2023151

UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

COMMISSIONERS: **Lina M. Khan, Chair**
Rebecca Kelly Slaughter
Christine S. Wilson
Alvaro M. Bedoya

In the Matter of **CHEGG, INC., a corporation.**	**DECISION AND ORDER** **DOCKET NO. C-**

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 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 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. The Respondent is Chegg, Inc., a Delaware corporation with its principal office or place of business at 3990 Freedom Circle, Santa Clara, CA 95054.

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

For purposes of this Order, the following definitions apply:

A. "**April 2018 Breach**" means the exposure of individuals' Covered Information from systems of or controlled by Respondent in or about April 2018.

B. "**April 2020 Breach**" means the exposure of individuals' Covered Information from systems of or controlled by Respondent in or about April 2020.

C. "**Clear and Conspicuous**" or "**Clearly and Conspicuously**" means that a required disclosure is difficult to miss (*i.e.*, easily noticeable) and easily understandable by ordinary consumers, including in all of the following ways:

1. In any communication that is solely visual or solely audible, the disclosure must be made through the same means through which the communication is presented. In any communication made through both visual and audible means, such as a television advertisement, the disclosure must be presented simultaneously in both the visual and audible portions of the communication even if the representation requiring the disclosure ("triggering representation") is made through only one means.

2. A visual disclosure, by its size, contrast, location, the length of time it appears, and other characteristics, must stand out from any accompanying text or other visual elements so that it is easily noticed, read, and understood.

3. An audible disclosure, including by telephone or streaming video, must be delivered in a volume, speed, and cadence sufficient for ordinary consumers to easily hear and understand it.

4. In any communication using an interactive electronic medium, such as the Internet or software, the disclosure must be unavoidable.

5. The disclosure must use diction and syntax understandable to ordinary consumers and must appear in each language in which the triggering representation appears.

6. The disclosure must comply with these requirements in each medium through which it is received, including all electronic devices and face-to-face communications.

7. The disclosure must not be contradicted or mitigated by, or inconsistent with, anything else in the communication.

8. When the representation or sales practice targets a specific audience, such as children, the elderly, or the terminally ill, "ordinary consumers" includes reasonable members of that group.

D. "**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.

E. "**Covered Information**" means information from or about an individual consumer, 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) geolocation information sufficient to identify street name and name of a city or town; (h) credit or debit card information (including a partial credit or debit card number with more than 5 digits); (i) user ID, or other persistent identifier that can be used to recognize a user over time and across different devices, websites, or online services; or (j) user account credentials, such as a login name and password (whether plain text, encrypted, hashed, and/or salted). "Covered Information" does not include information that a user intends to make public using Respondent's services.

F. "**Identified Breaches**" includes the September 2017 Breach, April 2018 Breach, June 2019 Breach, and April 2020 Breach.

G. "**June 2019 Breach**" means the exposure of individuals' Covered Information from systems of or controlled by Respondent that was discovered in or about June 2019.

H. "**Medical Information**" means information relating to the health of an individual consumer, including but not limited to medical history information, prescription information, hospitalization information, clinical laboratory testing information, health insurance information, or physician exam notes.

I. "**Respondent"** means Chegg, Inc., a Delaware corporation, and its successors and assigns.

J. "**September 2017 Breach**" means the exposure of individuals' Covered Information from systems of or controlled by Respondent in or about September 2017.

Provisions

I. Prohibition Against Misrepresentations

IT IS ORDERED that Respondent, and Respondent's officers, agents, employees, and attorneys, 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 promoting or offering for sale any product or service, must not misrepresent in any manner, expressly or by implication:

A. The extent to which Respondent collects, maintains, uses, discloses, deletes, or permits or denies access to any Covered Information; and

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

II. Data Retention and Deletion

IT IS FURTHER ORDERED that Respondent, within 60 days after issuance of this Order, must:

A. Document and adhere to a retention schedule for Covered Information. Such schedule shall set forth: (1) the purpose or purposes for which each type of Covered Information is collected; (2) the specific business needs for retaining each type of Covered Information; and (3) a set timeframe for deletion of each type of Covered Information (absent any intervening deletion requests from consumers) that precludes indefinite retention of any Covered Information; and

B. Provide a Clear and Conspicuous link on the homepage and initial login page of Respondent's websites directing consumers to an online form through which they can request access to or the deletion of their Covered Information. Respondent must respond to and fulfill every request either in accordance with the applicable consumer data access and deletion rights and related procedures prescribed by applicable law in the consumer's jurisdiction of residence or, if the location of the consumer's residence is unknown to Respondent, or if there are no applicable laws in the consumer's jurisdiction that provide for consumer rights to access or delete Covered Information, then in accordance with the consumer data access and deletion rights afforded by law to residents of the state in which Respondent's principal executive offices are located. If there are no laws that provide consumers with rights to access or delete Covered Information within the state in which Respondent's principal executive offices are located, then Respondent must fulfill any such requests within 45 days of receiving them. The time period to respond to the request may be extended once by an additional 45 days when reasonably necessary, provided the consumer is provided notice of the extension within the first 45-day period.

   Provided, however, that any Covered Information that Respondent is otherwise required to delete or destroy pursuant to this provision may be retained, and may be disclosed, as requested by a government agency or 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, or pursuant to written policies Clearly and Conspicuously posted on Respondent's websites relating to investigations or disciplinary actions by educational institutions concerning academic integrity.

III. Multi Factor Authentication for Users

IT IS FURTHER ORDERED that within six months after issuance of this Order, Respondent must provide multi-factor authentication methods as an option or as a requirement for consumer users. This time period may be extended for a reasonable time if such extension is approved in writing by a representative of the Commission. Respondent must not use, provide access to, or disclose any information collected for multi-factor authentication for any other purpose, unless such information is obtained separate and apart from enabling multi-factor authentication. Respondent may use equivalent, widely adopted industry authentication options that are not multi-factor, if the person responsible for the Information Security Program under sub-Provision V.C: (1) approves in writing the use of such equivalent authentication options; and (2) documents a written explanation of how the authentication options are widely adopted and at least equivalent to the security provided by multi-factor authentication.

IV. Notice to Individuals

IT IS FURTHER ORDERED that Respondent, within 60 days after issuance of this Order, must provide a notice to each individual whose unencrypted Social Security number, financial account information, date of birth, user account credentials, or Medical Information was exposed in an Identified Breach, to the extent such individual has not already previously been sent notification by Respondent. The notice shall be delivered by email and shall include an exact copy of the notice attached hereto as Attachment A ("Identified Breaches Notice"), with the subject line "Information about Chegg Data Breach." Respondent must not include with the Identified Breaches Notice any other information, documents, or attachments.

V. Mandated Information Security Program

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

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

B. Provide the written program and any evaluations thereof or material updates thereto 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 12 months and promptly (not to exceed 30 days) after a Covered Incident;

C. Designate a qualified employee to coordinate and be responsible for the Information Security Program;

D. Assess and document, at least once every 12 months and promptly (not to exceed 30 days) following a Covered Incident, internal and external risks to the security, confidentiality, or integrity of Covered Information that could result in the (1) unauthorized collection, maintenance, use, or disclosure of, or provision of access to, Covered Information; or the (2) misuse, loss, theft, alteration, destruction, or other compromise of such information;

E. Design, implement, maintain, and document safeguards that control for the internal and external risks Respondent identifies to the security, confidentiality, availability, or integrity of Covered Information identified in response to sub-Provision V.D. Each safeguard must take into account 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, alteration, or disclosure of, or provision of access to, Covered Information; or the (2) misuse, loss, theft, destruction, or other compromise of such information. Such safeguards must also include:

1. Training of all of Respondent's employees, at least once every 12 months, on how to safeguard Covered Information;

2. Documenting 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. Respondent shall revise and update this incident response plan to adapt to any changes to its assets or networks;

3. Implementing technical measures to log and monitor Respondent's networks and assets for anomalous activity and active threats. Such measures shall require Respondent to determine baseline system activity and identify and respond to anomalous events and unauthorized attempts to access or exfiltrate Covered Information;

4. Policies and procedures to minimize data collection, storage, and retention, including data deletion or retention policies and procedures;

5. Implementing data access controls for all assets (including databases) storing Covered Information and technical measures, policies, and procedures to minimize or prevent online attacks resulting from the misuse of valid credentials, including: (a) restricting inbound and outbound connections; (b) requiring and enforcing strong passwords or other credentials; (c) preventing the reuse of known compromised credentials to access Covered Information; (d) implementing automatic password resets for known compromised credentials; and (e) limiting employee access to what is needed to perform that employee's job function;

6. Requiring multi-factor authentication methods for all employees, contractors, and affiliates in order to access any assets (including databases) storing Covered Information. Such multi-factor authentication methods for all employees, contractors, and affiliates should not include telephone or SMS-based

authentication methods and must be resistant to phishing attacks. Respondent may use equivalent, widely adopted industry authentication options that are not multi-factor, if the person responsible for the Information Security Program under sub-Provision V.C: (1) approves in writing the use of such equivalent authentication options; and (2) documents a written explanation of how the authentication options are widely adopted and at least equivalent to the security provided by multi-factor authentication;

7. Developing and implementing configuration standards to harden system components against known threats and vulnerabilities. New system components shall not be granted access to Respondent's network, resources, or Covered Information until they meet Respondent's configuration standards;

8. Encryption of, at a minimum, all Social Security numbers, passport numbers, financial account information, tax information, dates of birth associated with a user's account, Medical Information associated with a user's account, and user account credentials on Respondent's computer networks, including but not limited to cloud storage;

9. Policies and procedures to ensure that all information technology ("IT") assets on Respondent's network with access to Covered Information are securely installed and inventoried at least once every 12 months;

10. Implementing vulnerability and patch management measures, policies, and procedures that require confirmation that any directives to apply patches or remediate vulnerabilities are received and completed and that include timelines for addressing vulnerabilities that account for the severity and exploitability of the risk implicated; and

11. Enforcing policies and procedures to ensure the timely investigation of data security events and the timely remediation of critical and high-risk security vulnerabilities.

F. Assess, at least once every 12 months and promptly (not to exceed 30 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 modify the Information Security Program based on the results;

G. Assess, prior to the acquisition of any entity that maintains, processes, or transmits Covered Information ("Acquired Entity"), the effectiveness of that entity's safeguards to protect such information. Either during the acquisition due diligence process or following such acquisition, Respondent must independently test the effectiveness of the Acquired Entity's safeguards to protect Covered Information. Respondent shall not integrate any application or information system into its network(s) until (1) all material risks to the security, confidentiality, and integrity of Covered Information identified in such a test are remediated; and (2) such application or information system meets the requirements of this Provision. *Provided, however,* that Respondent shall have 90 days

after integrating any application or information system of an acquired entity into its networks to implement the requirements of sub-Provision V.E.6 with respect to such application or system.

H. Test and monitor the effectiveness of the safeguards at least once every 12 months and promptly (not to exceed 30 days) following a Covered Incident and modify the Information Security Program based on the results. Such testing and monitoring must include vulnerability testing of Respondent's networks once every six months and promptly (not to exceed 30 days) after a Covered Incident, and penetration testing of Respondent's networks at least once every 12 months and promptly (not to exceed 30 days) after a Covered Incident;

I. 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

J. Evaluate and adjust the Information Security Program in light of any 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 V.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 12 months and modify the Information Security Program based on the results.

VI. Information Security Assessments By A Third Party

IT IS FURTHER ORDERED that, in connection with compliance with Provision V, Respondent shall 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 5 years after completion of such Assessment; and (4) will provide such documents to the Commission within ten days of receipt of a written request from a representative of the Commission. The Assessor may not withhold any documents from the Commission on the basis of a claim of confidentiality, proprietary or trade secrets, work product protection, attorney-client privilege, statutory exemption, or any similar claim.

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 shall have the authority to approve in her or his sole discretion.

C. The reporting period for the Assessments must cover: (1) the first 180 days after the issuance date of the Order for the initial Assessment; and (2) each two-year period thereafter for 20 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 V of this Order;

2. Assess the effectiveness of Respondent's implementation and maintenance of sub-Provisions V.A-J of this Order;

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 shall 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 assessment team worked on the Assessment. To the extent that Respondent revises, updates, or adds one or more safeguards required under Provision V 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. Each Assessment must be completed within 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 an unredacted copy of the initial Assessment to the Commission within 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 Chegg, Inc." 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 and provide to the Associate Director for Enforcement within 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.

VII. Cooperation With Third-Party Information Security Assessor

IT IS FURTHER ORDERED that Respondent, in connection with any Assessment required by Provision VI of this Order, shall:

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 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 V of this Order; (2) assessment of the effectiveness of the implementation and maintenance of sub-Provisions V.A-J of this Order; or (3) identification of any gaps or weaknesses in, or instances of material noncompliance with, the Information Security Program.

VIII. Annual Certifications

IT IS FURTHER ORDERED that Respondent shall:

A. One year after the issuance date of this Order, and each year thereafter, provide the Commission with a certification from the a senior corporate manager, or, if no such senior corporate manager exists, a senior officer of Respondent responsible for Respondent's Information Security Program that: (1) Respondent has established, implemented, and maintained the requirements of this Order; and (2) Respondent is not aware of any material noncompliance that has not been (a) corrected or (b) disclosed to the Commission. The certification must be based on the personal knowledge of a senior corporate manager, or, if no such senior corporate manager exists, a senior officer of Respondent responsible for Respondent's Information Security Program, or subject matter experts upon whom the senior corporate manager, or, if no such senior corporate manager exists, a senior officer of Respondent responsible for Respondent's Information Security Program 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 Chegg"

IX. Covered Incident Reports

IT IS FURTHER ORDERED that, within ten days of any notification to a United States federal, state, or local entity of a Covered Incident, Respondent shall 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 was affected by the Covered Incident;

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; and

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

G. 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 Chegg, Inc."

X. Order Acknowledgments

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

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

B. For 5 years after issuance of this Order, Respondent must deliver a copy of this Order to: (1) all principals, officers, and directors; (2) all employees having managerial responsibilities for cybersecurity, privacy, and the collection, use, or disclosure of Covered Information and all agents and representatives who participate in 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 XI. Delivery must occur within 10 days of issuance of this Order 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.

XI. 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: (a) 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; (b) identify all of Respondent's businesses by all of their names, telephone numbers, and physical, postal, email, and Internet addresses; (c) describe the activities of each business, including the goods and services offered, the means of advertising, marketing, and sales; (d) describe in detail whether and how Respondent is in compliance with each Provision of this Order; and (e) provide a copy of each Order Acknowledgment obtained pursuant to this Order, unless previously submitted to the Commission.

B. For 12 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: (a) any designated point of contact; or (b) the structure of 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 to the Commission notice of the filing of any bankruptcy

petition, insolvency proceeding, or similar proceeding by or against Respondent within 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 Chegg, Inc."

XII. Recordkeeping

IT IS FURTHER ORDERED that Respondent must create certain records for 12 years after issuance of the Order 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 consumer complaints and refund requests, whether received directly or indirectly, such as through a third party, and any response;

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

E. A copy of each widely disseminated, unique advertisement or other marketing material that references or otherwise relates to: (a) Respondent's privacy and data security practices; or (b) Respondent's websites or online services offered by Respondent that, if any, are directed at students in grades kindergarten through seventh grade.

XIII. 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; appear for depositions; and produce documents for inspection and copying. The Commission is also authorized to obtain discovery, without further leave of court, using any of the procedures prescribed by Federal Rules of Civil Procedure 29, 30 (including telephonic depositions), 31, 33, 34, 36, 45, and 69.

B. For matters concerning this Order, the Commission is authorized to communicate directly with Respondent. Respondent must permit representatives of the Commission to interview any employee or other person affiliated with Respondent who has agreed to such an interview. The person interviewed 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.

XIV. 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. This Order will terminate 20 years from the date of its issuance (which date may be stated at the end of this Order, near the Commission's seal), or 20 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 20 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:

Attachment A

[To be sent via email to last known email address from Respondent's CEO]

SUBJECT: Chegg data breach involving your personal information

Dear [Name],

We're writing because personal information about you that Chegg collected was stolen in one or more cyberattacks between 2017 and 2020. The unknown attackers could use your information at any time to commit identity theft or could sell it to other criminals. The Federal Trade Commission (FTC) sued us, alleging that we didn't provide reasonable security for your information. We're sending you this notice as part of a settlement with the FTC. Here's important information for you.

[For people affected by the September 2017 Breach]
About the Data Breach That Exposed Your Information [For people whose data was exposed in more than one breach, title the section "About the Data Breaches That Exposed Your Information"]
Your personal information was exposed in a September 2017 breach that affected some of our employees. The exposed information included your direct deposit information, [add, if applicable, Social Security number, financial account information, date of birth, and Okta username and password].

[For people affected by the April 2018 Breach]
About the Data Breach That Exposed Your Information
Your personal information was exposed in an April 2018 breach that affected users of our Chegg Study platform. The exposed information included your account email address and password [add, if applicable, Social Security number, financial account information, Medical Information, disability, birthday, first and last name, sexual orientation, religion, heritage, gender, ethnicity, citizenship, and parents' income range].

[For people affected by the June 2019 Breach]
About the Data Breach That Exposed Your Information
Your personal information was exposed in a June 2019 breach of the email inbox of one of our employees. The exposed information included your name [add, if applicable, Social Security number, financial account information, and Medical Information].

[For people affected by the April 2020 Breach]
About the Data Breach That Exposed Your Information
Your personal information was exposed in an April 2020 breach that affected current and former employees. The exposed information included your Social Security number, name, and address.

What You Can Do to Protect Yourself
These steps can help reduce your risk of identity theft.

1. Get your free credit report and review it for signs of identity theft. Order your free credit report at AnnualCreditReport.com. Review it for accounts and activity you don't recognize. If you discover that someone is misusing your personal information, visit IdentityTheft.gov to report and recover from identity theft. Recheck your credit reports periodically.

2. Place a credit freeze or fraud alert on your credit report. A credit freeze, also known as a security freeze, restricts access to your credit report. That means potential creditors can't get your credit report without your permission, making it less likely that an identity thief can open new accounts in your name. A freeze is free and remains in place until you ask the credit bureau to temporarily lift or remove it.

A fraud alert makes it harder for someone to open a new credit account in your name. It tells creditors to contact you before they open any new accounts in your name or change your accounts. A fraud alert is free and lasts for one year. After a year, you can renew it.

To freeze your credit report, contact **each of the three nationwide credit bureaus**, Equifax, Experian, and TransUnion. To place a fraud alert, contact **any one of the three nationwide credit bureaus**. The credit bureau you contact must tell the other two to place a fraud alert on your credit report.

Credit bureau contact information

Equifax
equifax.com/personal/credit-report-services
1-800-685-1111

Experian
experian.com/help
1-888-397-3742

TransUnion
transunion.com/credit-help
1-888-909-8872

Learn more about free credit freezes and fraud alerts at consumer.ftc.gov/articles/what-know-about-credit-freezes-and-fraud-alerts.

3. Visit IdentityTheft.gov/databreach. Get detailed information about steps to take to help protect yourself based on the type of personal information that was exposed.

What We're Doing to Protect Your Personal Information
As part of our settlement with the FTC, we're actively working on making changes to better protect your personal information and give you more control over it. We're planning to include easy-to-use options for you to access or delete your personal information, additional encryption protections for sensitive information we hold, and new multi-factor authentication options for

you to use when accessing our Chegg services. For more information about these upcoming changes, visit [link to FTC webpage hosting agreement containing consent order].

For More Information
If you have questions or concerns, please contact us at privacy@chegg.com or at 855-477-0177.

CHEGG CEO