi.Nguyen@doj.ca.gov
Attorneys for The People of the State of California

[EXEMPT FROM FILING FEES PURSUANT TO GOVERNMENT CODE SECTION 6103]

SUPERIOR COURT OF THE STATE OF CALIFORNIA

FOR THE COUNTY OF LOS ANGELES

THE PEOPLE OF THE STATE OF CALIFORNIA,

Plaintiff,

v.

ILLUMINATE EDUCATION, INC., a corporation,

Defendants.

Case No. 25STCV32380

COMPLAINT FOR PERMANENT INJUNCTION, CIVIL PENALTIES, AND OTHER EQUITABLE RELIEF

(CIVIL CODE, §§ 56.06(d), 56.101(a), 56.10(a); BUS. & PROF. CODE, §§ 17200 *et seq.*, 17500 *et seq.*)

Plaintiff, the People of the State of California ("Plaintiff" or the "People"), by and through Rob Bonta, Attorney General of the State of California, bring this action against Illuminate Education, Inc. ("Illuminate" or "Defendant") for violations of California's consumer and privacy laws. The People allege the following facts based on information and belief:

INTRODUCTION

1. From kindergarten through high school, schools play a crucial role in a child's life and development: schools provide an academic education while supporting a child's critical social and healthcare needs. To manage its educational, social, and healthcare obligations, schools must collect and track a vast amount of data about each student's learning and academics,

attendance, behavior, demographics, needs and accommodations, and physical, mental, and emotional health and conditions.

2. A student's record reveals sensitive and private information about a schoolchild's life and development. Protecting this student data is essential, as its exposure can have long-term consequences such as identity theft, personal embarrassment, or reputational or other harm. To help manage their data, schools contract with vendors to store, analyze, and safeguard student records.

3. Illuminate, an education-technology company, is a California company and acts as a vendor with school districts and schools, contracting for data storage and analysis services. Illuminate provides software to monitor and assess student academic progress as well as cloud-based storage of student data, personal information, and medical information.

4. Under California law, Illuminate is required to comply with several state privacy laws in managing this student data: the K-12 Pupil Online Personal Information Protection Act (KOPIPA), the Reasonable Data Security Law, and the Confidentiality of Medical Information Act (CMIA). KOPIPA and the Reasonable Data Security Law mandate a heightened legal obligation to protect student data and personal information from unauthorized access, destruction, use, modification, or disclosure and adhere to reasonable security procedures and practices. And because Illuminate also maintained medical information, such as the medical conditions related to the provision of special education services and accommodations, Illuminate was legally required under the CMIA to protect the confidentiality of that medical information and not disclose it without authorization.

5. In January 2022, Illuminate realized it had a massive breach involving California student data after noticing that some of its software was malfunctioning. After conducting an internal investigation, the company learned that it failed to terminate administrator credentials of a former employee who had left the company three years prior. This failure allowed a threat actor to steal the credentials and use them to access Illuminate's network. The threat actor took advantage of the administrator credentials' high level of privilege to create new accounts and to access, exfiltrate, and delete student data not only from active databases but also backup

databases. The breach impacted forty-nine (49) school districts and millions of students in the state, despite Illuminate's public promises about the reasonableness and adequacy of its data security.

6. Illuminate's failure to secure the student data it had contracted to store and protect violated multiple California laws. Accordingly, the People bring this action against Illuminate for violations of KOPIPA, the Reasonable Data Security Law, and the CMIA, as well as the Unfair Competition Law (UCL) and False Advertising Law (FAL).

PARTIES

7. Plaintiff is the People of the State of California. Plaintiff brings this action by and through Rob Bonta, Attorney General. The Attorney General is authorized by Civil Code section 56.36 to bring actions to enforce the Confidentiality of Medical Information Act, Business and Professions Code sections 17535 and 17536 to bring actions to enforce the False Advertising Law, and Business and Professions Code sections 17204 and 17206 to bring actions to enforce the Unfair Competition Law.

8. Defendant Illuminate Education, Inc., is a California corporation with its principal place of business at 2911 Peach Street, Wisconsin Rapids, WI 54494. Illuminate is a wholly owned subsidiary of Renaissance Learning, Inc.

JURISDICTION AND VENUE

9. Defendant has transacted business and continues to transact business within the State of California, including the County of Los Angeles, at all times relevant to this Complaint. The violations of law alleged in this Complaint occurred in the County of Los Angeles, and elsewhere in the State of California.

FACTUAL ALLEGATIONS

10. Illuminate offered software called "IO Suite," which included cloud-based storage and was designed to maintain student data, such as information related to academics and behavior, enrollment, demographics, special education and accommodations, and medical information. IO Suite received data from schools and school districts, as well as data that students, parents, teachers, administrators, and staff manually entered into the IO Suite. IO Suite

used that data to help educators monitor and assess learning, identify and manage academic and social-emotional behavior needs, and guide improvement.

11. On or around December 28, 2021, a threat actor used the credentials of a former Illuminate employee—who had left the company in 2017—to access the segment of Illuminate's network that operated IO Suite. The former employee had the highest level of administrator privileges for IO Suite. Using this former employee's administrator credentials, the threat actor created new account credentials to enable future access to Illuminate's network and IO Suite. The threat actor then accessed IO Suite databases in order to exfiltrate and delete student data. At the time, IO Suite databases and backup databases were stored in the same segment of Illuminate's network. As a result, the threat actor also accessed IO Suite backup databases and exfiltrated and deleted student data.

12. At the time of the breach, Illuminate used a threat detection tool that monitored for anomalous activity in the segment of Illuminate's network that operated IO Suite. This tool, however, lacked the capability to send alerts to security personnel once it flagged an issue. Illuminate did not implement a complementary tool that would send alerts when the monitoring tool detected anomalous activity, and it did not review the monitoring tool's logs. As a result, Illuminate was unaware that the monitoring tool had identified over forty anomalous events after the threat actor had accessed Illuminate's network and IO Suite databases that were later associated with the threat actor. Separately, Illuminate generated its own logs of user activity but never analyzed these logs to look for potentially suspicious or malicious activity.

13. Illuminate only learned of a problem when it was alerted that IO Suite was malfunctioning on or around January 8, 2022. Illuminate investigated the problem, identified the cybersecurity threat, and removed the threat actor from its systems.

14. The impacted student data included highly sensitive personal information and medical information. The student data included, among other information: name, birth date, email address, information related to the student's academics and behavior, enrollment, demographics (e.g., race), and whether the student received special education services or reasonable accommodations [Y/N] along with relevant contextual information (such as if a child

had autism). Also compromised was information that could reflect a student's medical condition but insofar as it relates to the provision of special education services; for example, a code reflecting that the student had a traumatic brain injury. However, not all data points were at issue for every student impacted by the breach impacting at least forty-nine (49) school districts all over California.

15. Illuminate's security procedures and practices were inadequate to protect the personal information, medical information, and student data of California residents from unauthorized access, acquisition, destruction, or disclosure in three specific ways.

16. First, Illuminate did not have reasonable account management and access controls. Contrary to basic security, Illuminate did not terminate the credentials of an employee who had left the company at least three years prior to the breach. This component of security is especially critical when the former employee had administrator credentials with high level of privileges. Further, Illuminate was unaware of this failure because Illuminate did not conduct audits to check that it had terminated the credentials of former employees or that all its valid credentials belonged only to current employees. Illuminate also did not monitor account creation and use, including the creation of new credentials or removal of default security requirements for new credentials. In addition, it did not implement measures to protect credentials and did not provide employee training on properly securing their credentials.[1]

17. Second, Illuminate failed to monitor and alert for suspicious logins and activity within its network. At the time of the data breach, Illuminate did not have real-time alerts and instead relied on logging user access and activity. However, Illuminate did not analyze any of its logs for suspicious or unauthorized activity.

18. Third, Illuminate did not secure its backup databases separately from its active databases. The entire purpose of a backup is to allow the recovery of data in case of data loss, corruption, system failure, or disaster to the active database. Thus, it is basic security and

[1] The former employee's credentials were an access key pair, which consists of a public key and a corresponding private key. The security of access key pairs largely depends on protecting the private key and keeping it secret, though it is a good practice to also protect the public key. It is unknown how the threat actor obtained the employee's access keys.

common sense to save and secure backups separate from active databases. Otherwise, any failure related to the active databases—whether failure of hardware or failure of security resulting in unauthorized access—would also affect the backup, negating the purpose of a backup. Illuminate's failure allowed the threat actor to compromise both the active and backup databases.

19. At all times relevant to this action, Illuminate represented that it took steps to prevent unauthorized access and disclosure of information, including that its measures "meet or exceed the requirements of applicable federal and state law." Illuminate also posted that it had signed the Student Privacy Pledge, in which it agreed to "maintain a comprehensive security program that is reasonably designed to protect the security, privacy, confidentiality and integrity of student personal information against risks[.]" The Future of Privacy Forum, one of the creators and administrators of the Student Privacy Pledge, dropped Illuminate from the list of signatories as a result of the breach.

FIRST CAUSE OF ACTION

VIOLATIONS OF THE UNFAIR COMPETITION LAW

(BUSINESS & PROFESSIONS CODE SECTION 17200 ET SEQ.)

20. The People realleged and incorporate by reference each of the paragraphs above, as well as the paragraphs below in the Second and Third Causes of Action, as though fully set forth herein.

21. Illuminate has engaged in unlawful, unfair, or fraudulent acts or practices, which constitute unfair competition within the meaning of Section 17200 of the Business and Professions Code. Illuminate's violation of the Section 17200 of the Business and Professions Code include but are not limited to:

a. Violation of the K-12 Pupil Online Personal Information Protection Act (Bus. & Prof. Code, § 22584). Illuminate is an operator of an online service, and/or online application and designed and marketed its service and application for K-12 school purposes. (§ 22584, subd. (a).) Illuminate failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the covered information it maintained as described in Paragraphs 5 and 15-1817.

(§ 22584, subd. (d)(1).) Illuminate also failed to protect the covered information it maintained in IO Suite on behalf of California school districts and schools from unauthorized access, destruction, use, modification, or disclosure. (*Ibid*.)

b. Violation of Civil Code section 1798.81.5. Illuminate is a business that maintains personal information, which includes medical information, about a California resident. Illuminate failed implement and maintain reasonable security procedures and practices appropriate to the nature of the personal information it maintained and to protect the personal information from unauthorized access, destruction, use, modification, or disclosure as described in Paragraphs 5 and 15-18.

c. Violation of the California Online Privacy Protection Act (CalOPPA, Bus. & Prof. Code, § 22575 *et seq.*). Illuminate is an operator of a commercial online service that collects personally identifiable information through the Internet about individual consumers residing in California who use its commercial online service. (§ 22575, subd. (a).) Illuminate's failure to comply with their posted privacy policy was negligent and material. (§ 22576, subd. (b).)

d. Violations of the Confidentiality of Medical Information Act (Civ. Code, § 56 *et seq*.), as alleged in the Second Cause of Action.

e. Violation of California consumers' right to privacy as established in article I, section 1 of the California Constitution by failing to protect student data, personal information, and medical information from unauthorized access, destruction, use, modification, or disclosure, failing to preserve the confidentiality of medical information, and permitting the unauthorized disclosure of medical information.

f. Violation of Business and Professions Code section 17500 as alleged in the Third Cause of Action.

g. Engaging in unfair business acts or practices, fraudulent acts or practices, and unfair, deceptive, untrue or misleading advertising including but not limited to Illuminate's data security practices at the time of the data breach and statements regarding its security measures in place at the time of the data breach.

SECOND CAUSE OF ACTION

VIOLATIONS OF THE CONFIDENTIALITY OF MEDICAL INFORMATION ACT (CIVIL CODE SECTION 56 ET SEQ.)

22. The People realleged and incorporate by reference each of the paragraphs above as though fully set forth herein.

23. Illuminate is deemed a provider of health care under Civil Code section 56.06, subdivision (a), because Illuminate is organized for the purpose of maintaining medical information in order to make the information available to schools, school districts, and students at their request, for purposes of allowing schools, school districts, and students to manage the student's information, or for the diagnosis and treatment of the student.

24. Illuminate is deemed a provider of health care under Civil Code section 56.06, subdivision (b), because Illuminate offers software to consumers that is designed to maintain medical information in order to make the information available to schools, school districts, and the student at their request, for the purposes of allowing schools, school districts, and students to manage the student's information, or for the diagnosis, treatment, or management of a medical condition of the student.

25. Because Illuminate is deemed a provider of healthcare under Civil Code section 56.06, subdivisions (a) and/or (b), Illuminate is subject to the requirements of the CMIA and obligated under Civil Code section 56.06, subdivision (d), to maintain the same standards of confidentiality required of a provider of health care with respect to medical information it maintains.

26. Civil Code section 56.10, subdivision (a), prohibits a provider of health care from disclosing medical information without first obtaining an authorization, unless a statutory exception applies.

27. Civil Code section 56.101, subdivision (a), requires that every provider of health care "who creates, maintains, preserves, stores, abandons, destroys, or disposes of medical information shall do so in a manner that preserves the confidentiality of the information contained therein."

28. Illuminate permitted a threat actor to access the IO Suite databases and thus access, acquire, modify, and delete medical data without the students' authorization. No statutory exception applied. As a result, Illuminate violated Civil Code section 56.10, subdivision (a).

29. The threat actor's access, acquisition, modification, and deletion of medical data in the IO Suite databases was a result of Illuminate's failure to maintain, preserve, and store medical information in a manner that preserves the confidentiality of the information. Furthermore, this failure was negligent. As a result, Illuminate violated Civil Code section 56.06, subdivision (d), and 56.101, subdivision (a).

30. Illuminate also negligently disclosed medical information in violation of Civil Code section 56.36, subdivision (c)(1), through the unauthorized disclosure and access by the threat actor.

THIRD CAUSE OF ACTION

VIOLATIONS OF THE FALSE ADVERTISING LAW

(BUSINESS AND PROFESSIONS CODE SECTION 17500 ET SEQ.)

31. The People realleged and incorporate by reference each of the paragraphs above as though fully set forth herein.

32. Illuminate has engaged in acts or practices that constitution violations of Business and Professions Code section 17500 et seq. by making or disseminating, or causing to be made or disseminated, untrue or misleading statements with the intent to induce members of the public to use Illuminate's services or products.

33. Illuminate's untrue or misleading statements include, but are not limited to, its statements regarding its security measures in place at the time of the data breach.

34. At the time these representations were made, Illuminate knew or by the exercise of reasonable care should have known that these representations were untrue or misleading.

PRAYER FOR RELIEF

WHEREFORE, the People pray for judgment as follows:

35. Pursuant to Business and Professions Code section 17203, that the Court enter all

orders necessary to prevent Illuminate, their successors, agents, representatives, employees, and all person who act in concert with Illuminate from engaging in any act or practice that constitutes unfair competition in violation of Business and Professions Code section 17200, including, but not limited to, alleged in this Complaint;

36. Pursuant to Business and Professions Code section 17535, that the Court enter all orders necessary to prevent Illuminate, their successors, agents, representatives, employees, and all person who act in concert with Illuminate from making any untrue or misleading statements in violation of Business and Professions Code section 17500, including, but not limited to, alleged in this Complaint;

37. Pursuant to Business and Professions Code section 17206, that the Court assess a civil penalty of Two Thousand Five Hundred Dollars ($2,500) for each violation of Business and Professions Code section 17200, as proved at trial.

38. Pursuant to Civil Code section 56.36, subdivision (c)(1), that the Court assess a civil penalty of Two Thousand Five Hundred Dollars ($2,500) for each violation of Civil Code sections 56.06, subdivision (d), 56.101, subdivision (a), and 56.10, subdivision (a), as proved at trial;

39. Pursuant to Business and Professions Code section 17536, that the Court assess a civil penalty of Two Thousand Five Hundred Dollars ($2,500) for each violation of Business and Professions Code section 17500, as proved at trial.

40. The People recover their cost of suit herein, including costs of investigation;

41. That the People receive all other relief to which they are legally entitled; and

42. For such other and further relief as the Court deems just and proper.

Dated: November 6, 2025

Respectfully submitted,

ROB BONTA
Attorney General of California

YEN P. NGUYEN
Deputy Attorney General
Attorneys for The People of the State of California