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) 510-4400
Fax: (415) 703-5480
E-mail: TiTi.Nguyen@doj.ca.gov

Attorneys for the People of the State of California

SUPERIOR COURT OF THE STATE OF CALIFORNIA

FOR THE COUNTY OF LOS ANGELES

UNLIMITED JURISDICTION

THE PEOPLE OF THE STATE OF CALIFORNIA, Plaintiff, **v.** **ILLUMINATE EDUCATION, INC.,** Defendant.	Case No. **[PROPOSED] FINAL JUDGMENT AND PERMANENT INJUNCTION**

Plaintiff, the People of the State of California ("the People" or "Plaintiff"), appearing through its attorney, Rob Bonta, Attorney General of the State of California, by Yen P. Nguyen, Deputy Attorney General, and Stacey D. Schesser, Supervising Deputy Attorney General, and Defendant Illuminate Education, Inc. ("DEFENDANT" or "ILLUMINATE"), appearing through its attorney, Christopher W. Keegan, of Kirkland & Ellis LLP, having stipulated to the entry of this Final Judgment and Permanent Injunction ("Judgment") by the Court without the taking of proof and without trial or adjudication of any fact or law, without this Judgment constituting evidence of or an admission by ILLUMINATE regarding any issue of law or fact alleged in the

Complaint on file, and without ILLUMINATE admitting any liability, and with all parties having waived their right to appeal, and the Court having considered the matter and good cause appearing:

IT IS HEREBY ORDERED, ADJUDGED, AND DECREED THAT:

I. PARTIES AND JURISDICTION

1. This Court has jurisdiction over the allegations and subject matter of the People's Complaint filed in this action, and the parties to this action; venue is proper in this County; and this Court has jurisdiction to enter this Judgment. This Judgment is entered pursuant to and subject to Business and Professions Code sections 17200 et seq. and 17500 et seq.

II. DEFINITIONS

The following terms in this Judgment shall have these meanings:

2. "DATA BREACH" means the security incident discovered by ILLUMINATE on or about January 8, 2022, in which intruder(s) gained unauthorized access to portions of the ILLUMINATE NETWORK that stored COVERED INFORMATION, and which impacted students in over a hundred schools or school districts in California.

3. "COVERED INFORMATION" has the same meaning as provided in Business & Professions Code section 22584, subdivision (a)(2), as it relates to information received by ILLUMINATE in connection with an ILLUMINATE PRODUCT.

4. "DEFENDANT" or "ILLUMINATE" means Illuminate Education, Inc., its wholly owned, integrated, and operated subsidiaries and divisions, successors and assigns, doing business in the United States.

5. "EFFECTIVE DATE" means the date that DEFENDANT is served with notice that the Judgment has been entered.

6. "ILLUMINATE NETWORK" means the networking equipment, databases or data stores, applications, servers, workstations, devices, and endpoints that: (a) are capable of using and sharing software, data, and hardware resources; (b) are owned, operated, or controlled by ILLUMINATE; and (c) collect, process, store, or have access to COVERED INFORMATION.

7. "ILLUMINATE USER" shall mean any employee, representative, contractor, subcontractor, or agent of ILLUMINATE for whom ILLUMINATE has created a user account and credentials to access the ILLUMINATE NETWORK.

8. "ILLUMINATE PRODUCT" shall mean eSchoolData, eduCLIMBER, DnA, FastBridge, and SchoolCity, and includes all versions and revisions, and any similar future product offered by Illuminate Education, Inc. or its wholly owned, integrated, and operated subsidiaries and divisions.

9. "SECURITY INCIDENT" means any compromise of the security, confidentiality, integrity, or availability of COVERED INFORMATION stored within, accessed, or transmitted through the ILLUMINATE NETWORK that results in the unauthorized acquisition of COVERED INFORMATION collected, processed, transmitted, stored, or disposed of by ILLUMINATE.

III. INJUNCTIVE PROVISIONS

10. Nothing in this Judgment alters the requirements of state or federal law to the extent they offer greater protection to California residents.

