

1 MICHAEL R. REESE (Cal. SBN 206773)  
2 *mreese@reesellp.com*

3 SUE J. NAM (Cal. SBN 206729)  
4 *snam@reesellp.com*

5 **REESE LLP**  
6 100 West 93<sup>rd</sup> Street, 16<sup>th</sup> Floor  
7 New York, New York 10025  
8 Telephone: (212) 643-0500

GEORGE V. GRANADE (Cal. SBN 316050)  
*ggranade@reesellp.com*

8484 Wilshire Boulevard, Suite 515

**REESE LLP**  
Los Angeles, California 90211  
Telephone: (310) 393-0070

9 CALEB MARKER (Cal. SBN 269721)  
10 *caleb.marker@zimmreed.com*

11 **ZIMMERMAN REED LLP**  
12 6420 Wilshire Blvd., Suite 1080  
13 Los Angeles, California 90048  
14 Telephone: (877) 500-8780

BRIAN C. GUDMUNDSON (to be admitted *pro hac vice*)  
*brian.gudmundson@zimmreed.com*

RACHEL K. TACK (to be admitted *pro hac vice*)  
*rachel.tack@zimmreed.com*

MICHAEL J. LAIRD (to be admitted *pro hac vice*)  
*michael.laird@zimmreed.com*

**ZIMMERMAN REED LLP**  
1100 IDS Center  
80 South 8th Street  
Minneapolis, Minnesota 55402  
Telephone: (612) 341-0400

*Attorneys For Plaintiff and the Proposed Class*

**UNITED STATES DISTRICT COURT**  
**NORTHERN DISTRICT OF CALIFORNIA**  
**SAN JOSE DIVISION**

17 \_\_\_\_\_ )  
18 JOSHUA KELLER, on behalf of himself and all )  
19 others similarly situated, )

Plaintiff, )

v. )

21 CHEGG, INC., )

Defendant. )  
22 )  
23 )  
24 )  
25 )  
26 )  
27 )  
28 )

CASE NO.: 22-cv-6986

**COMPLAINT**  
**CLASS ACTION**

**Jury Trial Demanded**

1 Plaintiff Joshua Keller (“Plaintiff”), by his undersigned counsel, files this Class Action  
2 Complaint on behalf of himself and a class of all similarly situated persons against Defendant Chegg,  
3 Inc. (“Chegg” or “Defendant”). Plaintiff bases the forgoing allegations upon personal information and  
4 belief, the investigation of counsel, and states the following:

5 **INTRODUCTION**

6 1. Chegg markets and sells direct-to-student educational products and services.<sup>1</sup> This  
7 includes renting textbooks, guiding customers in their search for scholarships, and offering online  
8 tutoring.<sup>2</sup> Chegg claims it “strive[s] to improve the overall return on investment in education by helping  
9 students learn more in less time and at a lower cost.”<sup>3</sup> The company also claims to bring “integrity to  
10 [its] products, customers, work environment, and the community.”<sup>4</sup> According to Chegg, the target  
11 audience for its services and products are primarily high school and college students.

12 2. Since approximately September 2107, Chegg experienced, at least, four data security  
13 breaches: (1) September 2017; (2) April 2018; (3) April 2019; and (4) April 2020 (collectively the “Data  
14 Breaches”).

15 3. The first data breach occurred in September 2017, when multiple Chegg employees fell  
16 for a phishing attack that allowed a hacker to gain access to employees’ direct deposit information.  
17 Upon information and belief, this breach was limited to the exposure of employee data.

18 4. Approximately seven months later, in April 2018, a former Chegg contractor used login  
19 information the company shared with employees and contractors to access one of Chegg’s third-party  
20 cloud databases, resulting in the exposure of millions of customers’ personal information. According to  
21 the Federal Trade Commission (“FTC”), Chegg allowed employees and third-party contractors to access  
22 Amazon-hosted storage with a single access key that provided full administrative privileges over all  
23

---

24 <sup>1</sup> *Multiple data breaches suggest ed tech company Chegg didn’t do its homework, alleges FTC*, Leslie  
25 Fair, Federal Trade Commission, Oct. 31, 2022: [https://www.ftc.gov/business-](https://www.ftc.gov/business-guidance/blog/2022/10/multiple-data-breaches-suggest-ed-tech-company-chegg-didnt-do-its-homework-alleges-ftc)  
26 [guidance/blog/2022/10/multiple-data-breaches-suggest-ed-tech-company-chegg-didnt-do-its-](https://www.ftc.gov/business-guidance/blog/2022/10/multiple-data-breaches-suggest-ed-tech-company-chegg-didnt-do-its-homework-alleges-ftc)  
27 [homework-alleges-ftc](https://www.ftc.gov/business-guidance/blog/2022/10/multiple-data-breaches-suggest-ed-tech-company-chegg-didnt-do-its-homework-alleges-ftc) (last visited Nov. 4, 2022).

28 <sup>2</sup> *Id.*

<sup>3</sup> *Id.*

<sup>4</sup> *Id.*

1 information.<sup>5</sup> The April 2018 data breach exposed the personal information of approximately forty (40)  
2 million customers. The exposed personal information included names, email addresses, passwords, and  
3 for certain users, sensitive scholarship information such as dates of birth, parents' income range, sexual  
4 orientation, and disabilities. Upon information and belief, this breach exposed both consumer and  
5 employee data.

6 5. In September 2018, a threat intelligence vendor informed Chegg that a file containing  
7 some of this exfiltrated information was available in an online forum.<sup>6</sup> Chegg reviewed the file as part  
8 of its own investigation, finding it held, among other things, approximately 25 million of the exfiltrated  
9 customers' passwords, from the April 2018 breach, in plain text, meaning the threat actors had cracked  
10 the hash for those passwords.<sup>7</sup> Chegg required approximately 40 million Chegg platform users to reset  
11 their passwords.<sup>8</sup> Even after this, Chegg continued to store consumer personal information in plain text.<sup>9</sup>

12 6. The third breach, in April 2019, was the result of another phishing attack, giving hackers  
13 access to a Chegg executive's email inbox, which contained personal information of Chegg users and  
14 employees, including financial and medical data.<sup>10</sup> Upon information and belief, this breach exposed  
15 both consumer and employee data.

16 7. And most recently, the fourth data breach in April 2020, exposed W-2 information,  
17 including birth dates and Social Security numbers for approximately 700 current and former employees.  
18 <sup>11</sup> Upon information and belief, this data breach was limited to the exposure of employee data.

19 8. From September 2017 through April 2020, Chegg did not make reasonable modifications  
20 to its data security, including an egregious failure to implement any phishing attack training for its  
21 employees. It also did not implement a written data security policy until January 2021.

22 \_\_\_\_\_  
23 <sup>5</sup> *FTC schools edtech giant Chegg over 'careless' cybersecurity practices*, Carly Page, Join  
24 TechCrunch+, Nov. 1, 2022: <https://techcrunch.com/2022/11/01/ftc-chegg-breaches-cybersecurity/>,  
(last visited Nov. 7, 2022).

25 <sup>6</sup> *In the Matter of CHEGG, INC., a corporation*, (last visited, Nov. 7, 2022),  
[https://www.ftc.gov/system/files/ftc\\_gov/pdf/2023151-Chegg-Complaint.pdf](https://www.ftc.gov/system/files/ftc_gov/pdf/2023151-Chegg-Complaint.pdf).

26 <sup>7</sup> *Id.*

27 <sup>8</sup> *Id.*

28 <sup>9</sup> *Id.*

<sup>10</sup> *Id.*

<sup>11</sup> *Id.*



**PARTIES**

1  
2 15. **Plaintiff** Joshua Keller is a resident of Hillsborough, California. He used Chegg’s  
3 services throughout his high school and college education, including for exam, homework, and project  
4 help. Plaintiff has been a Chegg customer for approximately the last six years. Plaintiff reasonably  
5 believes his data was compromised by the Chegg Data Breaches. After these data breaches and  
6 specifically over the last two months, Plaintiff experienced identity theft and fraud, including multiple  
7 credit checks initiated on his behalf and a credit card issued in his name, both without his authorization  
8 or consent. Plaintiff has spent time and effort with his bank dealing with this credit card fraud. He also  
9 noticed an increase in spam calls and emails and spent time and effort changing multiple passwords to  
10 his various subscriptions or accounts. Plaintiff reasonably believes that all of this, the identity theft and  
11 fraud and the increase in spam, is a direct and proximate result of the Chegg Data Breaches, particularly  
12 because this fraud all occurred after the Data Breach and Plaintiff does not reasonably believe it could  
13 be related to any other event.

14 16. **Defendant** Chegg is a Delaware limited liability company with its headquarters and  
15 principal place of businesses in Santa Clara, California.

**BACKGROUND**

16  
17 **A. Chegg Collects Sensitive Information from Users**

18 17. In providing its services and for employment, Chegg collects sensitive personal  
19 information from customers. This information includes name, email address, username, password,  
20 demographic, school, gender, age or birthdate, zip or postal code, photographs, information about  
21 academic and work history, phone number, mailing address, and information about interests and  
22 preferences.<sup>15</sup>

23 18. If a user requests information about Chegg’s scholarship services, the user is directed to  
24 update their profile. The additional information Chegg collects here includes a customer’s religious  
25 denomination, heritage, date of birth, parents’ income range, sexual orientation, military affiliations,  
26

27  
28 <sup>15</sup> *Privacy Policy*, (last visited, Nov. 7, 2022), <https://www.chegg.com/en-US/privacypolicy>.

1 citizenships, disabilities, interests, and participation in clubs and sports (collectively, the “Scholarship  
2 Search Data”).<sup>16</sup> This data is highly sensitive.

3 19. As another example, in connection with its online tutoring services, Chegg records videos  
4 of tutoring sessions that include Chegg users’ likeness, images, and voices. Again, this is highly  
5 sensitive information.

6 20. Chegg also collects information automatically when users use the services, including  
7 internet protocol (IP) address, user setting, MAC address, cookie identifies, mobile carrier mobile  
8 advertising and other unique identifies, details about users’ browser, operating system or device, location  
9 information, Internet or mobile service provider, pages that users visit before, during, and after using  
10 the services, information about links users click, and other information about how users use Chegg’s  
11 services.<sup>17</sup>

12 21. Taken together, these paragraphs, collectively and independently identify “Sensitive  
13 Information.”

14 **B. Chegg’s Inadequate Data Security Measures Exposed Customers’ Sensitive Information**

15 22. As part of its information technology infrastructure, Chegg uses a third-party service  
16 provided by Amazon Web Services called the Simple Storage Service (“S3”). S3 is a scalable cloud  
17 storage service that can be used to store and retrieve large amounts of data. The S3 stores data inside  
18 virtual containers, called “buckets,” against which individual access controls can be applied.<sup>18</sup>

19 23. Chegg relies on S3 buckets to store a wide variety of files that contain customers’  
20 sensitive personal information, including their names, passwords, dates of birth, and Scholarship Search  
21 Data.<sup>19</sup>

22 24. From at least 2017 to the 2020, Chegg has engaged in several practices that failed to  
23 provide reasonable security to prevent unauthorized access to customers’ personal information. Among  
24 other things, Chegg:

25  
26 <sup>16</sup> *Profile Info*, (last visited, Nov. 7, 2022), <https://www.chegg.com/my/profile>.

27 <sup>17</sup> *Privacy Policy*, *supra* note 7.

28 <sup>18</sup> *In the Matter of CHEGG, INC., a corporation*, *supra* note 6.

<sup>19</sup> *Id.*

- 1 a) failed to implement reasonable access controls to safeguard users' personal information  
2 stored in S3 databases until at least October 2018. Specifically, Chegg:
- 3 i) failed to require employees and third-party contractors that access the S3 databases to  
4 use distinct access keys, instead permitting employees and contractors to use a single  
5 AWS access key that provided full administrative privileges over all data in the S3  
6 databases ("AWS Root Credentials");
- 7 ii) failed to restrict access to systems based on employees' or contractors' job functions;
- 8 iii) failed to require multi-factor authentication for account access to the S3 databases; and
- 9 iv) failed to rotate access keys to the S3 databases;
- 10 b) stored users' and employees' personal information on Chegg's network and databases,  
11 including S3 databases, in plain text, rather than encrypting the information;
- 12 c) used outdated and unsecure cryptographic hash functions to protect users' passwords;
- 13 d) failed to provide adequate guidance or training for employees or third-party contractors  
14 regarding information security and safeguarding users' and employees' personal  
15 information, including, but not limited to, failing to require employees to complete any data  
16 security training;
- 17 e) failed to develop, implement, or maintain adequate written organizational information  
18 security standards, policies, procedures, or practices;
- 19 f) failed to have a policy, process, or procedure for inventorying and deleting users' and  
20 employees' personal information stored on Chegg's network after that information is no  
21 longer necessary; and
- 22 g) failed to adequately monitor its networks and systems for unauthorized attempts to transfer  
23 or exfiltrate users' and employees' personal information outside of Chegg's network  
24 boundaries.<sup>20</sup>

18 **C. Chegg's Inadequate Data Security Caused Multiple Data Breaches**

19 25. Chegg's failure to provide reasonable data security for the Sensitive Information it  
20 collected from customers has led to the repeated exposure of that personal information.

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

25 27. Seven months later, in April 2018, a former contractor accessed one of Chegg's S3  
26 databases using an AWS Root Credential. Although Amazon had provided public guidance to protect

27 \_\_\_\_\_  
28 <sup>20</sup> *In the Matter of CHEGG, INC., a corporation, supra* note 6.

1 AWS Root Credentials “like you would your credit card numbers or any other sensitive secret” and that  
2 Amazon “strongly recommend[s] that you do not use the root user for your everyday tasks, even the  
3 administrative ones,” Chegg shared the AWS Root Credentials among its employees and even outside  
4 contractors.<sup>21</sup> The former contractor exfiltrated a database containing personal information of  
5 approximately 40 million Chegg customers.

6 28. The exposed personal information included users’ email addresses, first and last names,  
7 passwords, religious denomination, heritage, date of birth, parents’ income range, sexual orientation,  
8 and disabilities. Chegg encrypted users’ passwords using an outdated function that had been criticized  
9 by experts for years prior to April 2018.<sup>22</sup> Had Chegg employed reasonable access controls and  
10 monitoring, it would have likely detected and/or stopped the attack more quickly.

11 29. In approximately April 2019, a senior Chegg executive fell for a phishing attack, giving  
12 a hacker access to the executive’s credentials to Chegg’s email platform and exposing personal  
13 information about consumers and employees of Chegg. This executive’s email system was in a default  
14 configuration state that allowed employees, as well as threat actors, to bypass Chegg’s multifactor  
15 authentication requirement while accessing the email platform. The threat actor exploited this shortfall  
16 and gained access to the executive’s email inbox, which contained the personal information of Chegg  
17 users and employees, including their financial and medical information.<sup>23</sup>

18 30. Had Chegg properly configured its systems, including requiring multifactor  
19 authentication for employees to access their emails, this phishing attack, and the resulting exposure of  
20 consumer Sensitive Information, could have been prevented.

21 31. In addition, Chegg’s failure to require employees to complete any data security training,  
22 including training to identify and respond to phishing attacks, contributed to the security incident.

23 32. Most recently, in April 2020, Chegg’s senior employee responsible for payroll fell for a  
24 phishing attack, giving the threat actor access to the employee’s credentials to Chegg’s payroll system.  
25 The threat actor exfiltrated the W-2 information, including the birthdates and Social Security numbers,

26 \_\_\_\_\_  
27 <sup>21</sup> *In the Matter of CHEGG, INC., a corporation, supra* note 6.

28 <sup>22</sup> *Id.*

<sup>23</sup> *Id.*



1 of approximately 700 current and former employees. Despite Chegg employees falling for phishing  
2 attacks on at least two prior occasions, Chegg still did not require, in or before April 2020, its employees  
3 to complete any data security training, including identifying and appropriately responding to phishing  
4 attacks.<sup>24</sup>

5 **D. Chegg Knew It Needed to Protect Customers’ Sensitive Information**

6 33. Chegg knew the user data it collected and stored in connection with its services was  
7 highly sensitive.

8 34. From approximately March 2017 to January 2020, Chegg’s privacy policy included the  
9 following language: “Chegg takes commercially reasonable security measures to protect the Personal  
10 Information submitted to us, both during transmission and once we receive it.”<sup>25</sup> From January 2020 to  
11 the present, Chegg’s privacy policy contained the following statement concerning that same personal  
12 information: “We take steps to ensure that your information is treated securely and in accordance with  
13 this Privacy Policy.”<sup>26</sup> These statements indicate that Chegg was aware the sensitive and personal nature  
14 of the user data it stored.

15 35. Additionally, in a February 7, 2022 Press Release, Chegg included some “Forward  
16 Looking Statements.” Within those statements, Chegg mentioned service disruptions related to  
17 cybersecurity and cyber-attacks twice throughout the statement, indicating that it was aware the potential  
18 for such threats.<sup>27</sup>

19 **E. Plaintiff’s and the Class’s Sensitive Information Has Value.**

20 36. The personal, health, and financial information of Plaintiff and the Class is valuable,  
21 intangible property. Indeed, it has market value to advertisers and cybercriminals seeking to obtain and  
22 use that information and the public and the marketplace values maintaining the privacy and  
23

24  
25 <sup>24</sup> *In the Matter of CHEGG, INC., a corporation, supra* note 6.

26 <sup>25</sup> *Id.*

27 <sup>26</sup> *Id.*

28 <sup>27</sup> *Chegg Investor Relations*, (last visited Nov. 7, 2022), <https://investor.chegg.com/Press-Releases/press-release-details/2022/Chegg-Reports-2021-Financial-Results-and-Gives-2022-Guidance/default.aspx>.

1 confidentiality of individuals' Sensitive Information. Thus, Chegg was on notice of the need to  
2 implement reasonable data security measures.

3 37. Unlike financial information, like credit card and bank account numbers, the PHI and  
4 certain PII exfiltrated in the Data Breach cannot be easily changed. Dates of birth and social security  
5 numbers are given at birth and attach to a person for the duration of his or her life. For these reasons,  
6 these types of information are the most lucrative and valuable to hackers.<sup>28</sup>

7 38. Birth dates, Social Security numbers, addresses, employment information, income, and  
8 similar types of information can be used to open several credit accounts on an ongoing basis rather than  
9 exploiting just one account until it's canceled.<sup>29</sup>

10 39. In 2013, the Organization for Economic Cooperation and Development ("OECD") even  
11 published a paper entitled "Exploring the Economics of Personal Data: A Survey of Methodologies for  
12 Measuring Monetary Value."<sup>30</sup> In this paper, the OECD measured prices demanded by companies  
13 concerning user data derived from "various online data warehouses."<sup>31</sup>

14 40. OECD indicated that "[a]t the time of writing, the following elements of personal data  
15 were available for various prices: USD 0.50 cents for an address, USD 2 [i.e., \$2] for a date of birth,  
16 USD 8 for a social security number (government ID number), USD 3 for a driver's license number and  
17 USD 35 for a military record. A combination of address, date of birth, social security number, credit  
18 record and military is estimated to cost USD 55."<sup>32</sup>

19 41. Consumers and businesses also place a considerable value on maintaining the privacy  
20 and confidentiality of their Sensitive Information. One 2002 study determined that U.S. consumers  
21 highly value a website's protection against improper access to their Sensitive Information, between  
22

23 <sup>28</sup> *Calculating the Value of a Data Breach – What Are the Most Valuable Files to a Hacker?* Donnellon  
24 McCarthy Enters, (last visited Nov. 7, 2022), <https://www.dme.us.com/2020/07/21/calculating-the-value-of-a-data-breach-what-are-the-most-valuable-files-to-a-hacker/>.

25 <sup>29</sup> *Anthem hack: Personal data stolen sells for 10x Price of Stolen Credit Card Numbers*, Tim  
26 Greene, <https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolensells-for-10x-price-of-stolen-credit-card-numbers.html> (last visited Jan. 18, 2022).

27 <sup>30</sup> *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary  
28 Value*, OECD Digital Economy Papers, NO. 220 (Apr. 2, 2013),  
<https://www.oecdilibrary.org/docserver/5k486qtxldmq-en.pdf>.

<sup>31</sup> *Id.* at 25.

<sup>32</sup> *Id.*

1 \$11.33 and \$16.58 per website.<sup>33</sup> The study further concluded that to U.S. consumers, the collective  
2 “protection against error, improper access, and secondary use of personal information is worth between  
3 \$30.49 and \$44.62.<sup>34</sup> This data is approximately twenty years old, and the dollar amounts would likely  
4 be exponentially higher today.

5 42. The FTC has also recognized that consumer data is a lucrative (and valuable) form of  
6 currency for businesses. In an FTC roundtable presentation, former Commissioner Pamela Jones  
7 Harbour underscored this point by reiterating that “most consumers cannot begin to comprehend the  
8 types and amount of information collected by businesses, or why their information may be commercially  
9 valuable.<sup>35</sup> Data is currency.<sup>36</sup>

10 43. When a data breach reveals Sensitive Information, it destroys the privacy and  
11 confidentiality of that data. Not only does that upset consumer expectations and wishes, but it also  
12 renders the data less valuable in the economy. Sensitive and personal “data has economic value” and  
13 can be used to further “artificial intelligence tools as well as the creation of intelligence targeting  
14 packages.” Indeed, the integrity of Sensitive Information is material to individual’s ability to prove their  
15 identity, which is necessary for individuals to obtain mortgages, credit cards, business loans; to submit  
16 tax returns; and to apply for a job.

17 44. Consumers, likewise, exchange this type of information to businesses in exchange  
18 for goods, services, access, or discounts.

19 45. When this information is released to cybercriminals and placed on the dark web, then  
20 individuals are less able to use that information to prove their identity because that information has been  
21 exposed to others willing or able to falsify and steal others’ identities. Thus, the value of the breached  
22 information is lessened and its usefulness impaired.

23  
24  
25 <sup>33</sup> 11-Horn Hann, Kai-Lung Hui, *et al*, *The Value of Online Information Privacy: Evidence from*  
*the USA and Singapore*, at 17. Marshall Sch. Bus., Univ. So. Cal. (Oct. 2002),  
<https://www.comp.nus.edu.sg/~ipng/research/privacy.pdf> (last visited Nov. 6, 2022).

26 <sup>34</sup> *Id.*

27 <sup>35</sup> Statement of FTC Commissioner Pamela Jones Harbour—Remarks Before FTC Exploring  
Privacy Roundtable, (Dec. 7, 2009) (last visited Nov. 7, 2022)  
<https://www.ftc.gov/news-events/news/speeches/remarks-ftc-exploring-privacy-roundtable>.

28 <sup>36</sup> *Id.*

1 46. Chegg's failure to provide reasonable data security for its users' Sensitive Information  
2 has caused and is likely to continue to cause substantial injury, including but not limited to identity theft,  
3 fraud, out-of-pocket monetary losses, decreased value of personal information, and time and effort spent  
4 remedying or attempting to prevent injuries, to those individuals whose data was exposed in breaches.

5 **CLASS ALLEGATIONS**

6 47. Plaintiff brings this action on behalf of himself and all other similarly situated Class  
7 members pursuant to Rule 23(a), (b)(2) and (b)(3) of the Federal Rules of Civil Procedure and seek  
8 certification of the following Nationwide Class:

9 All individuals whose data was impacted or otherwise compromised by one of, or any  
10 combination of the four, Chegg's Data Breaches.

11 48. Excluded from the class is Chegg and its subsidiaries and affiliates; all persons who make  
12 a timely election to be excluded from the class; government entities; and the judge to whom this case is  
13 assigned and his/her immediate family and court staff.

14 49. Plaintiff reserves the right to, after conducting discovery, modify, expand or amend the  
15 above Class definition or to seek certification of a class or Classes defined differently than above before  
16 any court determines whether certification is appropriate.

17 50. **Numerosity.** Consistent with Rule 23(a)(1), the members of the Class are so numerous  
18 and geographically dispersed that joinder of all Class members is impracticable. Plaintiff believes that  
19 there are millions of members of the Class. The number of reportedly impacted individuals already  
20 exceeds forty (40) million, and Plaintiff believes additional entities and persons may have been affected  
21 by the Data Breaches. The precise number of class members, however, is unknown to Plaintiff. Class  
22 members may be identified through objective means. Class members may be notified of the pendency  
23 of this action by recognized, Court-approved notice dissemination methods, which may include U.S.  
24 mail, electronic mail, internet postings, and/or published notice.

25 51. **Commonality and Predominance.** Consistent with Fed. R. Civ. P. 23(a)(2) and with  
26 23(b)(3)'s commonality and predominance requirements, this action involves common questions of law  
27  
28

1 and fact which predominate over any questions affecting individual Class members. These common  
2 questions include, without limitation:

- 3 a. Whether Chegg knew or should have known that its data environment and cybersecurity  
measures created a risk of a data breach;
- 4 b. Whether Chegg controlled and took responsibility for protecting Plaintiff's and the Class's  
5 data when solicited that data, collected it, and stored it on its servers;
- 6 c. Whether Chegg's security measures were reasonable considering the FTC data security  
7 recommendations, state laws and guidelines, industry standards, and common  
recommendations made by data security experts;
- 8 d. Whether Chegg owed Plaintiff and the Class a duty to implement reasonable security  
measures;
- 9 e. Whether Chegg's failure to adequately secure Plaintiff's and the Class's data constitutes a  
10 breach of its duty to institute reasonable security measures;
- 11 f. Whether Chegg's failure to implement reasonable data security measures allowed the breach  
of its data systems to occur and caused the theft of Plaintiff's and the Class's data;
- 12 g. Whether reasonable security measures known and recommended by the data security  
13 community could have prevented the breach;
- 14 h. Whether Plaintiff and the Class were injured and suffered damages or other losses because  
of Chegg's failure to reasonably protect its data systems; and
- 15 i. Whether Plaintiff and the Class are entitled to relief.

16 52. **Typicality.** Consistent with Fed. R. Civ. P. 23(a)(3), Plaintiff is a typical member of the  
17 Class. Plaintiff and the members of the Class are persons whose provided data to Chegg, whose data  
18 resided on Chegg's servers, and whose personally identifying information was exposed in Chegg's Data  
19 Breaches. Plaintiff's injuries are like other class members and Plaintiff seeks relief consistent with the  
20 relief due to the Class.

21 53. **Adequacy.** Consistent with Fed. R. Civ. P. 23(a)(4), Plaintiff is an adequate  
22 representative of the Class because Plaintiff is a member of the Class and is committed to pursuing this  
23 matter against Chegg to obtain relief for himself and for the Class. Plaintiff has no conflicts of interest  
24 with the Class. Plaintiff has also retained counsel competent and experienced in complex class action  
25 litigation of this type, having previously litigated data breach cases. Plaintiff intends to vigorously  
26 prosecute this case and will fairly and adequately protect the Class's interests.



1 consequences of the breach would largely fall on individual persons whose data was impacted and  
2 stolen. Therefore, the Data Breach, and the harm it caused Plaintiff and the Class, was the foreseeable  
3 consequence of Chegg’s unsecured, unreasonable data security measures.

4 59. Additionally, Section 5 of the Federal Trade Commission Act (“FTCA”), 15 U.S.C. § 45,  
5 required Chegg to take reasonable measures to protect Plaintiff’s and the Class’s sensitive data and is a  
6 further source of Chegg’s duty to Plaintiff and the Class. Section 5 prohibits unfair practices in or  
7 affecting commerce, including, as interpreted and enforced by the FTC, the unfair act or practice by  
8 businesses like Chegg of failing to use reasonable measures to protect sensitive data. Chegg, therefore,  
9 was required and obligated to take reasonable measures to protect data it possessed, held, or otherwise  
10 used. The FTC publications and data security breach orders described herein further form the basis of  
11 Chegg’s duty to adequately protect sensitive information. By failing to implement reasonable data  
12 security measures, Chegg acted in violation of § 5 of the FTCA.

13 60. Chegg is obligated to perform its business operations in accordance with industry  
14 standards. Industry standards are another source of duty and obligations requiring Chegg to exercise  
15 reasonable care with respect to Plaintiff and the Class by implementing reasonable data security  
16 measures that do not create a foreseeable risk of harm to Plaintiff and the Class.

17 61. Finally, Chegg assumed the duty to protect users’ sensitive data by soliciting, collecting,  
18 and storing users’ data and, additionally, by representing to consumers that it “takes commercially  
19 reasonable security measures to protect the Personal Information submitted to [it].”

20 62. Chegg breached its duty to Plaintiff and the Class by implementing unreasonable data  
21 security measures that it knew or should have known could cause a Data Breach. Chegg knew or should  
22 have known that hackers might target sensitive data that Chegg solicited and collected on its users and,  
23 therefore, needed to use reasonable data security measures to protect against a Data Breach. Indeed,  
24 Chegg acknowledged it was subject to certain standards to protect data and utilize other industry  
25 standard data security measures. Chegg, furthermore, represented to users that their data was safe with  
26 Chegg.





1 69. Chegg’s violation of Section 5 of the FTC Act constitutes negligence per se.

2 70. Plaintiff and the Class are within the class of persons Section 5 of the FTCA (and similar  
3 state statutes) was intended to protect. Additionally, the harm that has occurred is the type of harm the  
4 FTC Act (and similar state statutes) was intended to guard against. The FTC has pursued over fifty  
5 enforcement actions against businesses which, because of their failure to employ reasonable data  
6 security measures and avoid unfair and deceptive practices, caused the same type of harm suffered by  
7 Plaintiff and the Class.

8 71. As a direct and proximate result of Chegg’s negligence per se, Plaintiff and the Class  
9 have suffered and continue to suffer injury.

10 **COUNT III**

11 **Violation of the California Legal Remedies Act, Cal. Civ. Code §§ 1750, et seq.**  
12 **(Injunctive Relief Only)**

13 72. Plaintiff repeats and re-alleges the foregoing allegations as if fully set forth herein.

14 73. The Consumers Legal Remedies Act (“CLRA”) is liberally construed to protect  
15 consumers against unfair and deceptive business practices in connection with the conduct of businesses  
16 providing goods, property or services to consumers primarily for personal, family, or household use.

17 74. Chegg is a “person” as defined by the CLRA, and it provided “services” as defined under  
18 the act. Cal. Civ. Code §§ 1761(b)-(c), 1770.

19 75. The CLRA prohibits a defendant who is involved in a transaction from “[r]epresenting  
20 that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or  
21 quantities which they do not have.” *Id.* at § 1770(a)(5).

22 76. Additionally, the CLRA prohibits a defendant who is involved in a transaction from  
23 “[r]epresenting that goods or services are of a particular standard, quality, or grade . . . if they are of  
24 another.” *Id.* at § 1770(a)(7).

25 77. Plaintiff Keller and the Class members are “consumer[s]” as who were engaged in a  
26 “transaction” under the act. *Id.* at §§ 1761(d)-(e), 1770.

1 78. Chegg's acts and practices were intended to and did result in the sales of services to  
2 Plaintiff and the Class members in violation of Civil Code § 1770, including, but not limited to, the  
3 following:

- 4 a. Implementing and maintaining cybersecurity and privacy measures that were knowingly  
5 insufficient to protect Plaintiff Keller's and the Classes' sensitive data, which was a direct  
6 and proximate cause of the Data Breaches;
- 7 b. Failing to identify foreseeable security and privacy risks, remediate identified security and  
8 privacy risks, and adequately improve security and privacy measures despite knowing the  
9 risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breaches;
- 10 c. Failing to comply with common law and statutory duties pertaining to the security and  
11 privacy of Plaintiff Keller's and Class members' sensitive data, including duties imposed by  
12 the Federal Trade Commission Act, 15 U.S.C. § 45, which was a direct and proximate cause  
13 of the Data Breaches;
- 14 d. Omitting, suppressing, and concealing the material fact that they did not reasonably or  
15 adequately secure Plaintiff Keller's and Class members' sensitive data; and
- 16 e. Omitting, suppressing, and concealing the material fact that they did not comply with  
17 common law and statutory duties pertaining to the security and privacy of Plaintiff Keller's  
18 and Class members' sensitive data, including duties imposed by the Federal Trade  
19 Commission Act, 15 U.S.C. § 45.

20 79. Chegg's omissions were material because they were likely to and did deceive reasonable  
21 consumers about the adequacy of Chegg's data security and ability to protect the confidentiality of  
22 consumers' sensitive information that Chegg solicited, collected, and stored.

23 80. Had Chegg disclosed, rather than concealing, to Plaintiff and class members that their  
24 cybersecurity, digital platforms, and data storage systems were not secure and, thus, vulnerable to attack,  
25 Chegg would have been unable to continue in business and would have been forced to adopt reasonable  
26 data security measures and comply with the law.

27 81. Instead, Chegg received, maintained, and compiled Plaintiff's and class members'  
28 sensitive data as part of the services Chegg provided and for which Plaintiff and class members paid, in  
part, through transaction fees by (1) omitting and concealing information from Plaintiff Keller and Class  
members that Chegg's data security practices were knowingly insufficient to maintain the safety and  
confidentiality of Plaintiff's and class members' sensitive data and (2) that Chegg was not compliant  
with basic data security requirements and best practices to prevent a Data Breach. Accordingly, Plaintiff

1 Keller and the Class members acted reasonably in relying on Chegg’s omissions, the truth of which they  
2 could not have discovered.

3 82. On November 8, 2022, Plaintiff Keller and the Class sent notice to Chegg in compliance  
4 with California Civil Code § 1782(a) via certified mail. Plaintiff and the other members of the Class  
5 seek only injunctive relief in this complaint, but will amend this complaint to seek damages if Defendant  
6 does not comply with the California Civil Code § 1782(a) notice.

7 **COUNT IV**

8 **Violation of the California Civil Code § 1798.150**  
9 **(Actual Damages and Injunctive Relief Only)**

10 83. Plaintiff repeats and re-alleges the foregoing allegations as if fully set forth herein.

11 84. Chegg is a corporation organized or operated for the profit or financial benefit of its  
12 owners with annual net revenues over \$776.3 million in 2021 and between \$830 and \$850 million in  
13 2022.<sup>39</sup>

14 85. Chegg collects and stores consumers personal information, including sensitive and  
15 personal information, as defined by Cal. Civ. Code § 1798.81.5.

16 86. Chegg had a duty to implement and maintain reasonable security procedures and  
17 practices to protect Plaintiff Keller’s and members of the Class’s sensitive and personal data.

18 87. Chegg failed to meet its duty, resulting in unauthorized access and exfiltration, theft, or  
19 disclose of Plaintiff Keller’s, and the Class’s, personal and sensitive data in violation of § 1798.150.

20 88. Plaintiff Keller and members of the Class seek relief pursuant to § 1798.150(a), including  
21 *inter alia*, actual damages, injunctive relief, and any other relief this Court deems proper. Plaintiff Keller  
22 and the Class also seek attorneys’ fees and costs pursuant to Cal. Code Civ. Proc. § 1021.5. Plaintiff  
23 does not seek statutory damages in this complaint.

24 89. On November 8, 2022, Plaintiff Keller and the Class sent notice to Chegg in compliance  
25 with California Civil Code § 1798.150(b) via certified mail. Plaintiff and the other members of the Class  
26 seek only actual damages and injunctive relief in this complaint, but will amend this complaint to seek  
27 statutory damages if Defendant does not comply with the California Civil Code § 1798.150(b) notice.

28 <sup>39</sup> *Chegg Investor Relations, supra* note 26.

1 90. Because Chegg is still in possession of Plaintiff Keller’s, and the other members of the  
2 Class’s, sensitive and personal data, Plaintiff Keller seek injunctive or other equitable relief to ensure  
3 that Chegg implements and maintains reasonable data security measures and practices to prevent an  
4 event like the Data Breach from occurring again.

5 **COUNT V**

6 **Declaratory and Injunctive Relief**

7 91. Plaintiff repeats and re-alleges the foregoing allegations as if fully set forth herein.

8 92. Under the Declaratory Judgment Act, 28 U.S.C. §§2201, *et seq.*, this Court is authorized  
9 to enter a judgment declaring the rights and legal relations of the parties and grant further necessary  
10 relief. Furthermore, the Court has broad authority to restrain acts, such as those alleged herein, which  
11 are tortious, and which violate the terms of the federal and state statutes described above.

12 93. An actual controversy has arisen in the wake of the Data Breaches at issue regarding  
13 Defendant’s common law and other duties to act reasonably with respect to safeguarding the data of  
14 Plaintiff and the Class. Plaintiff alleges Chegg’s actions in this respect were inadequate and  
15 unreasonable and, upon information and belief, remain inadequate and unreasonable. Additionally,  
16 Plaintiff and the Class continue to suffer injury due to the continued and ongoing threat of additional  
17 fraud against them or on their accounts.

18 94. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a  
19 judgment declaring, among other things, the following:

- 20 a. Chegg owed, and continues to owe a legal duty to secure the sensitive information with  
21 which it is entrusted, specifically including information it obtains from its customers, and  
22 to notify impacted individuals of the Data Breach under the common law, Section 5 of  
23 the FTC Act;
- 24 b. Chegg breached, and continues to breach, its legal duty by failing to employ reasonable  
25 measures to secure its customers’ personal information; and
- 26 c. Chegg’s breach of its legal duty continues to cause harm to Plaintiff and the Class.

27 95. The Court should also issue corresponding injunctive relief requiring Chegg to employ  
28 adequate security protocols consistent with industry standards to protect its users’ and employees’ (*i.e.*,  
Plaintiff’s and the Class’s) data.



**JURY TRIAL DEMANDED**

Plaintiff hereby demands a jury trial for all the claims so triable.

**REESE LLP**

Dated: November 8, 2022

/s/ Michael R. Reese

Michael R. Reese

*mreese@reesellp.com*

Sue J. Nam

*snam@reesellp.com*

100 West 93rd Street, 16th Floor

New York, New York 10025

Telephone: (212) 643-0500

**REESE LLP**

George V. Granade (Cal. State Bar No. 316050)

*ggranade@reesellp.com*

8484 Wilshire Boulevard, Suite 515

Los Angeles, California 90211

Telephone: (310) 393-0070

**ZIMMERMAN REED LLP**

Caleb Marker

*caleb.marker@zimmreed.com*

6420 Wilshire Blvd., Suite 1080

Los Angeles, California 90048

Telephone: (877) 500-8780

**ZIMMERMAN REED LLP**

Brian C. Gudmundson

*bgudmundson@zimmreed.com*

Rachel K. Tack

*rachel.tack@zimmreed.com*

Michael J. Laird

*michael.laird@zimmreed.com*

1100 IDS Center

80 South 8th Street

Minneapolis, Minnesota 55402

Telephone: (612) 341-0400

*Counsel for Plaintiff and the Class*

# ClassAction.org

This complaint is part of ClassAction.org's searchable class action lawsuit database and can be found in this post: [Chegg Hit with Class Action Over 'At Least' Four Undisclosed Data Breaches from 2017-2020](#)

---