202-3151

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,	**DOCKET NO.**

COMPLAINT

The Federal Trade Commission, having reason to believe that Chegg, Inc., a corporation, has violated the provisions of the Federal Trade Commission Act, and it appearing to the Commission that this proceeding is in the public interest, alleges:

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

2. Chegg markets and sells direct-to-student educational products and services. Its "Required Materials" service includes selling and renting textbooks to students. Its "Chegg Services" products and services include online learning aids, such as online tutoring, writing assistance, a math-problem solver, and answers to common textbook questions. Chegg has asserted that the target audience for its services are primarily high school and college students.

3. The acts and practices of Chegg alleged in this complaint have been in or affecting commerce, as "commerce" is defined in Section 4 of the Federal Trade Commission Act.

Data Security

4. In providing its services, Chegg collects sensitive personal information from users. For example, in connection with its scholarship search service, Chegg has collected information about a user's religious denomination, heritage, date of birth, parents' income range, sexual orientation, and disabilities (collectively, the "Scholarship Search Data"). In a 2018 internal email, Chegg's employee in charge of cybersecurity described the Scholarship Search Data as "very sensitive."

5. As another example, in connection with its online tutoring services, Chegg recorded videos of tutoring sessions that included Chegg users' images and voices.

6. Chegg has also collected sensitive personal information from its employees in the course of employment. This includes employees' names, dates of birth, Social Security numbers, and financial information.

Chegg's Amazon S3 Storage

7. As part of its information technology infrastructure, Chegg uses a third-party service provided by Amazon Web Services called the Simple Storage Service ("S3"). S3 is a scalable cloud storage service that can be used to store and retrieve large amounts of data. The S3 stores data inside virtual containers, called "buckets," against which individual access controls can be applied.

8. Chegg relies on S3 buckets to store a wide variety of files that contain users' sensitive personal information, including their names, passwords, dates of birth, and Scholarship Search Data (collectively, the "S3 User Data").

Chegg's Lax Security Practices

9. From at least 2017 to the present, Chegg has engaged in a number of practices that, taken individually or together, failed to provide reasonable security to prevent unauthorized access to users' personal information. These shortcomings also failed to provide reasonable security for the personal information Chegg collects from its employees, which has similarly resulted in unauthorized access to that information. Among other things, Chegg:

a) failed to implement reasonable access controls to safeguard users' personal information stored in S3 databases until at earliest October 2018. Specifically, Chegg:

   i) failed to require employees and third-party contractors that access the S3 databases to use distinct access keys, instead permitting employees and contractors to use a single AWS access key that provided full administrative privileges over all data in the S3 databases ("AWS Root Credentials");

   ii) failed to restrict access to systems based on employees' or contractors' job functions;

   iii) failed to require multi-factor authentication for account access to the S3 databases; and

   iv) failed to rotate access keys to the S3 databases;

b) stored users' and employees' personal information on Chegg's network and databases, including S3 databases, in plain text, rather than encrypting the information;

c) used, until at least April 2018, outdated and unsecure cryptographic hash functions to protect users' passwords;

d) failed, until January 2021, to develop, implement, or maintain adequate written organizational information security standards, policies, procedures, or practices;

e) failed, until at earliest April 2020, to provide adequate guidance or training for employees or third-party contractors regarding information security and safeguarding users' and employees' personal information, including, but not limited to, failing to require employees to complete any data security training;

f) failed to have a policy, process, or procedure for inventorying and deleting users' and employees' personal information stored on Chegg's network after that information is no longer necessary; and

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

Chegg's Security Failures Led to Multiple Breaches

10. Chegg's failure to provide reasonable security for the personal information it collected from users and employees has led to the repeated exposure of that personal information.

11. In or around September 2017, Chegg employees fell for a phishing attack, giving the threat actors access to employees' direct deposit information. Prior to the hack, Chegg did not require employees to complete any data security training, including identifying and appropriately responding to phishing attacks; this failure contributed to the security incident.

12. In or around April 2018, a former contractor accessed one of Chegg's S3 databases using an AWS Root Credential. Although Amazon had provided public guidance to protect AWS Root Credentials "like you would your credit card numbers or any other sensitive secret" and that Amazon "strongly recommend[s] that you do not use the root user for your everyday tasks, even the administrative ones," Chegg shared the AWS Root Credentials among its employees and even outside contractors. Using the AWS Root Credentials, the former contractor exfiltrated a database containing personal information of approximately 40 million users of the Chegg platform. The exposed personal information included the S3 User Data consisting of users' email addresses, first and last names, passwords, and, for certain Chegg users, their Scholarship Search Data, consisting of their religious denomination, heritage, date of birth, parents' income range, sexual orientation, and disabilities. Although Chegg had stored passwords in a hashed format—appearing as a random set of numbers and letters based on a cryptographic tool—it had stored the remaining information in plain text in the S3 database. Moreover, Chegg encrypted users' passwords using the MD5 hash function, a cryptographic function that had been deprecated by experts for years prior to April 2018. Had Chegg employed reasonable access controls and monitoring, it would have likely detected and/or stopped the attack more quickly.

13. In September 2018, a threat intelligence vendor informed Chegg that a file containing some of the exfiltrated information was available in an online forum. Chegg reviewed the file as part of its own investigation, finding it held, among other things, approximately 25 million of the exfiltrated passwords in plain text, meaning the threat actors had cracked the hash for those passwords. Chegg required approximately 40 million Chegg platform users to reset their

passwords. And, while Chegg implemented some access controls—rotating credentials and creating credentials with access permissions tailored to an employee's job functions—it failed to address, and allowed to persist, the remaining data securities failures laid out in sub-Paragraphs 9.b-e. For example, Chegg continues to store consumer personal information in plain text in its AWS S3 buckets.

14. In or around April 2019, a senior Chegg executive fell victim to a phishing attack, giving the threat actor access to the executive's credentials to Chegg's email platform and exposing personal information about consumers and employees of Chegg. This executive's email system was in a default configuration state that allowed employees, as well as threat actors, to bypass Chegg's multifactor authentication requirement while accessing the email platform. The threat actor exploited this shortfall and gained access to the executive's email inbox, which contained the personal information of Chegg users and employees, including their financial and medical information. If Chegg had appropriately configured its systems to ensure that employee access to the email platform required the employee to go through Chegg's multifactor authentication process, this phishing attack, and the resulting exposure of consumer and employee personal information, could have been stopped. In addition, Chegg's failure to require employees to complete any data security training, including training to identify and respond to phishing attacks, contributed to the security incident.

15. In or around April 2020, Chegg's senior employee responsible for payroll fell victim to a phishing attack, giving the threat actor access to the employee's credentials to Chegg's payroll system. The threat actor exfiltrated the W-2 information, including the birthdates and Social Security numbers, of approximately 700 current and former employees. Despite Chegg employees falling victim to phishing attacks on at least two prior occasions, Chegg still did not require, in or before April 2020, its employees to complete any data security training, including identifying and appropriately responding to phishing attacks.

Injury to Consumers

16. The information collected by Chegg, including users' and employees' medical conditions and financial information, together with identifying information such as their names, email addresses, passwords, birthdates, and Social Security numbers, is highly sensitive.

17. Chegg's failure to provide reasonable security for users' and employees' personal information has caused or is likely to cause substantial injury to those users and employees in the form of fraud, identity theft, monetary loss, stigma, embarrassment, emotional distress, and time spent remedying or attempting to prevent any of these potential injuries.

18. In particular, medical and financial information is valuable on the open market, and wrongdoers frequently seek to purchase users' financial and health information on the dark web. This information is often used to commit identity theft and fraud. For example, identity thieves use stolen names, addresses, and Social Security numbers to apply for credit cards in the victim's name. When the identity thief fails to pay credit card bills, the victim's credit suffers.

19. In addition, because people often use the same email addresses and passwords for multiple accounts, exposure of such user credentials open users up to additional attacks by threat

actors, including credential stuffing attacks. A credential stuffing attack is when a threat actor uses stolen credentials from one website to access user accounts on a different website. Thus, for example, a threat actor could use the email address and cracked passwords exfiltrated from the Chegg S3 bucket that the threat intelligence vendor found in the online forum to attempt to access the users' financial accounts on other websites.

20. Even if identity theft and fraud do not occur immediately after a breach, a breach of personal information such as that stored in Chegg's system makes identity theft and fraud more likely in the future.

21. Furthermore, due to Chegg's failure to appropriately monitor its systems and lack of access controls and authentication protections for its S3 databases, users' and employees' personal information, including health information and financial information, may have been exposed in other instances—beyond the incidents described in Paragraphs 11-15—without Chegg's knowledge.

22. The harms described in Paragraphs 16-21 were not reasonably avoidable by users or employees, as users had no way to know about Chegg's information security shortcomings.

23. Further, the harms are not outweighed by any countervailing benefits to users or competition. Chegg could have prevented or mitigated these information security failures through readily available, and relatively low-cost, measures. For example, as part of its AWS service, Amazon offers server-side encryption that encrypts data at rest (such as the S3 User Data) using encryption keys managed by Amazon.

Chegg's Deceptive Security Statements

24. From at least March 2017 to January 2020, Chegg disseminated, or caused to be disseminated, a privacy policy that expressly applied to Chegg's websites, apps, and other services. During this time period, the privacy policy contained the following claim regarding the security measures Chegg used to protect the personal information it collected from users: "Chegg takes commercially reasonable security measures to protect the Personal Information submitted to us, both during transmission and once we receive it."

25. From January 2020 to the present, Chegg's privacy policy contained the following statement concerning that same personal information: "We take steps to ensure that your information is treated securely and in accordance with this Privacy Policy."

Count I
Unfair Data Security Practices

26. As described in Paragraphs 16-23, Chegg's failure to employ reasonable and appropriate measures to protect personal information caused or is 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. This practice is an unfair act or practice.

Count II
Data Security Misrepresentations

27. As described in Paragraphs 24-25, Chegg has represented, directly or indirectly, expressly or by implication, that it implemented reasonable measures to protect personal information against unauthorized access.

28. In fact, as set forth in Paragraph 9, Chegg did not implement reasonable measures to protect personal information against unauthorized access. Therefore, the representation set forth in Paragraph 27 is false or misleading.

Violations of Section 5

29. The acts and practices of Respondent as alleged in this complaint constitute unfair or deceptive acts or practices in or affecting commerce in violation of Section 5(a) of the Federal Trade Commission Act.

THEREFORE, the Federal Trade Commission this _____ day of _____, 20__, has issued this Complaint against Respondent.

By the Commission.

April J. Tabor
Secretary

SEAL: