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

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 bypao[(pe)-1u(—)Ta(e ex

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.

<u>Violations of Section 5</u>

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 WKday of -DQXU\, 20, has issued this Complaint against Respondent.

By the Commission.

April J. Tabor
Secretary

SEAL: