202-3105

UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

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

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

DECISION

The Federal Trade Commission ("Commission") initiated an investigation of certain acts and practices of the Respondent named in the caption. The Commission's Bureau of Consumer Protection ("BCP") prepared and furnished to Respondent a draft Complaint. BCP proposed to present the draft Complaint to the Commission for its consideration. If issued by the Commission, the draft Complaint would charge the Respondent with violations of the Federal Trade Commission Act.

Respondent and BCP thereafter executed an Agreement Containing Consent Order ("Consent Agreement"). The Consent Agreement includes: (1) statements by Respondent that it neither admits nor denies any of the allegations in the draft Complaint, except as specifically stated in this Decision and Order, and that only for purposes of this action, it admits the facts necessary to establish jurisdiction; and (2) waivers and other provisions as required by the Commission's Rules.

The Commission considered the matter and determined that it had reason to believe that Respondent has violated the Federal Trade Commission Act, and that a Complaint should issue stating its charges in that respect. The Commission accepted the executed Consent Agreement and placed it on the public record for a period of thirty (30) days for the receipt and consideration of public comments. The Commission duly considered any comments received from interested persons pursuant to Section 2.34 of its Rules, 16 C.F.R. § 2.34. Now, in further conformity with the procedure prescribed in Rule 2.34, the Commission issues its Complaint, makes the following Findings, and issues the following Order:

Findings

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

2. The Commission has jurisdiction over the subject matter of this proceeding and over the Respondent, and the proceeding is in the public interest.

ORDER

Definitions

A. "**Authorized User**" means any employee, contractor, agent, customer, or other person that is authorized to access any of Respondent's information systems or data.

B. "**Covered Incident**" means any incident that results in Respondent notifying, pursuant to a statutory or regulatory requirement, any U.S. federal, state, or local government entity that information of or about an individual consumer was, or is reasonably believed to have been, accessed, acquired, or publicly exposed without authorization.

C. "**Covered Information**" means information from or about an individual consumer used, collected or retained in connection with a Covered Product including: (a) a first and last name; (b) a home or physical address; (c) an email address or other online contact information, such as an instant messaging user identifier or a screen name; (d) a mobile or other telephone number; (e) a driver's license or other government-issued identification number; (f) date of birth; (g) Medical Information; (h) user ID, or other persistent identifier that can be used to recognize a user over time and across different devices, websites, or online services; (i) user account credentials, such as a login name and password (whether plain text, encrypted, hashed, and/or salted); (j) student demographic information (such as foster status, homelessness status, economic status, other population characteristics); (k) disability information; (l) special education needs information; or (m) disciplinary incident information.

D. "**Covered Product**" means any product offered by Respondent that is marketed, offered for sale, or sold, directly or indirectly, in the United States, including eSchoolData, eduCLIMBER, DnA, FastBridge and SchoolCity, and all versions, revisions, and successor products.

E. "**Deidentified Information**" means information that cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular person, in that Respondent must, at a minimum:

1. Have implemented technical safeguards that prohibit reidentification of the person to whom the information may pertain;

2. Have implemented business processes that specifically prohibit reidentification

of the information, including by buyers, customers, or other entities to whom Respondent provides the information;

3. Have implemented business processes to prevent inadvertent release of Deidentified Information; and

4. Make no attempt to reidentify the information.

F. "**Delete**," "**Deleted**," or "**Deletion**" means to remove Covered Information such that it is not maintained in retrievable form and cannot be retrieved in the normal course of business.

G. "**Medical Information**" means information relating to the health of an individual consumer, including but not limited to medical history information, prescription information, physical or mental health testing information, health insurance information, or physician exam or health professional notes.

H. "**Respondent**" means Illuminate Education, Inc., a California corporation, and its successors and assigns.

Provisions

I. Prohibition against Misrepresentations about Privacy and Security

IT IS ORDERED that Respondent, Respondent's officers, agents, employees, and all other persons in active concert or participation with any of them who receive actual notice of this Order, whether acting directly or indirectly, in connection with any product or service, must not misrepresent in any manner, expressly or by implication:

A. The extent to which Respondent protects the privacy, security, availability, confidentiality, or integrity of any Covered Information; or

B. The time period in which Respondent will notify school districts and students of a breach or unintended disclosure of any Covered Information.

II. Mandated Deletion and Data Minimization

IT IS FURTHER ORDERED that Respondent must:

A. Within 90 days of the Order Effective Date, Delete or destroy Covered Information, retention of which is neither (i) reasonably necessary to provide products or services under Respondent's contracts with its customers nor (ii) requested by Respondent's customers, and provide a written statement to the Commission, pursuant to the Provision entitled Compliance Reporting, confirming that all such data has been Deleted or destroyed, specifically enumerating which types of information were Deleted or destroyed; and

B. Refrain from collecting, processing, or maintaining any Covered Information not reasonably necessary to provide products or services under Respondent's contracts with its customers, except as requested by Respondent's customers.

Provided, however, that any Covered Information that any Respondent is otherwise required to Delete or destroy pursuant to this provision, or prohibited from collecting, processing, or maintaining pursuant to this provision, may be retained, collected, processed, or maintained pursuant to agreements with or instruction from Respondent's customers, as requested by a government agency or relevant school board or other public entity, or as otherwise required by law, regulation, court order, or other legal obligation, including as required by rules applicable to the safeguarding of evidence in pending litigation.

Provided further, that the deletion and minimization requirements listed in this Provision II do not apply to Deidentified Information.

III. Data Retention Limits

IT IS FURTHER ORDERED that Respondent, in connection with the storage, maintenance, use, or disclosure of, or provision of access to, Covered Information, must:

A. Within 90 days of the Order Effective Date, document, make publicly available on its website(s), and adhere to a retention schedule for Covered Information

required to be deleted in accordance with Provision II, setting forth in such schedule: (1) the purpose or purposes for which Covered Information is collected and maintained by Respondent; (2) the specific business needs for Respondent retaining such Covered Information; and (3) a set timeframe for Deletion of Covered Information (absent any intervening deletion requests from consumers) that is limited to the time reasonably necessary to fulfill the purpose or business need for which the Covered Information was collected, maintained, or retained. For clarity, the requirements of this Provision III.A additionally apply to the Covered Information of former customers and customers who migrate to a different Respondent product; and

B. Within 90 days after the Order Effective Date, provide a written statement to the Commission, pursuant to the Provision entitled Compliance Report and Notices, describing the retention schedule for Covered Information made publicly available on its website(s).

IV. Mandated Information Security Program and Data Management Procedures

IT IS FURTHER ORDERED that Respondent, and any business that Respondent controls, directly or indirectly, in connection with the maintenance, use, or disclosure of, or provision of access to, Covered Information, must, within ninety (90) days of the Order Effective Date, establish and implement, and thereafter maintain, a comprehensive information security program that protects the security, confidentiality, and integrity of such Covered Information ("**Information Security Program**"). To satisfy this requirement, Respondent must, at a minimum:

A. Document in writing the content, implementation, and maintenance of the Information Security Program;

B. Designate a qualified employee to coordinate and be responsible for the Information Security Program ("Qualified Individual");

C. Require the Qualified Individual to report in writing to Respondent's board of directors or governing body or, if no such board or equivalent governing body exists, to a senior officer of Respondent responsible for Respondent's Information Security Program at least once every twelve (12) months and promptly (not to exceed thirty (30) days) after a Covered Incident. The report must include the following information:

1. The overall status of the Information Security Program and Respondent's compliance with this Provision, including by providing the written program and any evaluations thereof or updates thereto; and
2. Material matters related to the Information Security Program, addressing issues such as risk assessment, risk management, and control decisions; service provider arrangements; results of testing, including any testing conducted pursuant to sub-Provision G of this Provision; Covered Incidents or violations of Respondent's information security policies or procedures and management's responses thereto; and recommendations for changes in the Information Security Program.

D. Assess and document, at least once every twelve (12) months and promptly (not to exceed one hundred and twenty (120) days) following a Covered Incident, reasonably foreseeable internal and external risks to the security, confidentiality, or integrity of Covered Information within the possession, custody, or control of Respondent that could result in the (1) unauthorized collection, maintenance, use, or disclosure of, provision of access to, or destruction of, Covered Information; or (2) misuse, loss, theft, alteration, or other compromise of such information. The risk assessments must be written.

E. Design, implement, maintain, and document safeguards that control for the internal and external risks identified in response to sub-Provision D. Each safeguard must be based on the volume and sensitivity of the Covered Information that is at risk, and the likelihood that the risk could be realized and result in the (1) unauthorized collection, maintenance, use, or disclosure of, provision of access to, or destruction of, Covered Information; or (2) misuse, loss, theft, alteration, or other compromise of such information. Such safeguards must also include:

1. Policies, procedures, standards, and technical measures to systematically inventory and classify Covered Information in Respondent's control, including policies, procedures, and technical measures to track and inventory the transfer and storage of Covered Information among and within Respondent's various networks, systems, and assets;

2. Policies, procedures, standards, and technical measures to log and monitor access to networks, systems, and assets in Respondent's control;

3. Policies, procedures, standards, and technical measures to monitor all of Respondent's networks, systems, and assets to identify and log anomalous activity and/or data security events, including unauthorized attempts to access or exfiltrate Covered Information from Respondent's networks, systems, and assets. Such measures must require Respondent to determine baseline system activity, identify and respond to anomalous events and unauthorized attempts to access or exfiltrate Covered Information, and verify the effectiveness of monitoring and logging;

4. Technical, organizational, and, as appropriate, physical controls to:

    a. Safeguard against unauthorized access to any network, system, or asset in Respondent's control that stores, collects, maintains, or processes Covered Information, including properly configured firewalls; intrusion detection and prevention systems configured to identify and prevent unauthorized access to networks, systems, or assets that store, process, or connect to networks, systems, or assets that store or process Covered Information; file integrity monitoring tools; data loss prevention tools; properly configured physical or logical segmentation of networks, systems, and databases;

restricting inbound connections to approved IP addresses; requiring that connections to the network, system, or asset are authenticated and encrypted; preventing the storage of unsecured access keys or other unsecured credentials on Respondent's networks, systems, or assets, or in any cloud-based services; requiring and enforcing strong passwords and other credentials;

b. For Respondent's employees and contractors, limit Authorized Users' access only to Covered Information that they need to perform their duties and functions, periodically audit Authorized Users' levels of access based on their need to know, and terminate access within 30 days following a change in Authorized Users' need to know (including because of the termination of employment or contract) or if Authorized Users engage in inappropriate access or usage; and

c. For Respondent's customers, limit Authorized Users' access only to their own Covered Information, and terminate access within 30 days following termination of the customer's access to the Covered Product in accordance with the customer's contract.

5. Policies and procedures to document in writing the content, implementation, and maintenance of an incident response plan designed to ensure the identification of, investigation of, and response to the unauthorized access to Covered Information. Such incident response plan must include policies and procedures to ensure the timely investigation of data security events and the timely remediation of critical and high-risk vulnerabilities. Respondent must revise and update this incident response plan to adapt to any changes to its networks, systems, and assets;

6. Regular security training programs, on at least an annual basis, that are updated, as applicable, to address internal or external risks identified by Respondent under sub-Provision D of this Order, and that include, at a minimum:

a. Security awareness training for all employees and service providers who have access to networks, systems, or assets that contain Covered Information on Respondent's security policies and procedures, including the requirements of this Order, to be conducted when an employee begins employment or takes on a new role in which the employee has access to networks, systems, or assets that contain Covered Information, and on at least an annual basis thereafter; and

b. For information security personnel, security updates and training sufficient to address relevant security risks.

7. Utilizing qualified information security personnel employed by Respondent or an affiliate or service provider sufficient to manage Respondent's information security risks and to perform or oversee the

Information Security Program, and verifying that key information security personnel take steps to maintain current knowledge of changing information security threats and countermeasures;

8. Protecting by encryption, at a minimum, databases in Covered Products designed to store all Covered Information held or transmitted by Respondent both in transit over external networks and at rest on Respondent's computer networks, including but not limited to cloud storage;

9. Requiring multi-factor authentication methods for all employees and contractors of Respondent in order to access any assets (including databases) storing Covered Information. Such multi-factor authentication methods for all employees and contractors of Respondent may not include telephone or SMS-based authentication methods and must be resistant to phishing attacks. Respondent may use widely adopted industry authentication options that provide at least equivalent security as the multi-factor authentication options required by this sub-Provision, if approved in writing by the Commission;

10. Technical measures, procedures, and policy provisions to address the maintenance of any new type of information related to consumers that was not being maintained as of the issuance date of this Order, including: (a) the purposes for which the new information is maintained; (b) the specific business needs for maintaining the new information; and (c) encryption of sensitive consumer information; and

11. Enforcing policies and procedures consistent with this Order designed to ensure the timely investigation of data security events and the timely remediation of critical and high-risk security vulnerabilities relating to Covered Information.

F. Assess, at least once every twelve (12) months and promptly (not to exceed one hundred and twenty (120) days) following a Covered Incident, the sufficiency of any safeguards in place to address the internal and external risks to the security, confidentiality, or integrity of Covered Information, and, if appropriate, modify the Information Security Program based on the results;

G. Test and monitor the effectiveness of the safeguards specified in this Provision at least once every twelve (12) months and promptly (not to exceed 120 days) following a Covered Incident and modify the Information Security Program based on the results. Such testing and monitoring must include vulnerability scanning of Respondent's network(s) containing Covered Information once every four months and promptly (not to exceed 120 days) after a Covered Incident, and penetration testing of Respondent's network(s) containing Covered Information at least once every twelve (12) months and promptly (not to exceed 120 days) after a Covered Incident;

H. Select and retain service providers capable of safeguarding Covered Information

they access through or receive from Respondent, and contractually require service providers to implement and maintain safeguards sufficient to address the internal and external risks to the security, confidentiality, or integrity of Covered Information; and

I. Evaluate and adjust the Information Security Program in light of any material changes to Respondent's operations or business arrangements, a Covered Incident, new or more efficient technological or operational methods to control for the risks identified in sub-Provision IV.D of this Order, or any other circumstances that Respondent knows or has reason to know may have an impact on the effectiveness of the Information Security Program or any of its individual safeguards. At a minimum, Respondent must evaluate the Information Security Program at least once every twelve (12) months and modify the Information Security Program based on the results.

V. Information Security Assessments by a Third Party

IT IS FURTHER ORDERED that, in connection with compliance with Provision IV of this Order titled Mandated Information Security Program and Data Management Procedures, Respondent must obtain initial and biennial assessments ("Assessments"):

A. The Assessments must be obtained from a qualified, objective, independent third-party professional ("Assessor"), who: (1) uses procedures and standards generally accepted in the profession; (2) conducts an independent review of the Information Security Program; (3) retains all documents relevant to each Assessment for five (5) years after completion of such Assessment: and (4) will provide such documents to the Commission within ten (10) days of receipt of a written request from a representative of the Commission. The Assessor may not withhold any documents relating to Assessments of Respondent from the Commission on the basis of a claim of confidentiality, proprietary or trade secrets, work product protection, attorney-client privilege, statutory protection, or any similar claim. Respondent may satisfy the requirements to obtain Assessments through the use of assessments that are also intended to meet the requirements of other regulatory mandates to which Respondent is subject, provided that such assessments meet the requirements of the Information Security Program set forth in this Order.

B. For each Assessment, Respondent must provide the Associate Director for Enforcement for the Bureau of Consumer Protection at the Federal Trade Commission with the name, affiliation, and qualifications of the proposed Assessor, whom the Associate Director will have the authority to approve in their sole discretion.

C. The reporting period for the Assessments must cover: (1) at least the first 180 days after the Information Security Program is established for the initial Assessment; and (2) each 2-year period thereafter for ten (10) years after issuance of the Order for the biennial Assessments.

D. Each Assessment must, for the entire assessment period:

(1) determine whether Respondent has implemented and maintained the Information Security Program required by Provision IV of this Order, titled Mandated Information Security Program and Data Management Procedures;

(2) assess the effectiveness of Respondent's implementation and maintenance of sub-Provisions IV.A-I;

(3) identify any gaps or weaknesses in, or instances of material noncompliance with, the Information Security Program;

(4) address the status of gaps or weaknesses in, or instances of material non-compliance with, the Information Security Program that were identified in any prior Assessment required by this Order; and

(5) identify specific evidence (including documents reviewed, sampling and testing performed, and interviews conducted) examined to make such determinations, assessments, and identifications, and explain why the evidence that the Assessor examined is (a) appropriate for assessing an enterprise of Respondent's size, complexity, and risk profile; and (b) sufficient to justify the Assessor's findings. No finding of any Assessment may rely primarily on assertions or attestations by Respondent's management. The Assessment must be signed by the Assessor, state that the Assessor conducted an independent review of the Information Security Program and did not rely primarily on assertions or attestations by Respondent's management and state the number of hours that each member of the Assessor's assessment team worked on the Assessment. To the extent that Respondent revises, updates, or adds one or more safeguards required under Provision IV of this Order during an Assessment period, the Assessment must assess the effectiveness of the revised, updated, or added safeguard(s) for the time period in which it was in effect, and provide a separate statement detailing the basis for each revised, updated, or additional safeguard.

E. The initial Assessment must be completed within one hundred and twenty (120) days after the end of the reporting period for the initial Assessment. Each subsequent biennial Assessment must be completed within sixty (60) days after the end of the reporting period to which the Assessment applies. Unless otherwise

directed by a Commission representative in writing, Respondent must submit the initial Assessment to the Commission within ten (10) days after the Assessment has been completed via email to DEbrief@ftc.gov or by overnight courier (not the U.S. Postal Service) to Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580. The subject line must begin, "In re Illuminate Education Inc., FTC File No. 2023105." Respondent must retain an unredacted copy of each subsequent biennial Assessment as well as a proposed redacted copy of each subsequent biennial Assessment suitable for public disclosure until the order is terminated and must provide each such Assessment to the Associate Director for Enforcement within ten (10) days of request. The initial Assessment and any subsequent biennial Assessment provided to the Commission must be marked, in the upper right-hand corner of each page, with the words "DPIP Assessment" in red lettering.

VI. Cooperation with Third Party Information Security Assessor

IT IS FURTHER ORDERED that Respondent, whether acting directly or indirectly, in connection with any Assessment required by Provision V of this Order titled Information Security Assessments by a Third Party, must:

A. Provide or otherwise make available to the Assessor all information and material in its possession, custody, or control that is relevant to the Assessment for which there is no reasonable claim of privilege;

B. Provide or otherwise make available to the Assessor information about Respondent's network(s) and all of Respondent's IT assets that maintain Covered Information so that the Assessor can determine the scope of the Assessment, and visibility to those portions of the network(s) and IT assets deemed in scope; and

C. Disclose all material facts to the Assessor, and not misrepresent in any manner, expressly or by implication, any fact material to the Assessor's: (1) determination of whether Respondent has implemented and maintained the Information Security Program required by Provision IV of this Order, titled Mandated Information Security Program and Data Management Procedures; (2) assessment of the effectiveness of the implementation and maintenance of sub-Provisions IV.A-I; or (3) identification of any gaps or weaknesses in, or instances of material noncompliance with, the Information Security Program.

VII. Annual Certification

IT IS FURTHER ORDERED that Respondent must:

A. One year after the issuance date of this Order, and each year thereafter, provide the Commission with a certification from Respondent's Chief Information Security Officer responsible for Respondent's Information Security Program that: (1) Respondent has established, implemented, and maintained the requirements of this Order; (2) Respondent is not aware of any material noncompliance that has

not been (a) corrected or (b) disclosed to the Commission; and (3) includes a brief description of all Covered Incidents during the certified period. The certification must be based on the personal knowledge of senior personnel or subject matter experts upon whom senior personnel reasonably relies in making the certification.

B. Unless otherwise directed by a Commission representative in writing, submit all annual certifications to the Commission pursuant to this Order via email to DEbrief@ftc.gov or by overnight courier (not the U.S. Postal Service) to Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580. The subject line must begin, "In re Illuminate Education Inc., FTC File No. 2023105."

VIII. Covered Incident Reports

IT IS FURTHER ORDERED that, within fourteen (14) days of any notification to a United States federal, state, or local entity of a Covered Incident, Respondent must submit a report to the Commission. The report must include, to the extent possible:

A. The date, estimated date, or estimated date range when the Covered Incident occurred;

B. A description of the facts relating to the Covered Incident, including the causes of the Covered Incident, if known;

C. A description of each type of information that triggered the notification;

D. The number of consumers whose information was affected by the Covered Incident;

E. The acts that Respondent has taken to date to remediate the Covered Incident and protect Covered Information from further exposure or access, and protect affected individuals from identity theft or other harm that may result from the Covered Incident;

F. As applicable, a statement that Respondent has received a request from a federal, state, or local law enforcement agency to delay notice to future affected consumers on the basis that such notice would interfere with an ongoing investigation and a copy of such request; and

G. A representative copy of any materially different notice sent by Respondent to its customers or consumers, or to any U.S. federal, state, or local government entity.

Unless otherwise directed by a Commission representative in writing, all Covered Incident reports to the Commission pursuant to this Order must be emailed to DEbrief@ftc.gov or sent by overnight courier (not the U.S. Postal Service) to Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580. The subject line must begin, "In re Illuminate Education Inc., FTC File No. 2023105."

IX. Order Acknowledgements

IT IS FURTHER ORDERED that Respondent obtain acknowledgments of receipt of this Order:

A. Respondent, within 10 days after the Order Effective Date, must submit to the Commission an acknowledgment of receipt of this Order sworn under penalty of perjury.

B. Respondent must deliver a copy of this Order to: (1) all principals, officers, and directors; (2) all employees, agents and representatives having managerial responsibilities for cybersecurity, privacy, and the collection, use, or disclosure of Covered Information; and (3) any business entity resulting from any change in structure as set forth in Provision X. Delivery must occur within 10 days of the Order Effective Date for current personnel. For all others, delivery must occur before they assume their responsibilities.

C. From each individual or entity to which Respondent delivered a copy of this Order, Respondent must obtain, within 30 days, a signed and dated acknowledgment of receipt of this Order.

X. Compliance Reporting

IT IS FURTHER ORDERED that Respondent make timely submissions to the Commission:

A. One year after issuance of this Order, Respondent must submit a compliance report, sworn under penalty of perjury. Respondent must:

1. Identify the primary physical, postal, and email address and telephone number, as designated points of contact, which representatives of the Commission may use to communicate with Respondent;

2. Identify all of Respondent's businesses by all of their names, telephone numbers, and physical, postal, email, and Internet addresses;

3. Describe the activities of each business, including the goods and services offered, the means of advertising, marketing, and sales;

4. Describe in detail whether and how Respondent is in compliance with each Provision of this Order; and

5. Provide a copy of each Order Acknowledgment obtained pursuant to this Order, unless previously submitted to the Commission.

B. For 10 years after issuance of this Order, Respondent must submit a compliance notice, sworn under penalty of perjury, within 14 days of any change in the following:

1. Any designated point of contact; or

2. The structure of Respondent or any entity that Respondent has any ownership interest in or controls directly or indirectly that may affect compliance obligations arising under this Order, including: creation, merger, sale, or dissolution of the entity or any subsidiary, parent, or affiliate that engages in any acts or practices subject to this Order.

C. Respondent must submit notice of the filing of any bankruptcy petition, insolvency proceeding, or similar proceeding by or against such Respondent within fourteen (14) days of its filing.

D. Any submission to the Commission required by this Order to be sworn under penalty of perjury must be true and accurate and comply with 28 U.S.C. § 1746, such as by concluding: "I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on: _____" and supplying the date, signatory's full name, title (if applicable), and signature.

E. Unless otherwise directed by a Commission representative in writing, all submissions to the Commission pursuant to this Order must be emailed to DEbrief@ftc.gov or sent by overnight courier (not the U.S. Postal Service) to: Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580. The subject line must begin: "In re Illuminate Education Inc., FTC File No. 2123105."

XI. Recordkeeping

IT IS FURTHER ORDERED that Respondent must create certain records for 10 years and retain each such record for 5 years. Specifically, Respondent must create and retain the following records:

A. Accounting records showing the revenues from all goods or services sold;

B. Personnel records showing, for each person providing services, whether as an employee or otherwise, that person's: name; addresses; telephone numbers; job title or position; dates of service; and (if applicable) the reason for termination;

C. Records of all customer and consumer complaints regarding security, privacy, or identity theft related to Covered Information whether received directly or indirectly, such as through a third party, and any response;

D. Copies of all subpoenas and other communications with law enforcement, if such communication relate to Respondent's compliance with this Order or relate to any Covered Incident;

E. A copy of each widely disseminated, unique advertisement or other marketing material making a representation subject to this Order;

F. A copy of each widely disseminated representation by Respondent that relates to

any Covered Incident or describes the extent to which Respondent maintains or protects the privacy, security and confidentiality of any Covered Information;

G. Records showing the Respondent's implementation of Provision III; and

H. All records necessary to demonstrate full compliance with each provision of this Order, including all submissions to the Commission.

XII. Compliance Monitoring

IT IS FURTHER ORDERED that, for the purpose of monitoring Respondent's compliance with this Order:

A. Within 14 days of receipt of a written request from a representative of the Commission, Respondent must: submit additional compliance reports or other requested information, which must be sworn under penalty of perjury; and produce documents for inspection and copying.

B. For matters concerning this Order, representatives of the Commission are authorized to communicate directly with Respondent. Respondent must permit representatives of the Commission to interview anyone affiliated with Respondent who has agreed to such an interview. The interviewee may have counsel present.

C. The Commission may use all other lawful means, including posing, through its representatives as consumers, suppliers, or other individuals or entities, to Respondent or any individual or entity affiliated with Respondent, without the necessity of identification or prior notice. Nothing in this Order limits the Commission's lawful use of compulsory process, pursuant to Sections 9 and 20 of the FTC Act, 15 U.S.C. §§ 49, 57b-1.

XIII. Order Effective Dates

IT IS FURTHER ORDERED that this Order is final and effective upon the date of its publication on the Commission's website (ftc.gov) as a final order (the "**Order Effective Date**"). This Order will terminate 10 years from the date of its issuance (which date may be stated at the end of this Order, near the Commission's seal), or 10 years from the most recent date that the United States or the Commission files a complaint (with or without an accompanying settlement) in federal court alleging any violation of this Order, whichever comes later; *provided, however*, that the filing of such a complaint will not affect the duration of:

A. Any Provision in this Order that terminates in less than 10 years;

B. This Order's application to any Respondent that is not named as a defendant in such complaint; and

C. This Order if such complaint is filed after the Order has terminated pursuant to this Provision.

Provided, further, that if such complaint is dismissed or a federal court rules that the Respondent did not violate any provision of the Order, and the dismissal or ruling is either not appealed or upheld on appeal, then the Order will terminate according to this Provision as though the complaint had never been filed, except that the Order will not terminate between the date such complaint is filed and the later of the deadline for appealing such dismissal or ruling and the date such dismissal or ruling is upheld on appeal.

By the Commission.

April J. Tabor
Secretary

SEAL:
ISSUED: