222-3105

UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

COMMISSIONERS: **Andrew N. Ferguson, Chair**
Mark R. Meador

In the Matter of **ILLUMINATE EDUCATION, INC., a corporation.**	**DOCKET NO.**

COMPLAINT

The Federal Trade Commission, having reason to believe that Illuminate Education, Inc., a corporation, has violated the provisions of the Federal Trade Commission Act, and it appearing to the Commission that this proceeding is in the public interest, alleges:

1. Respondent Illuminate Education, Inc. ("Illuminate") is a California corporation with its principal office or place of business at 2911 Peach Street, Wisconsin Rapids, WI 54494.

2. Illuminate is wholly owned by Illuminate Education Holdings, Inc., which was wholly owned by Illuminate Education Intermediate, Inc., which was wholly owned by Illuminate Education Holdings, LLC ("Illuminate Holdings"). Illuminate's subsidiaries include FastBridge Learning, LLC, DataCation, LLC, SchoolCity, LLC, and Sanford Systems, LLC.

3. On April 1, 2022, Illuminate Merger Sub, LLC, a wholly-owned subsidiary of Renaissance Learning, Inc. ("Renaissance"), merged with and into Illuminate Holdings, with Illuminate Holdings continuing as the surviving entity. As a result of the merger, Illuminate Holdings became a direct wholly-owned subsidiary of Renaissance and Illuminate became an indirect wholly-owned subsidiary of Renaissance.

4. The acts and practices of Illuminate alleged in this complaint have been in or affecting commerce, as "commerce" is defined in Section 4 of the Federal Trade Commission Act.

Illuminate's Business Model and Operations

5. Illuminate is an education technology company that makes cloud-based, Pre-K–12 educational software/web applications, and instructional and assessment tools. Illuminate markets and sells its products to schools and school districts for use by teachers and administrators. Its products, programs, and services allow schools and school districts to take attendance, administer testing, assess learning needs, monitor student progress, screen for learning disabilities, track social-emotional behavior, conduct data analytics and visualization, and develop instructional or intervention strategies. Illuminate has asserted that more than 17 million students, 5,200 school districts, and schools across all 50 states rely on Illuminate daily.

6. Illuminate acts as a service provider to schools or school districts pursuant to various contractual agreements. Illuminate agrees to contractual terms that direct the collection, use, and maintenance of personal information about students collected on behalf of schools and school districts. Illuminate's publicly available website notes the categories of Personal Information the Company collects on behalf of schools or school districts. They include:

- Demographic information including name, mailing address, email address, and date of birth;
- Student education records including student's grades, class enrollment, and behavioral records;
- Health-related information including student's immunizations and vision and hearing screening results;
- System usernames and passwords.

Illuminate's Information Technology Infrastructure

7. As part of its information technology infrastructure, Illuminate generally deploys its web applications in one of three cloud-based platforms: Amazon Web Services ("AWS"), Google Cloud Platform ("GCP"), or Microsoft Azure ("Azure"). All Illuminate applications within the IO Suite of products (comprising of applications including IO Assessment, IO Compass, Data Driven Classroom, IO Admin, and IO Auth), were deployed in AWS. Illuminate used the Amazon Elastic Compute Cloud (Amazon EC2), Amazon Relational Database Service ("Amazon RDS"), and Amazon Simple Storage Service ("S3") products in their environment.

8. Illuminate's IO Suite of products utilized EC2 and RDS databases as well as S3 buckets (collectively "AWS services") to store a wide variety of students' personal information. This personal information contained, among other things, student names, student identification numbers, dates of birth, email addresses, usernames, passwords, demographic information (such as race, home language, foster status, homelessness status, economic status), disability information, special education needs information, and disciplinary incident information, and was capable of being associated with a particular student.

9. Illuminate stored student data unencrypted. This personal information can be misused to facilitate identity theft and other harm to students. Illuminate's database backups contained some or all of the personal information described in Paragraph 8 for more than 10.1 million students.

December 2021 – January 2022 Data Breach

10. Illuminate's failures, as described in Paragraph 24, led to a breach in or around December 2021 through January 2022 of its network and databases, and the exfiltration of the student personal information of more than 10.1 million students.