11. The injunctive provisions of this Judgment shall apply to: (a) DEFENDANT; (b) its directors, officers, employees; (c) its subsidiaries and divisions; and (d) its successors and the assigns of all or substantially all of the assets of the business of Illuminate Education, Inc. or its wholly owned, integrated, and operated subsidiaries and divisions.

12. The injunctive terms contained in this Judgment are being entered pursuant to Business and Professions Code section 17203.

COMPLIANCE WITH LAW

13. ILLUMINATE shall comply with all applicable provisions in:

a. K-12 Pupil Online Privacy Information Protection Act (KOPIPA), Business and Professions Code section 22584;

b. California Online Privacy Protection Act (CalOPPA), Business & Professions Code sections 22575-22577;

c. Unfair Competition Law (UCL), Business and Professions Code section 17200, including in connection with its collection, maintenance, and safeguarding of COVERED INFORMATION; and

d. False Advertising Law (FAL), Business and Professions Code section 17500, including to the extent it represents how it maintains and/or protects the privacy, security, or integrity of COVERED INFORMATION.

DATA BREACH NOTIFICATION

14. For any SECURITY INCIDENT that occurs after the EFFECTIVE DATE, ILLUMINATE shall notify the school, school district, or other customer of ILLUMINATE on whose behalf ILLUMINATE processes the COVERED INFORMATION (the "OWNER"), in accordance with the terms of its applicable contract with the OWNER. If the OWNER determines that notices to California residents are required, ILLUMINATE shall offer to provide the OWNER of the COVERED INFORMATION assistance in notifying the affected California resident, or their parent(s) or legal guardian(s) if the affected California resident is a minor. ILLUMINATE shall cover the costs of its assistance and the notification in accordance with the terms of its applicable contract with the OWNER.

15. If ILLUMINATE provides notification pursuant to Paragraph 14 to an affected California resident, or their parent(s) or legal guardian(s) if the California resident is a minor, the notification shall conform to the requirements in Civil Code section 1798.82, subdivision (d), except as instructed by the OWNER for notices that are not required under Civil Code section 1798.82, subdivision (d).

INFORMATION SECURITY PROGRAM

16. Within one hundred and eighty (180) days after the EFFECTIVE DATE, ILLUMINATE shall implement, and thereafter shall maintain, regularly review and revise, and comply with an information security program, including the Specific Safeguards and Controls, set forth in Paragraphs 18 23- 42 below (collectively, "Information Security Program") designed to protect the security, integrity, availability, and confidentiality of the COVERED

INFORMATION that ILLUMINATE collects, stores, processes, uses, transmits, and/or maintains.

17. ILLUMINATE's Information Security Program shall be documented and shall contain administrative, technical, and physical safeguards appropriate to:

a. The size and complexity of ILLUMINATE's operations;

b. The nature and scope of ILLUMINATE's activities; and

c. The sensitivity of the COVERED INFORMATION that ILLUMINATE collects, stores, processes, uses, transmits, and/or maintains.

18. The Information Security Program shall be designed to:

a. Protect the security, integrity, availability, and confidentiality of COVERED INFORMATION;

b. Protect against credible threats that are known or reasonably foreseeable to the security, integrity, availability, and confidentiality of COVERED INFORMATION;

c. Protect COVERED INFORMATION from unauthorized access, destruction, use, modification, or disclosure;

d. Restrict access to COVERED INFORMATION based on necessity and job function;

e. Accurately and thoroughly assess the potential risks and vulnerabilities to the security, integrity, availability, and confidentiality of COVERED INFORMATION;

f. Assess the sufficiency and effectiveness of any safeguards in place to control the risks and vulnerabilities identified in subsection (e);

g. Adjust the safeguards and Information Security Program in light of the results of the assessments in subsections (e) and (f); and

h. Provide employee training, at least annually for existing employees and conduct an initial training for all new employees, concerning the proper handling and protection of COVERED INFORMATION.

19. ILLUMINATE may satisfy the implementation and maintenance of the Information Security Program and the safeguards required by this Judgment through review,

maintenance, and, if necessary, updating, of an existing information security program or existing safeguards, provided that such existing information security program or safeguards meet the requirements set forth in this Judgment.

20. Illuminate shall appoint a qualified individual who shall be responsible for implementing, maintaining, and monitoring the Information Security Program ("Chief Information Security Officer" or "CISO"). The CISO shall have the background and expertise in information security appropriate to the level, size, and complexity of her/his role in implementing, maintaining, and monitoring the Information Security Program. At a minimum, the CISO shall also:

a. Be or become knowledgeable of relevant and applicable state and federal privacy and data security statutes;

b. Ensure ILLUMINATE develops, implements, and maintains privacy and security privacy and procedures for ILLUMINATE that are consistent with applicable state and federal privacy laws;

c. Oversee ILLUMINATE's compliance with such policies and procedures; and

d. Oversee the implementation, maintenance, and monitoring of the Information Security Program.

The CISO shall have authority and autonomy to perform these responsibilities and to report any significant privacy or security concerns to the Chief Executive Officer or other ILLUMINATE executives.

21. ILLUMINATE shall provide notice of the requirements of this Judgment to the employees of ILLUMINATE's Information Security organization and shall implement training on the requirements of this Judgment to those employees. ILLUMINATE shall provide the training required under this Paragraph to such employees within one hundred eighty (180) days of the EFFECTIVE DATE of this Judgment or prior to their starting their responsibilities for implementing, maintaining, or monitoring the Information Security Program.

22. ILLUMINATE shall ensure that the Information Security Program receives reasonable resources for carrying out the Information Security Program.

SPECIFIC SAFEGUARDS AND CONTROLS

23. **Zero Trust Architecture:** ILLUMINATE shall consider and adopt where reasonably feasible the principals of zero trust architecture throughout the ILLUMINATE NETWORK, including:

a. Regularly monitoring, logging, and inspecting network traffic, including log-in attempts, through the implementation of hardware, software, or procedural mechanisms that record and evaluate such activity;

b. Authorizing and authenticating relevant device, user, and network activity within the ILLUMINATE NETWORK; and

c. Requiring appropriate authorization and authentication prior to any user's access to the ILLUMINATE NETWORK.

24. **Access Control and Account Management:** ILLUMINATE shall implement and maintain appropriate controls to manage access to and use of all ILLUMINATE USER accounts with access to COVERED INFORMATION, including individual accounts, administrator accounts, service accounts, and vendor accounts.

a. ILLUMINATE shall implement and maintain adequate access controls, processes, and procedures, the purpose of which shall be to grant access to the ILLUMINATE NETWORK only after the ILLUMINATE USER has been properly identified, authenticated, reviewed, and approved.

b. ILLUMINATE shall as soon as practicable, and within twenty-four (24) hours, terminate access privileges for all ILLUMINATE USER whose access to the ILLUMINATE NETWORK is no longer required or appropriate.

c. ILLUMINATE shall regularly inventory the ILLUMINATE USERS who have access to the ILLUMINATE NETWORK in order to review and determine whether or not such access remains necessary or appropriate. ILLUMINATE shall regularly compare

termination lists to user accounts to ensure access privileges have been appropriately terminated. At a minimum, such review shall be performed on a quarterly basis.

d. ILLUMINATE shall implement and maintain adequate administration processes and procedures to store and monitor the account credentials and access privileges of ILLUMINATE USERS who have privileges to design, maintain, operate, and update the ILLUMINATE NETWORK.

25. **Authentication:** ILLUMINATE shall implement and maintain reasonable policies and procedures requiring the use of authentication for ILLUMINATE USERS in accordance with industry standards, where commercially feasible, including as appropriate under industry standards, the use of strong passwords or public-private key pairs, password or key pair rotation, and ensuring that stored passwords and private keys are protected from unauthorized access.

26. **Privileged Account Management:**

a. ILLUMINATE shall limit access to COVERED INFORMATION to ILLUMINATE USERS accessing the ILLUMINATE NETWORK on a least-privileged basis.

b. ILLUMINATE shall implement and maintain reasonable controls to secure use of privileged credentials by ILLUMINATE USERS, such as through a Privileged Access Management tool or reasonably equivalent technology that vaults and rotates elevated credentials in places where privileged access credentials are required. Administrators shall be required to use Multi-Factor Authentication or reasonably equivalent technology to gain access to their safe within the vault to retrieve their credentials.

