Analysis of Proposed Consent Order to Aid Public Comment
***In the Matter of Chegg, Inc.,* File No. 2023151**

The Federal Trade Commission ("Commission") has accepted, subject to final approval, an agreement containing a consent order from Chegg, 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 Delaware corporation with its principal place of business in California. Respondent offers an online platform through which consumers utilize Respondent's subscription-based study aids, which have included tutoring, writing assistance, math-problem solvers, and answers to common textbook questions. Respondent also has helped consumers search for potential scholarship opportunities. In the course of using its services, Respondent's tens of millions of users have provided the company with their email addresses, first and last names, and passwords. Users of the scholarship search service have also provided Respondent with their religious denominations, heritages, dates of birth, parents' income ranges, sexual orientations, and disabilities. In addition, Respondent collects Social Security numbers, financial account information, and other personal information from its employees.

Despite representing to consumers that it would keep their sensitive information safe, Respondent failed to utilize reasonable information security measures to do so. As a result of Respondent's inadequate information security practices, hackers infiltrated Respondent's networks and accessed consumers' personal information on multiple occasions over the course of several years.

The Commission's proposed two-count complaint alleges that Respondent violated Section 5(a) of the FTC Act by (1) failing to employ reasonable information security practices to protect consumers' personal information, and (2) misrepresenting to consumers that it took reasonable steps to protect their personal information. With respect to the first count, the proposed complaint alleges that Respondent:

- failed to implement reasonable access controls to safeguard users' personal information by failing to (1) require employees and third-party contractors to use distinct access keys to databases containing users' personal information, instead allowing them to use a single access key with full administrative privileges, (2) restrict access to systems based on employees' or contractors' job functions, (3) require multi-factor authentication for employee and contractor account access to users' personal information, and (4) rotate access keys to databases containing users' personal information;

- stored users' and employees' personal information on its network and databases in plain text, rather than encrypting the information;

- used outdated and unsecure cryptographic hash functions to protect users' passwords;

- failed to develop, implement, or maintain adequate written organizational information security standards, policies, procedures, or practices;

- failed to provide adequate guidance or training for employees or contractors regarding information security and safeguarding consumers' personal information;

- failed to have a policy, process, or procedure for inventorying and deleting users' and employees' personal information stored on Respondent's network after that information was no longer needed; and

- failed to adequately monitor its networks and systems for unauthorized attempts to transfer or exfiltrate users' and employees' personal information outside of Respondent's network boundaries.

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 claimed that it used reasonable measures to protect personal information of consumers. The proposed complaint alleges that, in reality, and as noted above, Respondent failed to implement reasonable measures to protect consumers' personal information. 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 the extent to which it (1) collects, maintains, uses, discloses, deletes, or permits or denies access to consumers' personal information, and (2) protects the privacy, security, availability, confidentiality, or integrity of consumers' personal information.

Part II requires that Respondent (1) document and adhere to a retention schedule for the personal information it collects from consumers, including the purposes for which it collects such information and the timeframe for its deletion, and (2) provide an opportunity for consumers to request access to, and/or deletion of, their personal information.

Part III requires that Respondent provide multi-factor authentication methods as an option for users of its services.

Part IV requires that Respondent provide notice to any consumer whose Social Security number, financial information, date of birth, user account credentials, or medical information was exposed in a breach identified in the proposed complaint, provided that the consumer has not previously received such notice.

Part V requires Respondent to establish and implement, and thereafter maintain, a comprehensive information security program that protects the security, availability, confidentiality, and integrity of consumers' personal information.

Part VI requires Respondent to obtain initial and biennial information security assessments by an independent, third-party professional for 20 years.

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

Part VIII requires Respondent to submit an annual certification from a senior corporate manager (or senior 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 IX requires Respondent to notify the Commission any time it notifies a federal, state, or local government that consumer personal information was, or is reasonably believed to have been, accessed, acquired, or publicly exposed without authorization.

Parts X-XIII 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 XIV states that the Proposed Order will remain in effect for 20 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.