Analysis of Proposed Consent Order to Aid Public Comment
***In the Matter of Illuminate Education, Inc.,* File No. 2223105**

The Federal Trade Commission ("Commission") has accepted, subject to final approval, an agreement containing a consent order from Illuminate Education, Inc. ("Respondent").

The proposed consent order ("proposed order") has been placed on the public record for 30 days for receipt of public comments by interested persons. Comments received during this period will become part of the public record. After 30 days, the Commission will again review the agreement, along with the comments received, and will decide whether it should make final the proposed order or withdraw from the agreement and take appropriate action.

Respondent is a California corporation with its principal place of business in Wisconsin Rapids, WI. Respondent offers schools and districts a suite of software products and solutions, such as the IO Suite,[1] to help manage student information, assess literacy, track grades, communicate with parents, and determine students' academic and social-emotional behavior learning needs. In the course of providing its products and services, Respondent stores personal information of millions of students. The personal information includes students' name and address, parent contact information, grades, whether the student has specialized learning plans in place (such as Individualized Education Plans (IEP) or 504 Plans which can reveal special needs or disabilities), or whether the student receives free or reduced lunch.

The proposed complaint alleges that despite representing to school districts, students and their parents that it would keep their student personal information safe, Respondent failed to utilize reasonable information security measures to do so. The proposed complaint alleges that as a result of Respondent's unreasonable information security practices, a threat actor infiltrated Respondent's network, had unfettered access to students' personal information for 13 days, and exfiltrated millions of students' personal information.

The Commission's proposed three-count complaint alleges that Respondent violated Section 5(a) of the FTC Act by (1) unfairly failing to employ reasonable information security practices to protect students' personal information, (2) misrepresenting to school districts, students and their parents that it took reasonable steps to protect student personal information, and (3) misrepresenting to school districts that it would provide timely notifications regarding breach or unauthorized disclosure. With respect to the first count, the proposed complaint alleges that Respondent:

a) stored, until at least January 2022, students' personal information in 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;

[1] The IO suite of programs includes IO Admin, IO Assessment, IO Auth, IO Classroom, IO Compass, IO Insights, IO Messenger, and Data Driven Classroom.

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; and

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.

The proposed complaint alleges that Respondent could have addressed each of these failures by implementing readily available and relatively low-cost security measures.

The proposed complaint alleges that Respondent's failures caused, or are 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. Such practices constitute unfair acts or practices under Section 5 of the FTC Act.

With respect to the second count, the proposed complaint alleges that, at various times, Respondent represented to school districts, students and their parents that it used reasonable measures to protect student personal information. The proposed complaint alleges that, in reality, and as noted above, Respondent failed to implement reasonable measures to protect students' personal information. Such representations were, therefore, deceptive under Section 5 of the FTC Act.

Finally, the third count of the proposed complaint alleges that at various times Respondent represented that it would provide timely notifications to school districts whose data has been exposed as a result of a breach or unintended disclosure. The proposed complaint alleges that Respondent failed to timely notify school districts whose data had been exposed due to a breach or unintended disclosure. Such representations were, therefore, deceptive under Section 5 of the FTC Act.

Summary of Proposed Order with Respondent

The proposed order contains injunctive relief designed to prevent Respondent from engaging in the same or similar acts or practices in the future.

Part I prohibits Respondent from misrepresenting (1) the extent to which it protects the privacy, security, availability, confidentiality, or integrity of any covered information; and (2) the time period in which Respondent will notify school districts and students of a breach or unintended disclosure of any covered information as defined in the proposed order.

Part II requires that Respondent delete or destroy covered information that is not being retained in connection with providing products or services under Respondent's contracts with its customers or as requested by Respondent's customers.

Part III requires that Respondent document and adhere to a retention schedule for the covered information it collects from consumers, including the purposes for which it collects such information and the timeframe for its deletion.

Part IV requires Respondent to establish and implement, and thereafter maintain, a comprehensive information security program that protects the security, availability, confidentiality, and integrity of covered information.

Part V requires Respondent to obtain initial and biennial information security assessments by an independent, third-party professional for 10 years.

Part VI requires Respondent to disclose all material facts to the assessor required by **Part V** and prohibits Respondent from misrepresenting any fact material to the assessments required by **Part V**.

Part VII requires Respondent to submit an annual certification from the Chief Information Security Officer responsible for its information security program that the company has implemented the requirements of the Order and is not aware of any material noncompliance that has not been corrected or disclosed to the Commission.

Part VIII requires Respondent to notify the Commission any time it notifies a federal, state, or local government that information of or about a consumer was, or is reasonably believed to have been, accessed, acquired, or publicly exposed without authorization.

Parts IX - XII are reporting and compliance provisions, which include recordkeeping requirements and provisions requiring Respondent to provide information or documents necessary for the Commission to monitor compliance.

Part XIII states that the proposed order will remain in effect for 10 years, with certain exceptions.

The purpose of this analysis is to facilitate public comment on the proposed order, and it is not intended to constitute an official interpretation of the complaint or proposed order, or to modify the proposed order's terms in any way.