27. **Remote Access / Multi-Factor Authentication:** ILLUMINATE shall require the use of Multi-Factor Authentication or reasonably equivalent technology for all ILLUMINATE USER remote access to the ILLUMINATE NETWORK.

28. **Logging & Monitoring:** ILLUMINATE shall develop, implement, and maintain reasonable policies and procedures designed to properly log and monitor the ILLUMINATE NETWORK. At a minimum:

a. ILLUMINATE shall employ tools such as a Security Information and Event Monitoring solution ("SIEM") (or a reasonably equivalent technology), among others, to log and monitor network traffic to detect and respond to SECURITY INCIDENTS.

b. ILLUMINATE shall take reasonable steps to properly configure and regularly update or maintain the SIEM (or a reasonably equivalent technology) used pursuant to subsection (a) and shall take reasonable steps to adequately log system activity and identify potential SECURITY INCIDENTS for review. Using the SIEM (or a reasonably equivalent technology), ILLUMINATE shall actively review and analyze in real-time the logs of system activity and reasonably follow-up with respect to SECURITY INCIDENTS.

c. ILLUMINATE shall maintain logs in conformance with industry standards and all applicable laws.

d. In addition to the requirements set forth in subparagraphs (a) through (c) of this Paragraph, ILLUMINATE shall develop, implement, and maintain defined and specific policies and procedures with respect to logging and monitoring of the database(s) involved in the DATA BREACH and any database (or set of databases) that collect, process, transmit, and/or store COVERED INFORMATION. At a minimum:

i. ILLUMINATE shall deploy an appropriate database activity monitoring tool or a reasonably equivalent technology in the database(s) involved in the DATA BREACH and any database (or set of databases) that ILLUMINATE uses to collect, process, transmit, and/or store COVERED INFORMATION, to the extent it is commercially available.

ii. The monitoring of such database(s) shall include commercially reasonable query categories available in a database activity monitoring tool or reasonable equivalent issued to the relevant database(s).

iii. The monitoring of such database(s) shall be performed by appropriately trained or experienced personnel.

e. ILLUMINATE shall create a formalized procedure to track SECURITY INCIDENTS and alerts on privileged user queries on a regular basis and document identified issues and necessary action items.

29. **Encryption:** ILLUMINATE shall develop, implement, maintain, regularly review, and revise policies and procedures to encrypt COVERED INFORMATION at rest and in transit as reasonable and appropriate, and in accordance with applicable law.

30. **Unauthorized Applications:** ILLUMINATE shall maintain controls designed to identify and protect against the execution or installation of unauthorized applications on the ILLUMINATE NETWORK, such as whitelisting.

31. **Protecting Backup Databases:** ILLUMINATE shall develop, implement, and maintain reasonable policies and procedures designed to protect backup databases that collect, process, or store COVERED INFORMATION from unauthorized access, destruction, use, modification, or disclosure. At a minimum:

a. The backup databases shall not be within the same network segment as the original databases.

b. ILLUMINATE shall implement and maintain reasonable controls to manage access to backup databases.

32. **Risk Assessments:** ILLUMINATE shall develop, implement, and maintain a risk assessment program to identify, address, and, as appropriate, remediate cybersecurity risks affecting the ILLUMINATE NETWORK. At a minimum, ILLUMINATE shall have an annual cybersecurity risk assessment performed by an independent third party. The assessment shall include assessment of all reasonably anticipated, internal and external risks to the security, confidentiality, or availability of COVERED INFORMATION collected, processed, transmitted, stored, or disposed of by ILLUMINATE, excluding COVERED INFORMATION contained in legal documents and analyses that ILLUMINATE reasonably asserts are exempt from disclosure under legally-recognized privilege. Such reports shall be maintained by the CISO and be made available for inspection by the Third-Party Assessor described in Paragraph 43 of this Judgment.

33. **Vulnerability Management**: ILLUMINATE shall develop, implement, and maintain vulnerability scanning or a reasonably equivalent technology and remediation.

34. **Penetration Testing**: ILLUMINATE shall develop, implement, and maintain a penetration testing program designed to identify, assess, and remediate security vulnerabilities

within the ILLUMINATE NETWORK, which shall include annual external penetration tests or a reasonably equivalent technology and adequate remediation of vulnerabilities revealed by such testing. ILLUMINATE shall develop, implement, and maintain a penetration testing program and shall perform annual internal penetration tests. The reports of such external and internal penetration tests shall be maintained by the CISO for a period of not less than six (6) years and be made available for inspection by the Third-Party Assessor described in Paragraph 43 of this Judgment.

35. **Email Filtering and Phishing Solutions**: ILLUMINATE shall maintain email protection and filtering solutions for all ILLUMINATE email accounts, including email spam, phishing attacks, and anti-malware or a reasonably equivalent technology.

36. **Employee Training:** In addition to the requirements set forth in Paragraph 18(h) above, ILLUMINATE shall conduct an initial training for all new employees and, on at least an annual basis, train existing employees concerning its information privacy and security policies, the proper handling and protection of COVERED INFORMATION, and disciplinary measures for violation, up to and including termination. At a minimum, ILLUMINATE's new employee and annual training shall cover:

a. Cybersecurity threats including social engineering (such as phishing), malware, disinformation, and pretexting;

b. Information security; and

c. Privacy.

37. **Network Sensors:** ILLUMINATE shall deploy network sensors or a reasonably equivalent technology to detect attempts to communicate from the ILLUMINATE NETWORK to known malicious IP addresses.

38. **Endpoint Detection and Response:** ILLUMINATE will implement, maintain, and monitor controls designed to provide real-time notification of malicious systems modifications and anomalous systems activity in the ILLUMINATE NETWORK.

39. **Intrusion Detection and Prevention Solution(s):** ILLUMINATE shall develop, implement, and maintain an intrusion detection and prevention solution to assist in detecting and preventing unauthorized access to the ILLUMINATE NETWORK.

40. **Exfiltration Prevention:** ILLUMINATE shall develop, implement, and maintain technology to detect and prevent unauthorized data exfiltration from the ILLUMINATE NETWORK.

41. ILLUMINATE shall provide a reminder to the OWNER on whose behalf ILLUMINATE processes COVERED INFORMATION that they should perform a review of the stored COVERED INFORMATION. The reminder shall include:

a. A description of the products or services that ILLUMINATE provides to the OWNER of the COVERED INFORMATION;

b. A description of the types or categories of COVERED INFORMATION that ILLUMINATE generally collects, processes or stores for each ILLUMINATE PRODUCT used by the OWNER;

c. ILLUMINATE's obligations with respect to the retention and deletion of COVERED INFORMATION; and

d. The actions the OWNERS may take in the event they no longer need to retain the COVERED INFORMATION, and any explanation, if applicable, that such action may affect the continued use or functionality of the product.

The reminder shall occur at each new contract or renewal between ILLUMINATE and an OWNER of COVERED INFORMATION, under which ILLUMINATE processes COVERED INFORMATION. If the term of the contract is more than four (4) years, then the reminder shall occur at least once every two (2) years.

42. The obligations and other provisions of this Judgment set forth in Paragraphs 23 - 41 shall expire at the conclusion of a seven (7) year period after the Effective Date of this Judgment, unless they have expired at an earlier date pursuant to their specific terms.

ASSESSMENT AND REPORTING REQUIREMENTS

43. **Third-Party Assessment:** ILLUMINATE must conduct annual assessments of its general data security practices, as well as its compliance with the terms of this Judgment (the "Third-Party Assessment"). The Third-Party Assessments required by this Paragraph will be conducted by an independent third-party (the "Third-Party Assessor").

a. The Third-Party Assessor must be a Certified Information Systems Security Professional ("CISSP") or a Certified Information Systems Auditor ("CISA"), or a similarly qualified person or organization and have at least five (5) years of experience evaluating the effectiveness of computer system security or information system security.

b. The reporting period for the Third-Party Assessments must cover: (1) the first one hundred and eighty (180) days after the EFFECTIVE DATE for the initial Third-Party Assessment; and (2) each one-year period thereafter for five (5) years after the EFFECTIVE DATE for the annual Third-Party Assessments.

c. The findings of the Third-Party Assessment must be documented in an annual report (the "Third-Party Assessor's Report"). The Third-Party Assessor's Reports must:

i. Identify the specific administrative, technical, and physical safeguards maintained by ILLUMINATE;

ii. Document the extent to which the identified administrative, technical and physical safeguards are appropriate considering ILLUMINATE's size and complexity, the nature and scope of ILLUMINATE's activities, and the sensitivity of the COVERED INFORMATION maintained by ILLUMINATE;

iii. Assess and certify the extent to which the administrative, technical, and physical safeguards that have been implemented by ILLUMINATE meet the requirements of the Information Security Program; and

iv. Specifically review and evaluate ILLUMINATE's compliance with the access control and account management requirements set forth in Paragraph 24; the authentication requirements set forth in Paragraph 25; the privileged account management requirements set forth in Paragraph 26; the remote access and Multi-Factor authentication

requirements set forth in Paragraph 27; the logging and monitoring requirements set forth in Paragraph 28; the requirements with respect to backup database protections set forth in Paragraph 31; and the exfiltration prevention requirements set forth in Paragraph 40.

d. Each Third-Party Assessment must be completed within sixty (60) days after the end of the reporting period to which the Third-Party Assessment applies. ILLUMINATE must provide a copy of the Third-Party Assessor's Report to the California Attorney General's Office within ten (10) days of the completion of the Third-Party Assessment.

44. **SECURITY INCIDENT Reporting:** ILLUMINATE shall inform the Attorney General's Office, as set forth in Paragraph 51, of any SECURITY INCIDENT involving COVERED INFORMATION of more than 500 California residents in the most expedient time possible and without unreasonable delay.

45. All reports, reviews, and sharing of information pursuant to this Judgment shall be treated as confidential and as exempt from disclosure under the relevant public records laws, including California Government Code § 7920.000 et seq.

IV. MONETARY PROVISIONS

46. ILLUMINATE shall pay the Attorney General the amount of $3,250,000 in two (2) installments. Payment shall be made by wire transfer to the California Attorney General's Office pursuant to instructions provided by the California Attorney General's Office, with the first installment paid no later than thirty (30) days after the Effective Date and the second installment paid no later than ninety (90) days after payment of the first installment. These funds, and any interest accrued thereon, will be allocated and used by the Attorney General in accordance with section 17206 of the Business and Professions Code.

47. Except as otherwise expressly provided herein, each party shall bear its own attorneys' fees and costs.

V. ADDITIONAL GENERAL PROVISIONS

48. This Court retains jurisdiction of this matter for purposes of construction, modification, and enforcement of this Judgment.

49. Nothing in this Judgment shall be construed as relieving DEFENDANT of its obligations to comply with all state and federal laws, regulations, or rules, or as granting permission to engage in any acts or practices prohibited by such law, regulations, or rule.

50. DEFENDANT shall use reasonable efforts to notify its officers, directors, and employees responsible for carrying out and effecting the terms of this Judgment and the requirements therein.

51. Notices and reports under this Judgment shall be served by email and regular mail as follows:

To the People or People's counsel:

Yen P. (TiTi) Nguyen
Consumer Law Section—Privacy Unit
California Attorney General's Office
455 Golden Gate Ave., Suite 11000
San Francisco, California 94102-7004
Email: TiTi.Nguyen@doj.ca.gov

To DEFENDANT or DEFENDANT'S counsel:

Ted Wolf
Renaissance Learning, Inc.
2911 Peach Street
Wisconsin Rapids, WI 54494
Email: ted.wolf@renaissance.com

with copy to:
Email: neal.dittersdorf@renaissance.com

Lisa Madigan
Kirkland & Ellis LLP
333 West Wolf Point Plaza
Chicago, IL 60654
Email: lisa.madigan@kirkland.com

52. This Judgment shall take effect immediately upon entry thereof.

53. The clerk is ordered to enter this Judgment forthwith.

ORDERED AND ADJUDGED at Los Angeles, California, this ___ day of _____, 2025.

_____
Judge of the Superior Court