ATTORNEY GENERAL OF THE STATE OF NEW YORK
BUREAU OF INTERNET & TECHNOLOGY

In the Matter of

Assurance No. 25-057

Investigation by
LETITIA JAMES,
Attorney General of the State of New York, and by
BETTY A. ROSA
Commissioner of Education of the State of New York, of

ILLUMINATE EDUCATION, INC.,

Respondent.

ASSURANCE OF DISCONTINUANCE

The Office of the Attorney General of the State of New York ("NYAG") and the New York State Education Department ("NYSED") commenced an investigation pursuant to Executive Law § 63(12), General Business Law ("GBL") § 349, and Education Law § 2-d(7) into a data breach involving Illuminate Education, Inc. ("Illuminate" or "Respondent"). This Assurance of Discontinuance ("Assurance") contains the findings of the investigation and the relief agreed to by the NYAG, NYSED, and Illuminate (collectively, the "Parties"), whether acting through its respective directors, officers, employees, representatives, agents, affiliates, or subsidiaries.

NYAG AND NYSED FINDINGS

1. Illuminate is a California-based education technology company. The company develops web-based products that schools use to collect, organize, and analyze student data.

2. Much of the data that Illuminate collects, therefore, relates to children, including

student names, birth dates, grade levels, schools, courses, assessment scores, special education information, disability information, disciplinary information and other sensitive information.

3. In January 2020 and February 2021, a cybersecurity vendor warned Illuminate that certain of the company's data security practices related to an internal server created a "High risk" to the company. The vendor recommended that Illuminate address the issues, including by developing account management and password policies and procedures. Illuminate, however, failed to fully implement the policies and procedures recommended by the vendor. In a subsequent cyberattack in December 2021 and January 2022, information associated with approximately 1.7 million current and former New York students was stolen.

The Data Breach

4. For certain functionality, Illuminate products rely on Amazon Web Services (AWS), a widely-used cloud computing platform. Student data that school districts provide to Illuminate for use in Illuminate products is stored in databases on AWS.

5. In late December 2021 and early January 2022, one of Illuminate's AWS accounts was targeted in a cyberattack. Over the course of two days, December 27 and December 28, the attackers probed for access to Illuminate's AWS environment using five sets of stolen access keys. On December 28, the attackers found that the fifth access key, associated with an employee who had left the company years earlier, had sufficient privileges to enable them to gain access to the segment of Illuminate's AWS environment that housed the systems used to operate the IO Suite of products ("IO Account").

6. Between December 28 and January 8, the attackers exfiltrated hundreds of Illuminate database backups containing student information. The student information included

student names, birth dates, student ID numbers, demographic information, socioeconomic information, special education information, disability information, disciplinary information, English Language Learning information, grade levels, school affiliations, courses, and assessment scores. Illuminate had not encrypted the data at rest in these database backups.

7. At the time, Illuminate did not have a system or processes in place to monitor for malicious activity throughout its AWS environment. However, on or about January 5, 2022, Illuminate enabled an Amazon threat detection tool, GuardDuty, across all of its AWS accounts. GuardDuty is designed to monitor AWS accounts for suspicious or malicious activity. After discovering and investigating the cyberattack, Illuminate found that GuardDuty had been previously enabled in the IO Account on a limited basis. Illuminate personnel further found that GuardDuty had identified 44 anomalous events relating to the IO Account, all between December 27, 2021 and January 2, 2022, and all of which appeared to be associated with the attackers' unauthorized access of Illuminate's systems. The tool assigned 42 of the 44 events a severity level of "Medium," which Amazon states "indicates suspicious activity that deviates from normally observed behavior and, depending on your use case, may be indicative of a resource compromise." Illuminate did not review the tool's findings, however, and so did not realize that the attackers had gained access to Illuminate's systems.

8. On January 8, the attackers began deleting certain Illuminate AWS resources. Within several hours, Illuminate personnel detected the unauthorized activity, identified the compromised credentials the attackers had used to access the IO Account, and disabled the attackers' access.

9. Illuminate promptly engaged a cybersecurity firm to conduct a forensic

investigation. The cybersecurity firm confirmed that attackers had gained access to the IO Account and that the company's remedial actions had cut off the attackers' access. Illuminate also worked with the cybersecurity firm to negotiate the destruction of exfiltrated data from the attackers.

10. Illuminate subsequently conducted an analysis to identify the data that had been accessed. The company found that information associated with approximately 1,100,000 current and former New York students in more than 500 schools had been stolen. Between March 25 and April 5, 2022, Illuminate contacted school districts and schools it had identified to notify them of the breach. Illuminate also contacted students in school districts and schools that elected to have Illuminate provide notice to their students.

11. In 2023, Illuminate, under new ownership, discovered that the earlier analysis was incomplete, and that the data stolen by the attackers was associated with more students and schools than it had identified in its initial analysis. In September 2023, Illuminate contacted relevant school districts and schools to notify them of the newly identified records. In all, data associated with approximately 1.7 million current and former New York students in approximately 750 schools were stolen by the attackers in the breach.

12. Illuminate has not been able to determine how the attackers obtained the access keys used to gain admittance to the AWS Account.[1]

Illuminate's Vulnerability Management

13. In January 2020 and February 2021, an Illuminate vendor engaged to conduct

[1] Three of the five keys the attackers used had been hardcoded in Illuminate source code stored in an online code repository at times prior to the breach. By the time of the breach, Illuminate had removed two of the three keys from actively used source code. However, prior versions of source code that contained the keys remained in the online code repository. Illuminate has represented that it did not find evidence that the code repository had been compromised.

cybersecurity assessments of Illuminate's internal, non-cloud systems found that Illuminate's Identity and Access Management ("IAM") practices for an internal server "deviat[ed] from best practice." Among other issues, the vendor found that a large number of Illuminate user accounts appeared to be inactive, and that many user accounts had passwords that were set to never expire.

14. The vendor determined that these issues created a "High risk" to IAM at Illuminate. According to the vendor, a risk rating of "High" meant it was "highly likely a malicious event will occur and could be expected to have a severe or catastrophic adverse effect on organizational operations or organizational assets." The vendor recommended several measures Illuminate could take to address the issues, including developing account management and password policies and procedures to delete user accounts that were no longer needed and requiring users to change their passwords regularly.

15. Illuminate did not fully implement the policies and procedures recommended by the vendor until early 2022 following the data breach.

16. In at least one other instance, Illuminate failed to timely address identified vulnerabilities. In April 2022, Illuminate's vendor conducted a cybersecurity assessment of Illuminate's systems. Although Illuminate received an A- grade overall, the vendor identified several vulnerabilities that it rated as "High risk." Illuminate did not import these vulnerabilities into its vulnerability management system to track them or schedule remediation until July 15, 2022. The company has represented that it has since remediated the issues.

Illuminate's Representations and Contractual Obligations Regarding Data Security

17. Illuminate made a variety of representations and commitments to consumers and customers related to its data security program.

18. In 2016 Illuminate signed on to the Student Privacy Pledge, a public document authored by the advocacy group Future of Privacy Forum that consists of a series of commitments relating to the handling of students' personally identifiable information. Among other items, the pledge contained the following promises:

> We Commit to . . . Maintain a comprehensive security program that is reasonably designed to protect the security, privacy, confidentiality, and integrity of student personal information against risks – such as unauthorized access or use, or unintended or inappropriate disclosure – through the use of administrative, technological, and physical safeguards appropriate to the sensitivity of the information.

19. In a 2016 blog post announcing its decision to sign the pledge, Illuminate wrote that:

> Sharing that Illuminate has signed the Student Privacy Pledge will give parents and educators confidence that data privacy safeguards are in place when using Illuminate!

20. In 2020 the Student Privacy Pledge was updated. The following promise was added:

> We will incorporate privacy and security when developing or improving our educational products, tools, and services and comply with applicable laws.

Illuminate remained a signatory of the updated Student Privacy Pledge until it was removed by Future for Privacy Forum, the pledge creator, in August 2022.

21. Illuminate made similar commitments to protect student data in contracts with New York state school districts. For example, contracts with New York school districts contained the following provisions:

a. Illuminate "shall maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality, and integrity of Confidential

Information."

b. "As required by N.Y. Education Law §2-d, [Illuminate] agrees to use encryption technology to protect PISI while in motion or in its custody . . ."

c. Illuminate "agrees . . . to remediate any identified material security and privacy vulnerabilities in a timely manner."

d. Illuminate must "[a]utomatically de-provision accounts for terminated employees"

e. Illuminate should not "hardcode credentials."

f. "[A]ccounts that are managed locally by [Illuminate] must follow the principal [sic] of 'Least Privileged Access' whereby those user accounts are provided the most restrictive access necessary to perform the required business function."

g. Illuminate "shall return or destroy" confidential information in its possession upon "termination or expiration" of the contract.

22. Despite its representations and contractual commitments, Illuminate failed to maintain reasonable security measures to protect student data in several areas. These included:

a. Access Controls: Illuminate failed to implement and maintain appropriate controls to limit access to student data, including by failing to decommission inactive user accounts, failing to rotate user account credentials, failing to limit account permissions to only those that were necessary, and hardcoding access keys in source code.

b. Protection of Sensitive Information: Illuminate failed to encrypt student data maintained at rest.

c. Monitoring: Illuminate failed to implement and maintain appropriate systems and processes to monitor for and identify anomalous activity.

d. Vulnerability Management: Illuminate failed to timely remediate high risk vulnerabilities.

e. Retention Policies: Illuminate failed to maintain a policy governing the deletion or destruction of student data. In addition, for at least three school districts, Illuminate failed to destroy student data when its engagement with the district ended.

f. Incident Response: Illuminate initially failed to conduct a complete investigation to identify students whose information was accessed without authorization.

Post-Breach Improvements

23. Respondent has represented that, since learning of the breach in early 2022, it has taken steps to improve its information security program, including: (i) strengthening its IAM policies and practices, including by requiring credentials to be rotated, disabling inactive access keys, auditing IAM users, groups and roles to ensure that access rights are consistently tailored appropriately, and restricting creation of new IAM users to Illuminate security personnel; (ii) implementing redundant controls to monitor for anomalous and malicious activity; (iii) auditing its systems to identify all unencrypted personally identifiable information and has encrypted all student data; (iv) implementing several new data-related policies, including a data retention policy; and (v) incorporating its information security program into the information security program overseen by Respondent's parent company, which acquired Respondent in April 2022, three months after the breach.

Respondent Illuminate's Violations

24. NYAG and NYSED find that Illuminate's conduct violated Education Law § 2-d(5)(f), 8 NYCRR Part 121.9(a)(2), (a)(3), (a)(6), and (a)(7), and 8 NYCRR Part 121.10(a), which

require third-party contractors that receive student data to comply with educational agencies' data security and privacy policies, limit internal access to personally identifiable information, maintain reasonable administrative, technical and physical safeguards to protect personally identifiable information, use encryption to protect personally identifiable information at rest, and notify educational agencies of a breach without unreasonable delay. Illuminate's conduct also violated Executive Law § 63(12), which prohibits repeated fraudulent or illegal acts, and GBL § 349, which prohibits deceptive acts and practices.

25. Respondent neither admits nor denies the Findings of the NYAG and NYSED, paragraphs 1-24 above.

26. The NYAG and NYSED find the relief and agreements contained in this Assurance appropriate and in the public interest. THEREFORE, the NYAG and NYSED are willing to accept this Assurance pursuant to Executive Law § 63(15) and Education Law § 2-d, in lieu of commencing statutory and administrative proceedings for violations of Executive Law § 63(12), GBL § 349, Education Law § 2-d, 8 NYCRR Part 121.9(a)(2), (a)(3), (a)(6), and (a)(7), and 8 NYCRR Part 121.10(a).

IT IS HEREBY UNDERSTOOD AND AGREED, by and between the Parties:

PROSPECTIVE RELIEF

27. For the purposes of this Assurance, the following definitions shall apply:

a. "Covered Contract" shall mean a contract, and any renewal or extension of a contract, under which an Educational Agency uses an Illuminate Product and that is entered into at least one hundred twenty (120) days after the Effective Date.

b. "Educational Agency" shall mean a school district, board of cooperative educational services (BOCES), or public or nonpublic school in the State of New York, or the New York State Education Department.

c. "Illuminate Product" shall mean a product or service that is, or has been, owned, operated, or maintained by Respondent.

d. "Impacted Students" shall mean all Students whose data was accessed or acquired without authorization between December 28, 2021 and January 8, 2022.

e. "Personally Identifiable Information" shall mean personally identifiable information as defined in section 99.3 of title 34 of the Code of Federal Regulations implementing the Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g ("FERPA").

f. "Security Event" shall mean unauthorized access, use, or disclosure of Student Data owned, licensed, or maintained by Respondent.

g. "Student" shall mean any person residing in, or who has resided in, New York that is attending, has attended, or is seeking to enroll in an Educational Agency.

h. "Student Data" shall mean Personally Identifiable Information from the student records of an Educational Agency that was received by Respondent in connection with an Illuminate Product.

REPRESENTATIONS

28. Respondent shall comply with Executive Law § 63(12) and GBL § 349 in connection with its collection, use, and maintenance of Student Data, and shall not misrepresent

the manner or extent to which it protects the privacy, security, or confidentiality of Student Data.

EDUCATION LAWS AND REGULATIONS

29. Respondent shall comply with all provisions in Education Law § 2-d and 8 NYCRR Part 121 applicable to third-party contractors.

INFORMATION SECURITY PROGRAM

30. Respondent shall maintain a comprehensive information security program that is reasonably designed to protect the security, integrity, and confidentiality of Student Data that Respondent collects, stores, transmits, and/or maintains. Respondent shall document in writing the content, implementation, and maintenance of the information security program. The information security program shall, at a minimum, include the following processes:

a. Assess and document, not less than annually, internal and external risks to the security, integrity, and confidentiality of Student Data;

b. Design, implement, and maintain administrative, technical, and physical safeguards to control the internal and external risks Respondent identified that are appropriate to: (i) the size and complexity of Respondent's operations; (ii) the nature and scope of Respondent's activities; and (iii) the volume and sensitivity of the Student Data that Respondent collects, stores, transmits, and/or maintains;

c. Assess, not less than annually, the sufficiency of any safeguards in place to address the internal and external risks Respondent identified, and modify the information security program based on the results to ensure that the safeguards comply with (b) above;

d. Test and monitor the effectiveness of the safeguards not less than annually, and modify the information security program based on the results to ensure the safeguards comply with (b) above;

e. Take reasonable steps to select service providers (subcontractors) capable of reasonably safeguarding Student Data, contractually require service providers to implement and maintain reasonable safeguards to protect Student Data, and take reasonable steps to verify service providers are complying with the contractual requirements; and

f. Evaluate the information security program not less than annually and adjust the Program in light of any changes to Respondent's operations or business arrangements, or any other circumstances that Respondent knows or has reason to know may have an impact on the effectiveness of the Program.

31. Respondent shall appoint a qualified individual to be responsible for implementing, maintaining, and monitoring the information security program. The appointed individual shall have credentials, background, and expertise in information security appropriate to the level, size, and complexity of the individual's role in implementing, maintaining, and monitoring the information security program. The appointed individual shall report at a minimum semi-annually to the Chief Executive Officer and senior management, and shall report at a minimum semi-annually to the Board of Directors or equivalent governing body, or an appropriate committee thereof, concerning Respondent's security posture, the security risks faced by Respondent, and the information security program.

32. Respondent shall provide notice of the requirements of the AOD to its

management-level employees responsible for implementing, maintaining, or monitoring the information security program and shall implement appropriate training of such employees, including but not limited to training concerning FERPA, Education Law § 2-d, and associated regulations. The notice and training required under this paragraph shall be provided to the appropriate employees within sixty (60) days of the effective date of the AOD, or within thirty (30) days of when an employee first assumes responsibility for implementing, maintaining, or monitoring the information security program.

STUDENT DATA SAFEGUARDS AND CONTROLS

33. Access Controls: Respondent shall, to the extent it has not already done so, establish and implement, and, thereafter, maintain policies and procedures to appropriately limit access to Student Data. The policies and procedures shall require, at a minimum:

a. Granting individuals and organizations access only to those resources and Student Data that are necessary for their business functions;

b. Promptly removing individuals' access to resources and Student Data upon separation, or, upon an individual's change in responsibilities, promptly removing the individual's access to resources and data that are no longer needed to discharge those responsibilities;

c. Regularly rotating cryptographic keys used to access resources and Student Data;

d. Removing hardcoded login credentials from all code wherever feasible;

e. Implementing AWS best practices, as defined by Amazon,[2] for managing AWS access keys wherever feasible; and

f. Conducting an audit, not less than annually, to ensure compliance with these policies.

Notwithstanding the foregoing, Respondent shall be deemed in compliance with subparagraph (c), (d), or (e) if, with respect to the subparagraph, it implements an equivalent, widely adopted industry measure and the person responsible for the information security program: (1) approve(s) in writing the use of such equivalent measure, and (2) documents in writing how the measure is widely adopted and at least equivalent to the security provided by the subparagraph.

34. Monitoring: Respondent shall, to the extent it has not already done so, establish, and, thereafter, maintain a system designed to monitor Respondent's networks, systems, and assets for anomalous activity and/or data security events, including attempts to access Student Data without authorization, and to alert security personnel upon identification of suspicious activity. This system shall include, but not be limited to, software that inspects internet traffic and uses User and Entity Behavior Analytics or similar technologies or principles for analyzing user and entity behavior to detect anomalies and potential threats.

35. Encryption: Respondent shall, to the extent it has not already done so, establish and implement, and thereafter maintain, policies and systems to encrypt Student Data that it collects, stores, transmits, and/or maintains using an encryption method appropriate to the sensitivity of the Student Data.

[2] Amazon's best practices for managing AWS access keys is currently available online at: https://docs.aws.amazon.com/accounts/latest/reference/credentials-access-keys-best-practices.html.

36. Vulnerability Management: Respondent shall, to the extent it has not already done so, establish and implement, and, thereafter, maintain a vulnerability management program that includes, at a minimum:

a. Maintaining a system for tracking vulnerabilities;

b. Tracking identified vulnerabilities in the system promptly following identification;

c. Rating and ranking the criticality of all vulnerabilities in alignment with an established industry-standard framework (e.g., NVD, CVSS, or equivalent standard); and

d. Maintaining policies, procedures, and any applicable technical measures for remediating or otherwise mitigating any critical or high severity vulnerabilities promptly (but in no event later than thirty (30) days after the vulnerability is detected).

37. Contractual Requirements: Respondent shall include provisions implementing Paragraphs 37(a) and 37(b) below, subject to the conditions and limitations set forth in Paragraphs 37(c), (d) and (e) below, in the initial draft of all Covered Contracts or incorporated data protection terms that Respondent provides to an Educational Agency:

a. The Educational Agency may elect for Respondent to delete all Student Data that Respondent maintains in association with Illuminate Products under the Covered Contract for any Students identified by the Educational Agency. The Educational Agency may make such election, and Respondent shall delete all Student Data identified by Educational Agencies, annually in 2026 and semi-annually thereafter,

on a schedule for identification and deletion to be determined by Respondent and provided to the Educational Agency.

b. Within ninety (90) days of expiration or termination of the Covered Contract, Respondent shall delete all Student Data provided by the Educational Agency under the Covered Contract except for storage of Student Data in backup media, which may be retained for an additional ninety (90) days.

c. Nothing in Paragraph 37 should be construed as preventing Respondent from including in Covered Contracts

    i. Respondent's reasonable requirements relating to the procedures for the Educational Agency's election to delete Student Data under Paragraph 37(a) and identification of the Students whose data is to be deleted, and

    ii. Provisions excluding liability of Respondent and providing for indemnification of claims against Respondent resulting from the deletion of Student Data.

d. The provisions required under Paragraphs 37(a) and (b) may permit the retention of Student Data (1) as otherwise agreed by the Educational Agency in the Covered Contract or other written agreement, (2) for no more than one hundred twenty (120) days after expiration or termination of the Covered Contract, with an additional 90 days to delete Student Data in backup medium, pending renewal, extension, or replacement of the Covered Contract, unless the Educational Agency has communicated a final determination not to renew, extend, or sign a new agreement, (3) for no more than three hundred sixty-five (365) days after expiration or

termination of the Covered Contract, with an additional 90 days to delete Student Data in backup medium, for Student Data relating to student information systems, and (4) as required by law, regulation, court order, or rules applicable to the safeguarding of evidence in pending litigation.

e. Respondent and the Educational Agency may agree in writing or electronically to modify, amend or waive the provisions required under Paragraphs 37(a) and (b).

38. Data Retention and Deletion Notice: Respondent shall provide to each Educational Agency that is party to a Covered Contract an annual notice concerning the retention and deletion of Student Data (a "Notice"). The Notice shall be sent to at least one of the following for the Educational Agency: the data protection officer, the superintendent, the business official, or the notice recipient identified by the Educational Agency in accordance with the Covered Contract. The Notice may be delivered in writing or electronically, and may include additional communications to, or hyperlinked from, a Covered Contract that is signed in the applicable year. The Notice shall:

a. identify the categories of Student Data generally collected for the Illuminate Products used by the Educational Agency under the Covered Contract; and

b. state that the Educational Agency may respond and elect to have Respondent delete Student Data in accordance with the provisions described in Paragraph 37 above.

39. Data Retention Policies and Procedures: Respondent shall, to the extent it has not already done so, establish and implement, and, thereafter, maintain policies and procedures that govern the retention of Student Data consistent with its obligations under Paragraph 37. Not less than annually, Respondent shall conduct an audit to verify compliance with its policies and

procedures and contractual obligations concerning the deletion of Student Data. Respondent shall document the results of the audit in writing, maintain such documentation for seven (7) years from the date of each audit, and provide the documentation to the NYAG and NYSED upon request. Respondent shall comply with the Educational Agency's election for the disposition of Student Data in accordance with Paragraph 37.

40. Incident Response Plan: Respondent shall, to the extent it has not already done so, establish, and, thereafter, maintain a comprehensive incident response plan. The incident response plan shall be documented in writing and include, at a minimum, the following policies:

a. If Respondent has reason to believe a Security Event has occurred, Respondent shall promptly conduct a reasonable investigation to determine, at a minimum, whether Student Data was subject to a Security Event, and, if so, what Student Data was subject to a Security Event, and the Educational Agencies associated with the Student Data.

b. If Respondent determines Student Data is subject to a Security Event, Respondent shall notify each associated Educational Agency whose Student Data has been subject to the Security Event pursuant to 8 NYCRR Part 121.10 in the most expedient way possible and without unreasonable delay.

INFORMATION SECURITY PROGRAM ASSESSMENTS

41. Within one (1) year of the effective date of this Assurance, Respondent shall obtain a comprehensive assessment of the information security of Respondent's network conducted by an independent third-party auditor who uses procedures and standards generally accepted in the profession which shall be documented (a "Third-Party Audit Report") and provided to the NYAG

and NYSED within two weeks of completion. Annually for three (3) years thereafter, Respondent shall obtain Third-Party Audit Reports which Respondent shall maintain for six (6) years from the date of each Third-Party Audit Report and shall provide to the NYAG and NYSED upon request. The Third-Party Audit Report shall:

a. Identify the specific administrative, technical, and physical safeguards maintained by Respondent's information security program;

b. Document the extent to which the identified administrative, technical, and physical safeguards are appropriate considering Respondent's size and complexity, the nature and scope of Respondent's activities, and the sensitivity of the Student Data maintained on the network; and

c. Assess the extent to which the administrative, technical, and physical safeguards that have been implemented by Respondent meet the requirements of the information security program.

IDENTITY THEFT PROTECTION AND CREDIT MONITORING

42. Respondent shall offer, based on the age of the Impacted Students, identity theft protection or credit monitoring services to all Educational Agencies for their Impacted Students, to the extent such Educational Agencies were not previously offered identity theft protection or credit monitoring services for their Impacted Students by Illuminate. Such offer shall be for services at least reasonably equivalent in length and coverage as the offers previously made to Impacted Students to whom Illuminate has previously offered identity theft protection or credit monitoring services.

MONETARY RELIEF

43. Respondent shall pay to the State of New York one million, seven hundred thousand dollars ($1,700,000) in penalties and costs. Payment shall be made in full within fourteen (14) days of the effective date of this Assurance.

44. Payments shall be made in accordance with instructions provided by a NYAG representative and shall reference Assurance No. 25-057.

MISCELLANEOUS

45. Respondent expressly agrees and acknowledges that NYAG or NYSED may initiate a subsequent investigation, civil action, or proceeding to enforce this Assurance, for violations of the Assurance, or if the Assurance is voided pursuant to paragraph 53, and agrees and acknowledges that in the event the Assurance is voided pursuant to paragraph 53:

a. any statute of limitations or other time-related defenses are tolled from and after the effective date of this Assurance;

b. the NYAG may use statements, documents or other materials produced or provided by Respondent prior to or after the effective date of this Assurance;

c. any civil action or proceeding must be adjudicated by the courts of the State of New York, and that Respondent irrevocably and unconditionally waives any objection based upon personal jurisdiction, inconvenient forum, or venue; and

d. evidence of a violation of this Assurance shall constitute prima facie proof of a violation of the applicable law pursuant to Executive Law § 63(15).

46. If a court of competent jurisdiction determines that Respondent has violated the Assurance, Respondent shall pay to the NYAG and/or NYSED the reasonable cost, if any, of

obtaining such determination and of enforcing this Assurance, including without limitation legal fees, expenses, and court costs.

47. This Assurance is not intended for use by any third party in any other proceeding. This Assurance is not intended, and should not be construed, as an admission of liability by Respondent.

48. Illuminate shall include in any purchase, assignment, or transfer agreement pursuant to which Illuminate Products are purchased, assigned or transferred a provision that requires any New Business Owner or New Asset Owner to comply with Paragraphs 27-41 of this Assurance with respect to those Illuminate Products being purchased, assigned, or transferred. For purposes of this paragraph, "New Business Owner" shall mean a purchaser, assignee, or transferee of all or substantially all of Illuminate's business, and "New Asset Owner" shall mean any purchaser, assignee, or transferee of all or substantially all of the assets required to deliver or sell the Illuminate Products.

49. Respondent shall not permit another party to manage or control all or substantially all of the operation of an Illuminate Product unless that party has agreed in writing to comply with Paragraphs 27-41 of the Assurance with respect to that Illuminate Product being managed or controlled.

50. Nothing contained herein shall be construed as to deprive any person of any private right under the law.

51. Any failure by the NYAG or NYSED to insist upon the strict performance by Respondent of any of the provisions of this Assurance shall not be deemed a waiver of any of the provisions hereof, and the NYAG, notwithstanding that failure, shall have the right thereafter to

insist upon the strict performance of any and all of the provisions of this Assurance to be performed by Respondent.

52. All notices, reports, requests, and other communications pursuant to this Assurance must reference Assurance No. 25-057, and shall be in writing and shall, unless expressly provided otherwise herein, be given by hand delivery; express courier; or electronic mail at an address designated in writing by the recipient, followed by postage prepaid mail, and shall be addressed as follows:

If to Respondent Illuminate, to:

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
300 N. LaSalle
Chicago, IL 60654
Email: lisa.madigan@kirkland.com

If to NYAG, to:

Jordan Adler, Senior Enforcement Counsel, or in his absence,
to the person holding the title of Bureau Chief
Bureau of Internet & Technology
28 Liberty Street
New York, NY 10005

If to NYSED, to:

Whitney Braunlin, Chief Privacy Officer, or in her absence,
to the person holding the title of Chief Privacy Officer
New York State Education Department

89 Washington Avenue
Albany, NY 12234

53. NYAG and NYSED have agreed to the terms of this Assurance based on, among other things, the representations made to NYAG and NYSED by Respondent and its counsel and the factual investigation of NYAG and NYSED as set forth in the Findings, paragraphs 1-24 above. Respondent represents and warrants that neither it nor its counsel has made any material representations to NYAG that are inaccurate or misleading. If any material representations by Respondent or its counsel are later found to be inaccurate or misleading, this Assurance is voidable by NYAG in its sole discretion.

54. No representation, inducement, promise, understanding, condition, or warranty not set forth in this Assurance has been made to or relied upon by Respondent in agreeing to this Assurance.

55. The obligations of this Assurance set forth in paragraphs 30-40 shall expire at the conclusion of the seven (7) year period after the Effective Date.

56. Respondent represents and warrants, through the signature below, that the terms and conditions of this Assurance are duly approved.

57. Unless a term limit for compliance is otherwise specified within this Assurance, the Respondent's obligations under this Assurance are enduring. Nothing in this Agreement shall relieve Respondent of other obligations imposed by any applicable state or federal law or regulation or other applicable law.

58. Respondent agrees not to take any action or to make or permit to be made any public statement denying, directly or indirectly, any finding in the Assurance or creating the impression that the Assurance is without legal or factual basis. Nothing in this paragraph affects Respondent's

right to take legal or factual positions in defense of litigation or other legal proceedings.

59. Nothing contained herein shall be construed to limit the remedies available to NYAG or NYSED in the event that Respondent violates the Assurance after its effective date.

60. This Assurance may not be amended except by an instrument in writing signed on behalf of the Parties to this Assurance.

61. In the event that any one or more of the provisions contained in this Assurance shall for any reason be held by a court of competent jurisdiction to be invalid, illegal, or unenforceable in any respect, in the sole discretion of NYAG, such invalidity, illegality, or unenforceability shall not affect any other provision of this Assurance.

62. Respondent acknowledges that it has entered this Assurance freely and voluntarily and upon due deliberation with the advice of counsel.

63. This Assurance shall be governed by the laws of the State of New York without regard to any conflict of laws principles.

64. The Assurance and all its terms shall be construed as if mutually drafted with no presumption of any type against any party that may be found to have been the drafter.

65. This Assurance may be executed in multiple counterparts by the Parties hereto. All counterparts so executed shall constitute one agreement binding upon all Parties, notwithstanding that all Parties are not signatories to the original or the same counterpart. Each counterpart shall be deemed an original to this Assurance, all of which shall constitute one agreement to be valid as of the effective date of this Assurance. For purposes of this Assurance, copies of signatures shall be treated the same as originals. Documents executed, scanned and transmitted electronically and electronic signatures shall be deemed original signatures for purposes of this Assurance and all

matters related thereto, with such scanned and electronic signatures having the same legal effect as original signatures.

66. The effective date of this Assurance shall be October 29, 2025.

LETITIA JAMES **ATTORNEY GENERAL OF THE STATE OF NEW YORK** By: _____ Jordan Adler Bureau of Internet and Technology New York State Attorney General 28 Liberty St. New York, NY 10005 Phone: (212) 416-8433 Fax: (212) 416-8369 11/5/2025 Date **BETTY A. ROSA** **COMMISSIONER OF EDUCATION OF THE STATE OF NEW YORK** By: _____ Whitney Braunlin Chief Privacy Officer New York State Education Department 89 Washington Avenue Albany, NY 12234 Phone: 518-464-6400 11/3/2025 Date	**ILLUMINATE EDUCATION, INC.** By: _____ Chris Bauleke Chief Executive Officer October 29, 2025 Date