FTC Brings Action Against Ed Tech Provider Chegg for Careless Security that Exposed Personal Data of Millions of Customers

FTC order against Chegg will require company to shore up its security against data breaches, and delete unnecessary data

October 31, 2022

The Federal Trade Commission is taking action against education technology provider Chegg Inc. for its lax data security practices that exposed sensitive information about millions of its customers and employees, including Social Security numbers, email addresses and passwords. Chegg allegedly failed to fix problems with its data security despite experiencing four security breaches since 2017. The FTC's proposed order requires the company to bolster its data security, limit the data the company can collect and retain, offer users multifactor authentication to secure their accounts, and allow users to access and delete their data.

"Chegg took shortcuts with millions of students' sensitive information," said Samuel Levine, Director of the FTC's Bureau of Consumer Protection. "Today's order requires the company to strengthen security safeguards, offer consumers an easy way to delete their data, and limit information collection on the front end. The Commission will continue to act aggressively to protect personal data."

The California-based company has sold educational products and services targeted to high school and college students, including online tutoring and a college scholarship search service. Chegg collects a variety of personal information about its users. For example, as part of its scholarship search service, Chegg has collected information about users' religious denominations, heritage,
dates of birth, sexual orientation, and disabilities. It also has collected and stored sensitive personal information about its employees, including dates of birth, Social Security numbers, and financial and medical data.

In a complaint, the FTC alleged that Chegg failed to protect the personal information it has collected from its users and employees. As a result, the company experienced four data breaches that exposed that personal information. The first occurred in September 2017, when multiple Chegg employees fell for a phishing attack that allowed a hacker to gain access to employees’ direct deposit information. Less than a year later, a former Chegg contractor used login information the company shared with employees and outside contractors to access one of Chegg’s third-party cloud databases containing personal information of approximately 40 million customers. The exposed personal information included names, email addresses, passwords, and for certain users, sensitive scholarship data such as dates of birth, parents’ income range, sexual orientation, and disabilities. In the next two years, Chegg experienced two more data breaches involving phishing attacks that successfully targeted Chegg employees. These attacks exposed sensitive data about Chegg’s employees including medical and financial information.

The FTC’s complaint alleges that these data breaches stemmed from Chegg’s poor data security practices, which included:

- **Failing to implement basic security measures**: The FTC alleged that despite its promises, Chegg failed to use “commercially reasonable security measures” to protect personal information it collected and stored. For example, at various times throughout the relevant time period, it did not require employees to use multifactor authentication measures to log into its third-party databases, allowed employees and contractors to use a single login to access those databases, and failed to monitor its network and databases for threats.

- **Storing information insecurely**: Chegg stored personal data on its cloud storage databases in plain text and used until at least 2018 outdated and weak encryption to protect user passwords.

- **Failing to Develop Adequate Security Policies and Training**: Even after experiencing three phishing attacks, the company failed to provide adequate security training to employees and contractors and implement a written security policy until January 2021.

As a result of these failures, some of the data about Chegg’s 40 million customers stolen by its...
former contractor was later found for sale online. Chegg’s failure to protect its employees’ medical and financial data was particularly problematic since this information is valuable on the open market and is used to commit identity theft and fraud, according to the complaint.

As part of the proposed order, Chegg will be required to take several steps to address the problems outlined in the FTC’s complaint including:

- **Detail and Limit Data Collection**: Chegg must document and follow a schedule that sets out what personal information the company collects, why it collects the information, and when it will delete the information.

- **Provide Consumer Access to Data**: Chegg must provide its customers access to data collected about them and allow them to request that the company delete that data.

- **Implement Multifactor Authentication**: Chegg must provide multifactor authentication or another authentication method to its customers and employees to help protect their accounts.

- **Implement Security Program**: Chegg must implement a comprehensive information security program that addresses the flaws in the company’s data security practices including encrypting consumer data and providing security training to its employees.

The action against Chegg is part of the FTC’s aggressive efforts to ensure education technology companies protect and secure personal data they collect and do not collect more information than is necessary. In May 2022, the Commission issued a policy statement warning education technologies against illegally collecting personal information from children under 13 in violation of the Children’s Online Privacy Protection Act, which also requires companies to secure the data they collect. The Commission also is taking steps to bolster security market-wide, including initiating an advance notice of proposed rulemaking on commercial surveillance and lax data security practices. And the FTC continues to hold companies accountable for failing to secure consumer data. Earlier this month, the FTC announced an order with the online alcohol delivery marketplace Drizly and its CEO for its lax data security practices.

The Commission voted 4-0 to issue the proposed administrative complaint and to accept the consent agreement with Chegg.

The FTC will publish a description of the consent agreement package in the Federal Register.
The agreement will be subject to public comment for 30 days after publication in the Federal Register after which the Commission will decide whether to make the proposed consent order final. Instructions for filing comments will appear in the published notice. Once processed, comments will be posted on Regulations.gov.

NOTE: The Commission issues an administrative complaint when it has “reason to believe” that the law has been or is being violated, and it appears to the Commission that a proceeding is in the public interest. When the Commission issues a consent order on a final basis, it carries the force of law with respect to future actions. Each violation of such an order may result in a civil penalty of up to $46,517.

The Federal Trade Commission works to promote competition and protect and educate consumers. Learn more about consumer topics at consumer.ftc.gov, or report fraud, scams, and bad business practices at ReportFraud.ftc.gov. Follow the FTC on social media, read consumer alerts and the business blog, and sign up to get the latest FTC news and alerts.

Contact Information

Media Contacts

Juliana Gruenwald Henderson
Office of Public Affairs
202-326-2924

Peter Kaplan
Office of Public Affairs
202-468-7684

Staff Contacts

Brian Shull
Bureau of Consumer Protection
202-326-3734

Miles Plant
Bureau of Consumer Protection
202-326-2526

Genevieve Bonan
Bureau of Consumer Protection
202-326-3139