This document is scheduled to be published in the Federal Register on 11/14/2022 and available online at **federalregister.gov/d/2022-24690**, and on **govinfo.gov**

BILLING CODE: 6750-01-P

FEDERAL TRADE COMMISSION

[File No. 202 3151]

Chegg, Inc.; Analysis of Proposed Consent Order to Aid Public Comment

AGENCY: Federal Trade Commission.

ACTION: Proposed consent agreement; request for comment.

SUMMARY: The consent agreement in this matter settles alleged violations of federal law prohibiting unfair or deceptive acts or practices. The attached Analysis of Proposed Consent Order to Aid Public Comment describes both the allegations in the draft complaint and the terms of the consent order—embodied in the consent agreement—that would settle these allegations.

DATES: Comments must be received on or before [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE *FEDERAL REGISTER*].

ADDRESSES: Interested parties may file comments online or on paper by following the instructions in the Request for Comment part of the **SUPPLEMENTARY INFORMATION** section below. Please write "Chegg, Inc.; File No. 202 3151" on your comment and file your comment online at *https://www.regulations.gov* by following the instructions on the web-based form. If you prefer to file your comment on paper, please mail your comment to the following address: Federal Trade Commission, Office of the Secretary, 600 Pennsylvania Avenue NW, Suite CC-5610 (Annex D), Washington, DC 20580.

FOR FURTHER INFORMATION CONTACT: Brian Shull (202-326-3734) or Genevieve Bonan (202-326-3139), Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580.

SUPPLEMENTARY INFORMATION: Pursuant to Section 6(f) of the Federal Trade Commission Act, 15 U.S.C. 46(f), and FTC Rule § 2.34, 16 CFR 2.34, notice is hereby

given that the above-captioned consent agreement containing a consent order to cease and desist, having been filed with and accepted, subject to final approval, by the Commission, has been placed on the public record for a period of 30 days. The following Analysis to Aid Public Comment describes the terms of the consent agreement and the allegations in the complaint. An electronic copy of the full text of the consent agreement package can be obtained at *https://www.ftc.gov/news-events/commission-actions*.

You can file a comment online or on paper. For the Commission to consider your comment, we must receive it on or before [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE *FEDERAL REGISTER*]. Write "Chegg, Inc.; File No. 202 3151" on your comment. Your comment—including your name and your state—will be placed on the public record of this proceeding, including, to the extent practicable, on the *https://www.regulations.gov* website.

Because of heightened security screening, postal mail addressed to the Commission will be subject to delay. We strongly encourage you to submit your comments online through the *https://www.regulations.gov* website.

If you prefer to file your comment on paper, write "Chegg, Inc.; File No. 202 3151" on your comment and on the envelope, and mail your comment to the following address: Federal Trade Commission, Office of the Secretary, 600 Pennsylvania Avenue NW, Suite CC-5610 (Annex D), Washington, DC 20580.

Because your comment will be placed on the publicly accessible website at *https://www.regulations.gov*, you are solely responsible for making sure your comment does not include any sensitive or confidential information. In particular, your comment should not include sensitive personal information, such as your or anyone else's Social Security number; date of birth; driver's license number or other state identification number, or foreign country equivalent; passport number; financial account number; or credit or debit card number. You are also solely responsible for making sure your

comment does not include sensitive health information, such as medical records or other individually identifiable health information. In addition, your comment should not include any "trade secret or any commercial or financial information which . . . is privileged or confidential"—as provided by Section 6(f) of the FTC Act, 15 U.S.C. 46(f), and FTC Rule § 4.10(a)(2), 16 CFR 4.10(a)(2)—including competitively sensitive information such as costs, sales statistics, inventories, formulas, patterns, devices, manufacturing processes, or customer names.

Comments containing material for which confidential treatment is requested must be filed in paper form, must be clearly labeled "Confidential," and must comply with FTC Rule § 4.9(c). In particular, the written request for confidential treatment that accompanies the comment must include the factual and legal basis for the request, and must identify the specific portions of the comment to be withheld from the public record. *See* FTC Rule § 4.9(c). Your comment will be kept confidential only if the General Counsel grants your request in accordance with the law and the public interest. Once your comment has been posted on the *https://www.regulations.gov* website—as legally required by FTC Rule § 4.9(b)—we cannot redact or remove your comment from that website, unless you submit a confidentiality request that meets the requirements for such treatment under FTC Rule § 4.9(c), and the General Counsel grants that request.

Visit the FTC Website at *http://www.ftc.gov* to read this document and the news release describing the proposed settlement. The FTC Act and other laws the Commission administers permit the collection of public comments to consider and use in this proceeding, as appropriate. The Commission will consider all timely and responsive public comments it receives on or before [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE *FEDERAL REGISTER*]. For information on the Commission's privacy policy, including routine uses permitted by the Privacy Act, see *https://www.ftc.gov/site-information/privacy-policy*.

Analysis of Proposed Consent Order to Aid Public Comment

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 from 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. While 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 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 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 Respondent could have addressed each of these failures by implementing readily available and relatively low-cost security measures. It also alleges 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 it used reasonable measures to protect personal information of consumers. The proposed complaint alleges 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 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 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.

By direction of the Commission.

April J. Tabor,

Secretary.

[FR Doc. 2022-24690 Filed: 11/10/2022 8:45 am; Publication Date: 11/14/2022]