11. On or around January 8, 2022, Illuminate received an automated alert notifying it that several Illuminate websites had suddenly become unavailable. An employee of Illuminate's software development team received the alert and notified members of the engineering and DevSecOps (development, security, and operations) teams, who discovered malicious activity in Illuminate's IO Suite.

12. Upon discovering malicious activity in the IO Suite, Illuminate retained a third-party incident response team to investigate the incident. The incident response team confirmed that the threat actor gained entry into Illuminate's AWS environment using existing sets of access key pairs for Identity and Access Management ("IAM") users. The investigation discovered that the threat actor first gained access to Illuminate's network on December 27, 2021, and remained undetected in Illuminate's network until January 8, 2022, when Illuminate discovered and terminated their access.

13. The investigation detailed that the threat actor used 5 different sets of credentials in attempts to gain unauthorized access to a section of Illuminate's AWS environment known as the IO account. The set of credentials that allowed the threat actor to successfully breach the IO account belonged to a former employee with IAM administrator privileges. The threat actor used this newfound admin-level access to generate a token and create a new user with similar access as the compromised employee's account that could bypass the requisite MFA authentication to freely access Illuminate's AWS environment.

14. With unfettered access to Illuminate's IO account for 13 days, the threat actor performed several malicious activities including modifying Illuminate's AWS security groups, resetting database passwords, deleting database resources, exfiltrating 787 SQL server backups, and compromising the personal information of more than 10.1 million students. The threat actor carried out these activities in Illuminate's AWS environment without detection and without triggering Illuminate's threat detection or response system until, as noted above, several Illuminate websites were found to be unavailable due to the threat actor's activities.

15. The key pair the threat actor used to gain entry into Illuminate's AWS environment belonged to a former employee, an IAM user with administrator privileges, who had departed Illuminate in April 2018, over three and a half years before the breach. Illuminate did not disable nor rotate this former employee's key pair upon their departure, or anytime during the three and a half years prior to the breach. The threat actor's use of a former employee's credentials to gain access to Illuminate's AWS environment should have been flagged as suspicious activity. This lack of flagging of suspicious activity highlights the lack of adequate logging and alerting across the entire enterprise by Illuminate.

16. Once detected, the threat actor threatened to expose the stolen student personal information unless Illuminate paid a ransom. Illuminate eventually agreed to pay an undisclosed

amount in exchange for the receipt of the stolen data; however, the threat actor did not return all of the stolen data. Illuminate has not been able to conclusively verify that the threat actor deleted all stolen data. Additionally, Illuminate cannot confirm whether the threat actor made copies of the stolen data, or sold, or otherwise shared the stolen data with other parties.

Illuminate's Security Failures

17. Illuminate had been on notice from at least January 2020 of numerous security vulnerabilities present in its network and failed to take steps to correct them. From 2020 to at least 2022, Illuminate retained a third-party vendor to conduct annual Cybersecurity Assessments and NIST Cybersecurity Framework Assessments. The vendor's January 2020 assessment of Illuminate's network identified several major security vulnerabilities, provided recommended remediations, and assigned Illuminate an overall "C" security grade, which denotes that an organization requires several updates and remediations to bring its state of security up to an acceptable level. The January 2020 assessment identified major security vulnerabilities including Illuminate's weak IAM practices, outdated software, use of weak credentials, and insecure system configurations.

18. Despite receiving the vendor's corrective action plan, Illuminate failed to adequately address the security failures that had been identified. As reflected in the same vendor's February 2021 Cybersecurity Assessment findings, more than a year after the January 2020 assessment, Illuminate still had not addressed its weak IAM practices and use of weak credentials. Illuminate's Director of Data Privacy & Security, hired in October 2021, noted that Illuminate had inadequate controls for theft detection and monitoring and that its system was vulnerable to potential for breach from an unintended disclosure of personal data.

19. In the wake of the December 2021-January 2022 data breach, Illuminate's own post-breach analyses and actions highlight the company's lack of adequate IAM practices, logging, monitoring, detection, and alerting capabilities, which were exposed during the course of this data breach. For example, Illuminate's analyses acknowledged that the local IAM user credential used by the threat actor belonged to an employee that departed the company in 2018 and that the employee's credentials were approximately 10 years old. Similarly, Illuminate failed to timely configure AWS GuardDuty to appropriately log events and generate actionable security alerts for suspicious security events until after the threat actor had breached Illuminate's environment. Finally, Illuminate didn't expand the deployment of vital threat detection and response tools to cover their AWS environment until after the January 2022 breach.

Notification to Schools, School Districts, and Students

20. Illuminate and its third-party vendor confirmed the data breach on January 8, 2022, and concluded the breach investigation on or around March 25, 2022. Illuminate employed disparate breach notification practices with schools, school districts, and students across the country. Illuminate offered affected students complimentary access to 12 months of identity monitoring services, and for students over 18 Illuminate offered 12 months of credit monitoring services.

21. While some school districts, students and their parents were notified of the breach in a timely manner, some were not. For example, Illuminate's initial notifications occurred from

March 2022 to July 2022. Illuminate's subsequent notifications to various school districts, students and their parents, however, occurred as late as October 2023, nearly two years after the data breach. Remarkably, in October 2023, nearly 387,000 current and former students were newly identified as being affected by Illuminate's December 2021 – January 2022 data breach. Illuminate's internal breach notification procedure in effect at the time of this data breach required notification to affected parties no later than 72 hours from the determination of a breach.

Illuminate's Data Maintenance Practices

22. Illuminate also failed to implement reasonable data retention practices and procedures, which further exacerbated the severity of the breach. As of 2021, Illuminate was aware that because the company lacked records retention limits and deletion requirements, the company had failed to delete student data in instances where it was contractually required to do so, with the result that the company retained terabytes of unmanaged and unstructured data. Illuminate did not begin to maintain a data retention policy until March 2022, well after the data breach. Similarly, Illuminate did not maintain a comprehensive data map for its extensive trove of student personal information until after the start of the Commission's investigation. Illuminate's lack of proper data inventorying and cataloging impaired Illuminate's ability to notify school districts of the data breach, so affected parties could not take mitigating actions.

23. In some instances, Illuminate retained data belonging to former schools and school districts that were never fully onboarded. For example, this data breach exposed student data from 2018-2019 for an Illinois school district that never operationalized Illuminate's IO product. Similarly, the breach exposed student data from a former client, a New York school district from approximately 2011-2013, almost a decade before the breach. Illuminate's failure to implement reasonable data retention practices and procedures resulted in Illuminate keeping former students' personal information, at times, for years longer than it was necessary.

Illuminate's Unfair Security Practices

24. From at least 2019 to the present, Illuminate has engaged in a number of practices that, together, failed to provide reasonable security to prevent unauthorized access to students' personal information and timely notify consumers of the breach. Among other things, Illuminate:

a) stored, until at least January 2022, students' personal information on Illuminate's network in S3 buckets in plaintext, rather than encrypting the information;

b) failed to implement reasonable access controls to safeguard students' personal information stored in AWS services. Specifically, Illuminate:

i) failed, until at least April 2022, to audit and remove inactive accounts, accounts with expired passwords, and accounts with passwords that never expire;

ii) failed, until at least April 2022, to enforce single sign on (SSO) and multifactor authentication (MFA) on AWS services;

iii) failed to implement standard cybersecurity safeguards such as consistent policy and procedure deployment and maintaining data inventory or data flow diagrams, even when cybersecurity assessments that Illuminate obtained from a third-party vendor between at least 2019 and 2021 had specifically highlighted these failures;

iv) failed, until at least April 2022, to implement a reasonable Identity and Access Management (IAM) policy, and to appropriately provision role-based access; and

v) failed to appropriately configure, secure, and monitor AWS S3 buckets;

c) failed to employ effective threat detection and response on its network and databases;

d) failed to employ effective vulnerability monitoring and patch management practices;

e) improperly configured, or failed to implement, logging and monitoring tools to appropriately capture and alert on suspicious data security events;

f) failed, until at least November 2022, to establish a comprehensive incident management or incident response plan;

g) failed, until at least March 2022, to have a policy, process, or procedure for inventorying and deleting students' personal information stored on Illuminate's network after that information is no longer necessary, which prevented complying with contractual requirements related to deletion;

h) failed to implement reasonable data retention practices and procedures; and

i) failed to timely notify school districts, students, and parents of the breach.

Injury

25. Illuminate stored information including students' disability and detailed demographic information, together with identifying information such as their names, email addresses, and birthdates.

26. Illuminate's failure to provide reasonable security for students' personal information has caused or is likely to cause substantial injury to those students in the form of fraud, identity theft, monetary loss, and time spent remedying or attempting to prevent any of these potential injuries. Such injury includes parents' spending time and effort monitoring the identity and credit for their children beyond the one or two years of monitoring that IE provided.

27. Such injury also includes reputational harm resulting from disclosure of information, such as Individualized Education Program (IEP) status, special education status, or medical diagnoses, that may affect students' future ability to obtain employment or admittance into higher education. As early as August 2017, Illuminate has publicly recognized what can result from a lack of adequately securing student personal information and employing reasonable data security

measures. Illuminate claimed on its website:

> [T]reating student data with respect is just the right thing to do. So, what could happen if a system was accessed by someone without approval (whether by stealing login information or hacking a system)? That data could be used for:
>
> - Creating contact lists for email scams or targeted advertising
> - Finding addresses and other contact info for family members
> - Changing a student's grades
> - Viewing personal information meant to be private, such as learning and physical disabilities, or even medications

28. Due to Illuminate's lack of access controls and authentication protections for its AWS environment and failure to appropriately monitor its systems, students' personal information, including disability and detailed demographic information, was exposed without Illuminate's knowledge.

29. Students, parents, and school districts had no way of independently knowing about Illuminate's information security shortcomings and could not reasonably have avoided possible harms from failures described in Paragraphs 18-20.

30. The 387,000 current and former students newly identified in October 2023 as being affected by Illuminate's data breach also had no way of avoiding possible harms resulting from Illuminate's untimely breach notification. Students and their parents therefore could not take prompt steps in the wake of the breach to mitigate potential harm to their identity and credit or take steps to shield their personal information.

31. Further, the harms are not outweighed by any countervailing benefits to users or competition. Illuminate could have prevented or mitigated these information security failures through readily available, and relatively low-cost, measures. For example, Illuminate could have encrypted all student personal information, implemented regular review of access permissions, properly configured the multifactor authentication bypass rule within AWS to check for satisfactory alternative authentication methods, employed effective endpoint detection and response tools, and configured effective alert capabilities. Any of these measures would likely have prevented or minimized the impact of the December 2021-January 2022 breach.

Illuminate's Information Security and Privacy Statements

32. Illuminate made explicit representations about its information security practices that led school districts, students and their parents to believe that it used reasonable and appropriate information security practices to protect students' personal information.

33. For example, Illuminate's Privacy Policy in effect from July 2017 until approximately August 2022, included the following statements:

> We protect your data like it's our own.

We pledge our unwavering commitment to student data privacy.

We take security measures—physical, electronic, and procedural—to help defend against the unauthorized access and disclosure of your information. In addition to the restrictions discussed in this Privacy Policy, our employees are required to comply with information security safeguards, and our systems are protected by technological measures to help prevent unauthorized individuals from gaining access.

Illuminate's Privacy & Data Security Statements to School Districts

34. Beginning in or around January 2018, in numerous contracts for services in multiple states, Illuminate made privacy and data security representations to schools and school districts in which it purported to employ reasonable and appropriate security measures to safeguard students' personal information.

New York

35. For example, Illuminate made representations to at least three schools or school districts in New York. In March 2018 Illuminate represented to a New York City charter school that it "maintains strict administrative, technical and physical procedures to protect information stored in our servers," and that "[a]ccess to information is limited (through user/password credentials and two factor authentication) to those employees who require it to perform their job functions." Illuminate also represented it "implemented practices and procedures designed to meet or exceed … private industry best practices, regarding the proper handling and security of student information."

36. Similarly, in January and October 2020, Illuminate represented to a city board of education and a Hudson Valley school district that as required by N.Y. Education Law §2-d, it agreed to use encryption technology to protect student data while in motion or in its custody from unauthorized disclosure. In addition to these representations, Illuminate represented that it maintained a log of data-changing operations, and conducted periodic risk assessments and remediated any identified material security and privacy vulnerabilities in a timely manner.

Connecticut

37. Illuminate made similar data security representations to school districts in Connecticut. Between 2018 and 2020, Illuminate represented it would take actions (such as encryption) designed to ensure the security and confidentiality of student data. Similarly, Illuminate also represented that it had put in place reasonable and appropriate security, technical, and organizational measures to protect its usage of student data against accidental or unlawful destruction or accidental loss, alterations, and unauthorized use, disclosure, or access.

Colorado

38. Between 2019 and 2021, Illuminate entered into similar contracts for services with school districts in Colorado. Like the representations made in Paragraph 45, Illuminate warranted it had put in place reasonable and appropriate security, technical, and organizational measures to protect its usage of students' personal information against accidental or unlawful destruction or

accidental loss, alterations, and unauthorized use, disclosure, or access. For example, Illuminate represented it would store and process student data in accordance with commercial standard practices that are no less rigorous than those outlined in the SANS Top 20 Security Controls, and that student data would be encrypted in transmission and at rest in accordance with NIST Special Publication 800-57.

39. As described in Paragraph 24, despite the representations Illuminate made in Paragraphs 35-38 to various school districts across New York, Connecticut, and Colorado, Illuminate failed to:

- deprovision accounts for terminated employees;
- enable appropriate logging and multi-factor authentication;
- take measures to maintain reasonable administrative, technical and physical safeguards and practices;
- limit internal access;
- encrypt student personal information; and
- timely remediate any material security and privacy vulnerabilities identified through internal risk assessments.

Illuminate's Breach Notification Statements

40. Illuminate has made representations about the swiftness of its breach or unauthorized disclosure notifications to schools and school districts. For example, in contracts with school districts in New York and Connecticut, Illuminate promised to provide notifications of any breach or unauthorized release of student data as early as 24 or 48 hours, respectively, from the knowledge or discovery of a potential breach.

41. As described in Paragraph 21, despite the representations Illuminate made in Paragraph 40 to various school districts regarding swift breach or unauthorized disclosure notifications, Illuminate failed to provide breach notifications to most schools until March to July 2022, well over three months after the fact. And in some cases, Illuminate notified schools, school districts, and approximately 387,000 students about the breach of their personal information as late as October 2023, nearly two years after the breach.

Count I
Unfair Information Security Practices

42. As described in Paragraph 24, Illuminate's failure to employ reasonable and appropriate measures to protect personal information caused or is likely to cause substantial injury to consumers that is not outweighed by countervailing benefits to consumers or competition and is not reasonably avoidable by consumers themselves. This practice is an unfair act or practice.

Count II
Data Security Misrepresentations

43. As described in Paragraphs 33-38, Illuminate has represented, directly or indirectly, expressly or by implication, that it implemented reasonable measures to protect personal information against unauthorized access.

44. In fact, as set forth in Paragraph 39, Illuminate did not implement reasonable measures to protect personal information against unauthorized access. Therefore, the representation set forth in Paragraph 43 is false or misleading.

Count III
Misrepresentations to School Districts Regarding Notice

45. As described in Paragraph 40, in connection with the collection, use and maintenance of school district data consisting of personal information collected about students, Illuminate has represented that it would timely notify school districts whose data has been exposed as a result of a breach or unintended disclosure of confidential or personally identifiable information.

46. In fact, as described in Paragraph 41, Illuminate failed to provide timely notice to school districts and students whose personal information was exposed because of the breach. Therefore, Illuminate's representations as set forth in Paragraph 45 are false or misleading.

Violations of Section 5

47. The acts and practices of Illuminate as alleged in this complaint constitute unfair or deceptive acts or practices in or affecting commerce in violation of Section 5(a) of the Federal Trade Commission Act.

THEREFORE, the Federal Trade Commission this____day of_____, 20_, has issued this Complaint against Respondent.

By the Commission.

April J. Tabor
Secretary

SEAL: