

1 Robert S. Green (State Bar No. 136183)
 2 James Robert Noblin (State Bar No. 114442)
 3 Emrah M. Sumer (State Bar No. 329181)
 4 **GREEN & NOBLIN, P.C.**
 5 2200 Larkspur Landing Circle, Suite 101
 6 Larkspur, California 94939
 7 Telephone: (415) 477-6700
 8 Facsimile: (415) 477-6710
 9 Email: gnecf@classcounsel.com

7 Counsel for Plaintiff and the Proposed Class,
 8 ANASTASIYA KISIL, mother and natural guardian
 9 of "JOHN DOE," an infant, individually and on behalf
 10 of others similarly situated

11 **UNITED STATES DISTRICT COURT**
 12 **CENTRAL DISTRICT OF CALIFORNIA**

13 -----
 14 ANASTASIYA KISIL, mother and
 15 natural guardian of "JOHN DOE," an
 16 infant, individually and on behalf of
 17 others similarly situated,

Civil Action No.:

**CLASS ACTION
 COMPLAINT**

18 Plaintiff,

19 -against-

21 ILLUMINATE EDUCATION, INC.
 22 d/b/a PUPIL PATH,

23 Defendant.
 24 -----

1 Plaintiff ANASTASIYA KISIL, mother and natural guardian of “JOHN DOE,”
2 an infant (“Plaintiff”), individually and on behalf of all others similarly situated (the
3 “Class” or “Class members”), brings this Class Action Complaint against Illuminate
4 Education, Inc. d/b/a Pupil Path (“Illuminate” or “Defendant”), based on her
5 individual experiences and personal information, and investigation by her counsel.

6 **INTRODUCTION**

7 1. Plaintiff, individually and on behalf of all others similarly situated, brings
8 this class action suit against Defendant because of Defendant’s failure to safeguard the
9 confidential information of over two million current and former elementary and high
10 school students in school districts in New York City and elsewhere in the State of
11 New York, and in the States of California, Connecticut, and Oklahoma. The full
12 extent of the confidential information stolen is still uncertain but is currently known to
13 include highly sensitive personal and medical identifying information such as names,
14 addresses, demographic information, grades, academic and behavioral records, test
15 results, enrollment date, disability accommodation information, free or reduced-priced
16 lunch status, language preference, attendance records, physical performance records,
17 biometrics, and medical data. (the “Data Breach”).

18 2. Illuminate maintains a nationwide internet platform that stores and
19 assesses data concerning students in grades K-12 on a contract basis to school districts
20 nationwide, with access provided to educators, students and parents as an aid to
21 educational evaluation, monitoring of progress, and determining an educational plan
22 (as well as information concerning educators), headquartered in Irvine, California. It
23 also provides educational software applications and technology support to the school
24 districts. With data stored regarding at least seventeen million students nationwide,
25 Illuminate collects a significant amount of sensitive data from current and former
26 students, as delineated above.

27 3. On or about January 8, 2022, Illuminate became aware of “suspicious
28 access” to its systems that had occurred between on or about December 28, 2021, and

1 January 8, 2022, where unauthorized parties obtained the personally identifiable
2 information (“PII”) and protected health information (“PHI”) of current and former
3 students in school districts throughout the country (collectively, “Private
4 Information”). However, it was not until or about March 25, 2022, and in some cases
5 later than that, Illuminate began to notify school districts of the Data Breach, first
6 doing so by notifying the New York City Department of Education. As yet, Illuminate
7 has still failed to directly notify students and their parents of the Data Breach.

8 4. The Private Information that was compromised in the Data Breach can be
9 used to gain unlawful access to other online accounts of the students and their parents,
10 carry out identity theft, or commit other fraud and can be disseminated on the internet,
11 available to those who broker and traffic in stolen Private Information.

12 5. The illegal access to Private Information of minors is particularly
13 nefarious, as awareness of such access is typically delayed for a much longer period of
14 time in the case of children as opposed to adults, giving perpetrators more time to use
15 the Private Information for illegal purposes before detection.

16 6. While the sophistication of the methods employed in effectuating the
17 Data Breach is not publicly known, it is certain that the Data Breach could have been
18 avoided through basic security measures, encrypting, authentications, and training.

19 7. At all relevant times, Defendant promised and agreed in various
20 documents to safeguard and protect Private Information in accordance with federal,
21 state, and local laws, and industry standards, including the California Consumer
22 Privacy Act. Defendant made these promises and agreements on their websites and
23 other written notices and extended this commitment to situations in which third parties
24 handled Private Information on their behalf.

25 8. Contrary to these promises, and despite the fact that the threat of a data
26 breach has been a well-known risk to Defendant, especially due to the valuable and
27 sensitive nature of the data Defendant collects, stores and maintains, Defendant failed
28 to take reasonable steps to adequately protect the Private Information of current and

1 former students and educators. The Data Breach was a direct result of Defendant’s
2 failure to implement adequate and reasonable cyber-security procedures and protocols
3 necessary to protect Private Information.

4 9. As a result of Defendant’s failure to take reasonable steps to adequately
5 protect the Private Information of current and former students and educators,
6 Plaintiff’s and Class members’ Private Information is now on the internet for anyone
7 and everyone to acquire, access, and use for unauthorized purposes for the foreseeable
8 future.

9 10. Defendant’s failure to implement and follow basic security procedures
10 has resulted in ongoing harm to Plaintiff and Class members who will continue to
11 experience a lack of data security for the indefinite future and remain at serious risk of
12 identity theft and fraud that would result in significant monetary loss and loss of
13 privacy.

14 11. Accordingly, Plaintiff seeks to recover damages and other relief resulting
15 from the Data Breach, including but not limited to, compensatory damages,
16 reimbursement of costs that Plaintiff and others similarly situated will be forced to
17 bear, and declaratory judgment and injunctive relief to mitigate future harms that are
18 certain to occur in light of the scope of this breach.

19 **JURISDICTION AND VENUE**

20 12. This Court has subject matter jurisdiction pursuant to the Class Action
21 Fairness Act of 2005, 28 U.S.C. § 1332(d), because the aggregate amount in
22 controversy exceeds \$5 million, exclusive of interest and costs; the number of
23 members of the proposed Class exceeds 100, and diversity exists because Plaintiff and
24 Defendant are citizens of different states. Subject matter jurisdiction is also based
25 upon the Federal Trade Commission Act (“FTCA”) and the Federal Education Rights
26 and Privacy Act (“FERPA”). This Court also has supplemental jurisdiction over the
27 state law claims pursuant to 28 U.S.C. § 1367.

1 Connecticut, New York, and Oklahoma, and possibly other States, whose Private
2 Information and other sensitive data were collected and stored by Defendant through
3 its PupilPath system and provided to students' respective school districts.

4 18. Defendant's PupilPath system is licensed to 5,000 schools nationally and
5 has a total enrollment of approximately 17 million students.

6 19. On or about between December 28, 2021, and January 8, 2022,
7 Defendant became aware of "suspicious access" to its systems.

8 20. However, it was not until on or about March 25, 2022, and in some cases
9 later than that, that Defendant began to notify school districts of the Data Breach, first
10 doing so by notifying the New York City Department of Education.

11 21. As yet, Illuminate has still failed to directly notify students and their
12 parents of the Data Breach.

13 22. As part of Defendant's contracts with the various and several school
14 districts, of which Plaintiff and Class Members were foreseeable third-party
15 beneficiaries, the school districts were required to agree to Defendant's Privacy
16 Policy, Terms of Use, Payment Authorization, and Consent to Electronic Transactions
17 and Disclosures.

18 23. Defendant promised to protect the Private Information and other data of
19 current and former students in the various and several school districts, in accordance
20 with the applicable Federal, State, and local statutes and regulations, emphasizing its
21 purported commitment to protection of Private Information and other data on its
22 website and elsewhere.

23 24. Defendant's website claims:

24 We protect your data like it's our own. In alignment with the Family
25 Educational Rights and Privacy Act (FERPA), we deploy
26 meaningful safeguards to protect student data.

27 We pledge our unwavering commitment to student data privacy.
28

1 We aim to give educators the confidence that all your data remains
2 secure when you use our site and services.

3 Whether collected directly from our Website or maintained on behalf
4 of your Educational Organization, protecting the privacy of your
5 information is important to us. We take security measures—physical,
6 electronic, and procedural—to help defend against the unauthorized
7 access and disclosure of your information. In addition to the
8 restrictions discussed in this Privacy Policy, our employees are
9 required to comply with information security safeguards, and our
10 systems are protected by technological measures to help prevent
11 unauthorized individuals from gaining access. The specific measures
12 Illuminate takes to secure your information are defined by the
13 contract between Illuminate and your Educational Organization.
14 These measures meet or exceed the requirements of applicable
15 federal and state law. Illuminate’s employees are trained to observe
16 and comply with applicable federal and state privacy laws in the
17 handling, processing, and storage of your information.

18 25. Defendant has failed to maintain the confidentiality of Private
19 Information and other data, failed to prevent cybercriminals from access and use of
20 Private Information and other data, failed to avoid accidental loss, disclosure, or
21 unauthorized access to Private Information and other data, failed to prevent the
22 unauthorized disclosure of Private Information and other data, and failed to provide
23 security measures consistent with industry standards for the protection of PII and other
24 data, of current and former students whose data Defendant has collected and stored.

25 26. This Data Breach was foreseeable, in light of the much-publicized wave
26 of data breaches in recent years. Since at least 2015, the Federal Bureau of
27 Investigation (“FBI”) has specifically advised private industry about the threat of
28 “Business E-Mail Compromise” (“BEC”). The FBI calls BEC “a growing financial
fraud that is more sophisticated than any similar scam the FBI has seen before and
one—in its various forms—that has resulted in actual and attempted losses of more
than a billion dollars to businesses worldwide.” The FBI notes that “scammers’

1 methods are extremely sophisticated,” and warns companies that “the criminals often
2 employ malware to infiltrate company networks.”¹

3 27. Accordingly, Defendant knew, or should have known, given the vast
4 amount of Private Information and other data it collects, manages, and maintains, that
5 they were targets of security threats, and therefore understood the risks posed by
6 unsecure data security practices and systems. Defendant’s failure to heed warnings
7 and to otherwise maintain adequate security practices resulted in this Data Breach.

8 28. Defendant, at all relevant times, had a duty to Plaintiff and Class
9 members to properly secure their Private Information and other data, encrypt and
10 maintain such information using industry standard methods, train their employees,
11 utilize available technology to defend their systems from invasion, act reasonably to
12 prevent foreseeable harm to Plaintiff and Class members, and promptly notify the
13 respective school districts, Plaintiff and Class members when Defendant became
14 aware of the potential that Plaintiff’s and Class Members’ Private Information and
15 other data may have been compromised.

16 29. Defendant’s duty to use reasonable security measures arose as a result of
17 the special relationship that existed between Defendant, on the one hand, and Plaintiff
18 and the Class Members, on the other hand. The special relationship arose because
19 Plaintiff and the Members of the Class entrusted Defendant with their Private
20 Information and other data by virtue of being students at the respective school districts
21 with which Defendant had contracted to provide services, and by virtue of Federal,
22 State and local statutes and regulations. Defendant had the resources necessary to
23 prevent the Data Breach but neglected to adequately invest in security measures,
24 despite their obligation to protect such information. Accordingly, Defendant breached
25 their common law, statutory, and other duties owed to Plaintiff and Class Members.

26 _____
27 ¹ BUSINESS E-MAIL COMPROMISE: AN EMERGING GLOBAL THREAT,
28 <https://www.fbi.gov/news/stories/business-e-mail-compromise> (last visited June 13,
2022).

1 30. Defendant’s duty to use reasonable security measures also arose under
2 Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits
3 “unfair . . . practices in or affecting commerce,” including, as interpreted and enforced
4 by the FTC, the unfair practice of failing to use reasonable measures to protect
5 confidential data by entities such as Defendant.

6 31. Defendant’s duty to use reasonable security measures also arose under
7 the Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g, which states that
8 “any data collected under this subparagraph shall be protected in a manner that will
9 not permit the personal identification of students and their parents”.

10 32. Defendant’s duty to use reasonable security measures also arose under
11 the California Consumer Privacy Act.

12 33. The FTC has established data security principles and practices for
13 businesses as set forth in its publication, Protecting Personal Information: A Guide for
14 Business.² Among other things, the FTC states that companies should encrypt
15 information stored on computer networks and dispose of consumer information that is
16 no longer needed. The FTC also says to implement policies for installing vendor-
17 approved patches to correct problems, and to identify operating systems. The FTC
18 also recommends that companies understand their network’s vulnerabilities and
19 develop and implement policies to rectify security deficiencies. Further, the FTC
20 recommends that companies utilize an intrusion detection system to expose a data
21 breach as soon as it occurs; monitor all incoming traffic for activity that might indicate
22 unauthorized access into the system; monitor large amounts of data transmitted from
23 the system and have a response plan ready in the event of a data breach. The FTC
24 describes “identifying information” as “any name or number that may be used, alone
25 or in conjunction with any other information, to identify a specific person,” including,
26

27 ² https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_protecting-
28 [personal-information.pdf](https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_protecting-personal-information.pdf) (last visited June 13, 2022).

1 among other things, “[n]ame, Social Security number, date of birth, official State or
2 government issued driver’s license or identification number, alien registration number,
3 government passport number, employer or taxpayer identification number.” (17
4 C.F.R. § 248.201 (2013)).

5 34. The FTC has prosecuted a number of enforcement actions against
6 companies for failing to take measures to adequately and reasonably protect consumer
7 data. The FTC has viewed and treated such security lapses as an unfair act or practice
8 prohibited by Section 5 of the Federal Trade Commission Act (“FTCA”), 15 U.S.C.
9 § 45.

10 35. Defendant failed to maintain reasonable data security procedures and
11 practices.

12 36. Accordingly, Defendant did not comply with state and federal statutory
13 and regulatory requirements and industry standards, as discussed above.

14 37. Defendant was at all times fully aware of their obligations to protect the
15 Private Information and other data of current and former students. Defendant was also
16 aware of the significant consequences that would result from its failure to do so.

17 38. To date, Defendant may have merely offered identity monitoring to those
18 affected by the Data Breach. The offer, however, is wholly inadequate as it fails to
19 provide for the fact that victims of data breaches and other unauthorized disclosures
20 commonly face multiple years of ongoing identity theft, and it entirely fails to provide
21 any compensation for the unauthorized release and disclosure of Plaintiff’s and Class
22 Members’ Personal Information and other data.

23 39. Furthermore, Defendant’s identity monitoring offer to Plaintiff and Class
24 Members squarely places the burden on Plaintiff and Class Members, rather than upon
25 the Defendant, to investigate and protect themselves from Defendant’s tortious acts
26 resulting in the Data Breach, rather than automatically enrolling Plaintiff and Class
27 Members in identity monitoring services upon discovery of the breach.

28

1 40. As a result of the Data Breach and Defendant’s failure to provide timely
2 notice to Plaintiff and Class Members, Plaintiff and Class Members’ Private
3 Information and other data are now in the hands of unknown hackers, and Plaintiff
4 and Class Members now face an imminent, heightened, and substantial risk of identity
5 theft and other fraud, which is a concrete and particularized injury traceable to
6 Defendant’s conduct. Accordingly, Plaintiff and the Class Members have suffered
7 “injury-in-fact.” See *Attias v. CareFirst, Inc.*, 865 F.3d 620 (D.C. Cir. 2017).

8 41. As a direct and proximate result of Defendant’s wrongful actions and
9 inaction, Plaintiff and Class Members have suffered injury and damages, including the
10 increased risk of identity theft and identity fraud, improper disclosure of Private
11 Information and other data, the time and expense necessary to mitigate, remediate, and
12 sort out the increased risk of identity theft and to deal with governmental agencies,
13 including the various departments of education.

14 **CLASS ACTION ALLEGATIONS**

15 42. Plaintiff brings this action and seeks to certify and maintain it as a class
16 action under Federal Rules of Civil Procedure 23(a), (b)(2), (b)(3), and/or (c)(4), on
17 behalf of herself, and the following proposed Classes (collectively, the “Class”).

18 43. The Nationwide Class is defined as follows: All individuals residing in
19 the United States whose Private Information and other data was compromised in the
20 Data Breach occurring in or about December 2021 to January 2022.

21 44. The California Class is defined as follows: All individuals residing in
22 California whose Private Information and other data was compromised in the Data
23 Breach occurring in or about December 2021 to January 2022.

24 45. The Colorado Class is defined as follows: All individuals residing in
25 Colorado whose Private Information and other data was compromised in the Data
26 Breach occurring in or about December 2021 to January 2022.

1 46. The Connecticut Class is defined as follows: All individuals residing in
2 Connecticut whose Private Information and other data was compromised in the Data
3 Breach occurring in or about December 2021 to January 2022.

4 47. The New York Class is defined as follows: All individuals residing in
5 New York whose Private Information and other data was compromised in the Data
6 Breach occurring in or about December 2021 to January 2022.

7 48. The Oklahoma Class is defined as follows: All individuals residing in
8 Oklahoma whose Private Information and other data was compromised in the Data
9 Breach occurring in or about December 2021 to January 2022.

10 49. Excluded from each of the above proposed Classes are: Defendant, any
11 entity in which Defendant has a controlling interest, is a parent or subsidiary, or which
12 is controlled by Defendant, as well as the officers, directors, affiliates, legal
13 representatives, heirs, predecessors, successors, and assigns of Defendant; and judicial
14 officers to whom this case is assigned and their immediate family members.

15 50. Plaintiff reserves the right to re-define the Class definitions after
16 conducting discovery.

17 51. Each of the proposed Classes meets the criteria for certification under
18 Rule 23(a), (b)(2), (b)(3) and/or (c)(4).

19 52. Numerosity. Fed. R. Civ. P. 23(a)(1). Pursuant to Rule 23(a)(1), the
20 members of the Class are so numerous and geographically dispersed that the joinder
21 of all members is impractical. While the exact number of Class members is unknown
22 to Plaintiff at this time, the proposed Class includes potentially millions of individuals
23 whose Private Information and other data was compromised in the Data Breach. Class
24 members may be identified through objective means, including by and through
25 Defendant's business records and those of the respective school districts. Class
26 members may be notified of the pendency of this action by recognized, Court-
27 approved notice dissemination methods, which may include U.S. mail, electronic
28 mail, internet postings, and/or published notice.

1 53. Commonality. Fed. R. Civ. P. 23(a)(2) and (b)(3). Pursuant to Rule
2 23(a)(2) and with 23(b)(3)'s predominance requirement, this action involves common
3 questions of law and fact that predominate over any questions affecting individual
4 Class Members. The common questions include:

- 5 (a) Whether Defendant had a legal duty to implement and maintain
6 reasonable security procedures and practices for the protection of
7 Plaintiff's and Class Members' Private Information and other data;
8 (b) Whether Defendant breached its legal duty to implement and
9 maintain reasonable security procedures and practices for the
10 protection of Plaintiff's and Class Members' Private Information
11 and other data;
12 (c) Whether Defendant's conduct, practices, actions, and omissions,
13 resulted in or were the proximate cause of the data breach,
14 resulting in the loss of Private Information and other data of
15 Plaintiff and Class Members;
16 (d) Whether Defendant had a legal duty to provide timely and accurate
17 notice of the Data Breach to Plaintiff and Class Members;
18 (e) Whether Defendant breached its duty to provide timely and
19 accurate notice of the Data Breach to Plaintiff and Class Members;
20 (f) Whether and when Defendant knew or should have known that its
21 computer systems were vulnerable to attack;
22 (g) Whether Defendant failed to implement and maintain reasonable
23 and adequate security measures, procedures, and practices to
24 safeguard Plaintiff's and Class Members' Private Information and
25 other data;
26 (h) Whether Defendant breached express or implied contract with the
27 various and several school districts and Plaintiff and the Class in
28

1 failing to have adequate data security measures despite promising
2 to do so;

3 (i) Whether Defendant's conduct was negligent;

4 (j) Whether Defendant's conduct was *per se* negligent;

5 (k) Whether Defendant's practices, actions, and omissions constitute
6 unfair or deceptive business practices;

7 (l) Whether Plaintiff and Class Members suffered legally cognizable
8 damages as a result of Defendant's conduct, including increased
9 risk of identity theft and loss of value of their personal and
10 financial information; and

11 (m) Whether Plaintiff and Class Members are entitled to relief,
12 including damages and equitable relief.

13 53. Typicality. Fed. R. Civ. P. 23(a)(3). Pursuant to Rule 23(a)(3), Plaintiff's
14 claims are typical of the claims of the Members of the Class. Plaintiff, as all Members
15 of the Class, were injured through Defendant's uniform misconduct described above
16 and asserts similar claims for relief. The same events and conduct that give rise to
17 Plaintiff's claims also give rise to the claims of every other Class Member because
18 Plaintiff and each Class Member are persons that have suffered harm as a direct result
19 of the same conduct engaged in by Defendant and resulting in the Data Breach.

20 54. Adequacy of Representation (Fed. R. Civ. P. 23(a)(4). Pursuant to Rule
21 23(a)(4), Plaintiff and their counsel will fairly and adequately represent the interests of
22 the Class Members. Plaintiff has no interest antagonistic to, or in conflict with, the
23 interests of the Class Members. Plaintiff's attorneys are highly experienced in the
24 prosecution of consumer class actions and data breach cases.

25 55. Superiority (Fed. R. Civ. P. 23(b)(3). Pursuant to Rule 23(b)(3), a class
26 action is superior to individual adjudications of this controversy. Litigation is not
27 economically feasible for individual Members of the Class because the amount of
28 monetary relief available to individual Plaintiff is insufficient in the absence of the

1 class action procedure. Separate litigation could yield inconsistent or contradictory
2 judgments and increase the delay and expense to all parties and the court system. A
3 class action presents fewer management difficulties and provides the benefits of a
4 single adjudication, economy of scale, and comprehensive supervision by a single
5 court.

6 56. Risk of Inconsistent or Dispositive Adjudications and the
7 Appropriateness of Final Injunctive or Declaratory Relief (Fed. R. Civ. P. 23(b)(1)
8 and (2)). In the alternative, this action may properly be maintained as a class action,
9 because:

- 10 (a) The prosecution of separate actions by individual members of the
11 Class would create a risk of inconsistent or varying adjudication
12 with respect to individual members of the Class, which would
13 establish incompatible standards of conduct for Defendant; or
14 (b) The prosecution of separate actions by individual Members of the
15 Class would create a risk of adjudications with respect to
16 individual Members of the Class which would, as a practical
17 matter, be dispositive of the interests of other Members of the
18 Class not parties to the adjudications, or substantially impair or
19 impede their ability to protect their interests; or
20 (c) Defendant has acted or refused to act on grounds generally
21 applicable to the Class, thereby making appropriate final injunctive
22 or corresponding declaratory relief with respect to the Class as a
23 whole.

24 57. Issue Certification (Fed. R. Civ. P. 23(c)(4)). In the alternative, the
25 common questions of fact and law, set forth above, are appropriate for issue
26 certification on behalf of the proposed Class.

FIRST CAUSE OF ACTION FOR NEGLIGENCE
(On behalf of Plaintiff, the Nationwide Class and the California, Colorado, Connecticut, New York and Oklahoma Classes)

1
2
3 58. The Plaintiff repeats, reiterates and realleges each and every allegation
4 set forth in the preceding paragraphs above as if set forth in full herein.

5 59. Defendant required Plaintiff and Class Members to submit non-public,
6 sensitive PII and other data via its contracts with the respective school districts.

7 60. Defendant had, and continues to have, a duty to Plaintiff and Class
8 Members to exercise reasonable care in safeguarding and protecting their Private
9 Information and other data. Defendant also had, and continues to have, a duty to use
10 ordinary care in activities from which harm might be reasonably anticipated, such as
11 in the collection, storage and protection of Private Information and other data within
12 their possession, custody and control and that of its vendors.

13 61. Defendant's duty to use reasonable security measures arose as a result of
14 the special relationship that existed between Defendant and students and former
15 students. The special relationship arose because Plaintiff and the Members of the
16 Class had entrusted Defendant with their Private Information and other data by virtue
17 of being students at the respective school districts with which Defendant had
18 contracted to provide services. Only Defendant was in a position to ensure that its
19 systems were sufficient to protect against the harm to Plaintiff and the Class Members
20 from a data breach.

21 62. Defendant violated these standards and duties by failing to exercise
22 reasonable care in safeguarding and protecting Plaintiff and Class Members' Private
23 Information and other data by failing to design, adopt, implement, control, direct,
24 oversee, manage, monitor, and audit appropriate data security processes, controls,
25 policies, procedures, protocols, and software and hardware systems to safeguard and
26 protect the Private Information and other data entrusted to it, including Plaintiff and
27 Class Members' Private Information and other data as aforesaid. It was reasonably
28 foreseeable to Defendant that its failure to exercise reasonable care in safeguarding

1 and protecting Plaintiff and Class Members' Private Information and other data by
2 failing to design, adopt, implement, control, direct, oversee, manage, monitor, and
3 audit appropriate data security processes, controls, policies, procedures, protocols, and
4 software and hardware systems would result in the unauthorized release, disclosure,
5 and dissemination of Plaintiff and Class Members' Private Information and other data.

6 63. Defendant, by and through its negligent actions, inaction, omissions, and
7 want of ordinary care, unlawfully breached its duties to Plaintiff and Class Members
8 by, *inter alia*, failing to exercise reasonable care in safeguarding and protecting
9 Plaintiff and Class Members' Private Information and other data within their
10 possession, custody and control.

11 64. Defendant, by and through its negligent actions, inactions, omissions, and
12 want of ordinary care, further breached its duties to Plaintiff and Class Members by
13 failing to design, adopt, implement, control, direct, oversee, manage, monitor and
14 audit their processes, controls, policies, procedures, protocols, and software and
15 hardware systems for complying with the applicable laws and safeguarding and
16 protecting their Private Information and other data.

17 65. But for Defendant's negligent breach of the above-described duties owed
18 to Plaintiff and Class Members, their Private Information and other data would not
19 have been released, disclosed, and disseminated without their authorization.

20 66. Plaintiff and Class Members' Private Information and other data was
21 transferred, sold, opened, viewed, mined and otherwise released, disclosed, and
22 disseminated to unauthorized persons without their authorization as the direct and
23 proximate result of Defendant's failure to design, adopt, implement, control, direct,
24 oversee, manage, monitor and audit its processes, controls, policies, procedures and
25 protocols for complying with the applicable laws and safeguarding and protecting
26 Plaintiff and Class Members' Private Information and other data.

27 67. As a direct and proximate result of Defendant's above-described
28 wrongful actions, inaction, omissions, and want of ordinary care that directly and

1 proximately caused the Data Breach, Plaintiff and Class Members have suffered, and
2 will continue to suffer, ongoing, imminent, and impending threat of identity theft
3 crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual
4 identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm;
5 loss of the confidentiality of the stolen confidential data; the illegal sale of the
6 compromised data on the dark web; expenses and/or time spent on credit monitoring
7 and identity theft insurance; time spent scrutinizing bank statements, credit card
8 statements, and credit reports; expenses and/or time spent initiating fraud alerts,
9 decreased credit scores and ratings; lost work time; and other economic and non-
10 economic harm.

11 68. Defendant's above-described wrongful actions, inaction, omissions, and
12 want of ordinary care that directly and proximately caused this Data Breach constitute
13 negligence.

14 69. Plaintiff is entitled to compensatory and consequential damages suffered
15 as a result of the Data Breach.

16 70. Plaintiff is also entitled to injunctive relief requiring Illuminate to, *e.g.*,
17 (i) strengthen its data security programs and monitoring procedures; (ii) submit to
18 future annual audits of those systems and monitoring procedures; and (iii)
19 immediately provide robust and adequate credit monitoring to all Class Members, and
20 any other relief this Court deems just and proper.

21 **SECOND CAUSE OF ACTION FOR NEGLIGENCE *PER SE***
22 **(On behalf of Plaintiff, the Nationwide Class and the California, Colorado,**
23 **Connecticut, New York and Oklahoma Classes)**

24 69. The Plaintiff repeats, reiterates and realleges each and every allegation
25 set forth in the preceding paragraphs above as if set forth in full herein.

26 70. Pursuant to the Federal Trade Commission Act ("FTCA"), 15 U.S.C. §
27 45, Defendant had a duty to provide fair and adequate computer systems and data
28

1 security to safeguard the personal and financial information of Plaintiff and Class
2 Members.

3 71. The FTCA prohibits “unfair . . . practices in or affecting commerce,”
4 including, as interpreted and enforced by the FTC, the unfair act or practice by
5 businesses, such as Defendant, of failing to use reasonable measures to protect the
6 Private Information and other data of Plaintiff and Class Members. The pertinent FTC
7 publications and orders form part of the basis of Defendant’s duty in this regard.

8 72. Defendant required, gathered, and stored personal and financial
9 information of Plaintiff and Class Members to fulfill its contracts with the various and
10 several school districts.

11 73. Defendant violated the FTCA by failing to use reasonable measures to
12 protect the Private Information and other data of Plaintiff and Class Members and by
13 not complying with applicable industry standards, as described herein.

14 74. Plaintiff and Class Members are within the class of persons that the FTC
15 Act was intended to protect.

16 75. The harm that occurred as a result of the Data Breach is the type of harm
17 the FTCA was intended to guard against. The FTC has pursued enforcement actions
18 against businesses, which, as a result of their failure to employ reasonable data
19 security measures and avoid unfair and deceptive practices, caused the same harm as
20 that suffered by Plaintiff and Class Members.

21 76. As a direct and proximate result of Defendant’s negligence *per se*,
22 Plaintiff and Class Members have suffered, and continue to suffer, injuries, damages
23 arising from identify theft; from their needing to contact agencies administering
24 unemployment benefits; potentially defending themselves from legal action base upon
25 fraudulent applications for unemployment benefits made in their name; contacting
26 their financial institutions; loss of use of funds; closing or modifying financial
27 accounts; damages from lost time and effort to mitigate the actual and potential impact
28 of the data breach on their lives; closely reviewing and monitoring their accounts for

1 unauthorized activity which is certainly impending; placing credit freezes and credit
2 alerts with credit reporting agencies; and damages from identify theft, which may take
3 months or years to discover and detect.

4 77. Defendant's violation of the FTCA constitutes negligence *per se*.

5 78. For the same reasons and upon the same bases, Defendant's violation of
6 the Family Educational Rights and Privacy Act, the California Consumer Privacy Act,
7 the California Customer Records Act, the California Unfair Competition Law, the
8 New York SHIELD Act and New York GBL §349 and various other State and local
9 statutes, constitutes negligence *per se*.

10 79. As a direct and proximate result of Defendant's violation of the foregoing
11 statutes and regulations, Plaintiff and Class Members have suffered injury and are
12 entitled to compensatory, consequential, and punitive damages in an amount to be
13 proven at trial.

14 **THIRD CAUSE OF ACTION FOR BREACH OF CONTRACT**
15 **(On behalf of Plaintiff, the Nationwide Class and the California, Colorado,**
16 **Connecticut, New York and Oklahoma Classes)**

17 79. The Plaintiff repeats, reiterates and realleges each and every allegation
18 set forth in the preceding paragraphs above as if set forth in full herein.

19 80. Defendant required, gathered, and stored Private Information and other
20 data of Plaintiff and Class Members to fulfill its contracts with the various and several
21 school districts.

22 81. There was offer, acceptance and consideration, the consideration being
23 the fees paid by the various and several school districts for Defendant's services,
24 including the provisions of those agreements pertaining to the protection of students'
25 and former students' Private Information and other data.

26 82. The various and several school districts have performed and satisfied all
27 of their obligations to Defendant pursuant to their contracts.
28

1 83. Defendant breached its contractual obligations to protect the students’
2 and former students’ Private Information and other data it possessed and with which it
3 was entrusted when the information was accessed by unauthorized persons as part of
4 the Data Breach.

5 84. Plaintiff and Class Members were foreseeable third-party beneficiaries of
6 said contracts.

7 85. As a direct and proximate result of Defendant’s breach of contract,
8 Plaintiff and Class Members have suffered, and continue to suffer, injuries, damages
9 arising from identify theft; from their needing to contact educational agencies;
10 potentially defending themselves from legal action base upon fraudulent applications
11 for benefits made in their names; contacting their financial institutions; loss of use of
12 funds; closing or modifying financial accounts; damages from lost time and effort to
13 mitigate the actual and potential impact of the Data Breach on their lives; closely
14 reviewing and monitoring their accounts for unauthorized activity which is certainly
15 impending; placing credit freezes and credit alerts with credit reporting agencies; and
16 damages from identity theft, which may take months or years to discover and detect.

17 86. The above constitutes breach of contract by Defendant.

18 87. The Plaintiff repeats, reiterates and realleges each and every allegation
19 set forth in the preceding paragraphs above as if set forth in full herein.

20 88. Defendant required, gathered, and stored Private Information and other
21 data of Plaintiff and Class Members to fulfill its contracts with the various and several
22 school districts.

23 89. By virtue of the above, Defendant entered into implied contracts with
24 Plaintiff and Class Members by which Defendant agreed to safeguard and protect such
25 information, to keep such information secure and confidential, and to timely and
26 accurately notify Plaintiff and Class Members if their data had been breached and
27 compromised or stolen.

28

1 90. Plaintiff and Class Members fully performed their obligations under the
2 implied contracts with Defendant.

3 91. Defendant breached the implied contracts it made with Plaintiff and Class
4 Members by failing to safeguard and protect student' and former students' Private
5 Information and other data, and by failing to provide timely and accurate notice to
6 them that Private Information and other data was compromised as a result of the Data
7 Breach.

8 92. As a direct and proximate result of Defendant's breach of implied
9 contract, Plaintiff and Class Members have suffered, and continue to suffer, injuries,
10 damages arising from identify theft; from their needing to contact agencies
11 administering benefits; potentially defending themselves from legal action base upon
12 fraudulent applications for unemployment benefits made in their name; contacting
13 their financial institutions; loss of use of funds; closing or modifying financial
14 accounts; damages from lost time and effort to mitigate the actual and potential impact
15 of the data breach on their lives; closely reviewing and monitoring their accounts for
16 unauthorized activity which is certainly impending; placing credit freezes and credit
17 alerts with credit reporting agencies; and damages from identify theft, which may take
18 months or years to discover and detect.

19 93. The above constitutes breach of implied contract by Defendant.

20 94. Plaintiff and Class Members are therefore entitled to damages, including
21 restitution and unjust enrichment, disgorgement, declaratory and injunctive relief, and
22 attorney fees, costs, and expenses.

23 **FOURTH CAUSE OF ACTION FOR MISREPRESENTATION**
24 **(On behalf of Plaintiff, the Nationwide Class and the California, Colorado,**
25 **Connecticut, New York and Oklahoma Classes)**

26 94. The Plaintiff repeats, reiterates and realleges each and every allegation set
27 forth in the preceding paragraphs above as if set forth in full herein.

1 95. A special, privity-like relationship existed between Defendant and
2 Plaintiff and Class Members herein because Plaintiff and the Members of the Class
3 entrusted Defendant with their Private Information and other data by virtue of being
4 students at the respective school districts with which Defendant had contracted to
5 provide services, and by virtue of Federal, State and local statutes and regulations.

6 96. The Defendant incorrectly represented to Plaintiff and Class Members
7 that they would take appropriate measures to safeguard their Private Information and
8 other data and promptly notify them of a data breach.

9 97. Plaintiff and Class Members reasonably relied upon said representations
10 in that they held Defendant in a position of trust as guardians of their Private
11 Information and other data.

12 98. As a direct and proximate result of Defendant's misrepresentation,
13 Plaintiff and Class Members have suffered, and continue to suffer, injuries, damages
14 arising from identify theft; from their needing to contact agencies administering
15 benefits; potentially defending themselves from legal action base upon fraudulent
16 applications for benefits made in their name; contacting their financial institutions;
17 loss of use of funds; closing or modifying financial accounts; damages from lost time
18 and effort to mitigate the actual and potential impact of the data breach on their lives;
19 closely reviewing and monitoring their accounts for unauthorized activity which is
20 certainly impending; placing credit freezes and credit alerts with credit reporting
21 agencies; and damages from identify theft, which may take months or years to
22 discover and detect.

23 99. The above constitutes misrepresentation on the part of Defendant.

24 **FIFTH CAUSE OF ACTION FOR BREACH OF FIDUCIARY DUTY**
25 **(On behalf of Plaintiff, the Nationwide Class and the California, Colorado,**
26 **Connecticut, New York and Oklahoma Classes)**

27 100. The Plaintiff repeats, reiterates and realleges each and every allegation
28 set forth in the preceding paragraphs above as if set forth in full herein.

1 101. A fiduciary relationship existed between Plaintiff and Class Members and
2 Defendant, in that Defendant was in a position of trust with respect to Plaintiff and
3 Class Members by virtue of being students at the respective school districts with
4 which Defendant had contracted to provide services, and by virtue of Federal, State
5 and local statutes and regulations.

6 102. Defendant owed a duty to Plaintiff and Class Members to insure that the
7 Private Information and other data entrusted to them was safeguarded pursuant to
8 common law and statute.

9 103. The Defendant engaged in misconduct, consisting of the failure to
10 safeguard the Private Information and other data of Plaintiff and Class Members that
11 had been entrusted to them, in violation of the duty to exercise due care, their
12 contractual obligations and their statutory obligations pursuant to the Federal Trade
13 Commission Act (“FTCA”), the Family Educational Rights and Privacy Act, the
14 California Consumer Privacy Act, the California Customer Records Act, the
15 California Unfair Competition Law, the New York SHIELD Act and New York GBL
16 §349 and various other State and local statutes, constitutes negligence *per se*.

17 104. As a direct and proximate result of Defendant’s breach of fiduciary duty,
18 Plaintiff and Class Members have suffered, and continue to suffer, injuries, damages
19 arising from identify theft; from their needing to contact agencies administering
20 benefits; potentially defending themselves from legal action base upon fraudulent
21 applications for benefits made in their name; contacting their financial institutions;
22 loss of use of funds; closing or modifying financial accounts; damages from lost time
23 and effort to mitigate the actual and potential impact of the data breach on their lives;
24 closely reviewing and monitoring their accounts for unauthorized activity which is
25 certainly impending; placing credit freezes and credit alerts with credit reporting
26 agencies; and damages from identify theft, which may take months or years to
27 discover and detect.

28

1 105. As a direct and proximate result of Defendant’s breach of their fiduciary
2 duty, Plaintiff and Class Members have suffered and will continue to suffer other
3 forms of injury and/or harm, and other economic and non-economic losses.

4 106. The above constitutes breach of fiduciary duty on the part of Defendant.

5 **SIXTH CAUSE OF ACTION FOR INVASION OF PRIVACY**
6 **(On behalf of Plaintiff, the Nationwide Class and the California, Colorado,**
7 **Connecticut, New York and Oklahoma Classes)**

8 107. The Plaintiff repeats, reiterates and realleges each and every allegation
9 set forth in the preceding paragraphs above as if set forth in full herein.

10 108. Plaintiff and the Class Members have a legally protected privacy interest
11 in their Private Information, which is and was collected, stored and maintained by
12 Defendant, and they are entitled to the reasonable and adequate protection of their
13 Private Information against foreseeable unauthorized access, as occurred with the
14 Data Breach.

15 109. Plaintiff and the Class Members reasonably expected that Defendant
16 would protect and secure their Private Information from unauthorized parties and that
17 their Private Information would not be accessed, exfiltrated, and disclosed to any
18 unauthorized parties or for any improper purpose.

19 110. The Defendant unlawfully invaded the privacy rights of Plaintiff and the
20 Class Members by engaging in the conduct described above, including by failing to
21 protect their Private Information by permitting unauthorized third-parties to access,
22 exfiltrate and view this Private Information. Likewise, Defendant further invaded the
23 privacy rights of Plaintiff and Class Members, and permitted cybercriminals to invade
24 the privacy rights of Plaintiff and Class Members, by unreasonably and intentionally
25 delaying disclosure of the Data Breach, and failing to properly identify what Private
26 Information had been accessed, exfiltrated, and viewed by unauthorized third-parties.

1 111. This invasion of privacy resulted from Defendant’s failure to properly
2 secure and maintain Plaintiff and Class Members’ Private Information, leading to the
3 foreseeable unauthorized access, exfiltration, and disclosure of this unguarded data.

4 112. Plaintiff and Class Members’ Private Information is the type of sensitive,
5 personal information that one normally expects will be protected from exposure by the
6 very entity charged with safeguarding it. Further, the public has no legitimate concern
7 in Plaintiff and Class Members’ Private Information, and such information is
8 otherwise protected from exposure to the public by various statutes, regulations and
9 other laws.

10 113. The disclosure of Plaintiff and Class Members’ Private Information to
11 unauthorized parties is substantial and unreasonable enough to be legally cognizable
12 and is highly offensive to a reasonable person.

13 114. Defendant’s willful and reckless conduct which permitted unauthorized
14 access, exfiltration and disclosure of Plaintiff and Class Members’, Private
15 Information is such that it would cause serious mental injury, shame or humiliation to
16 people of ordinary sensibilities.

17 115. The unauthorized access, exfiltration, and disclosure of Plaintiff and
18 Class Members’ Private Information was without their consent, and in violation of
19 various statutes, regulations and other laws.

20 116. As a result of the invasion of privacy caused by Defendant, Plaintiff and
21 Class Members suffered and will continue to suffer damages and injury as set forth
22 herein.

23 117. Plaintiff and Class Members seek all monetary and non-monetary relief
24 allowed by law, including damages, punitive damages, restitution, injunctive relief,
25 reasonable attorneys’ fees and costs, and any other relief that is just and proper.
26
27
28

1 **SEVENTH CAUSE OF ACTION FOR VIOLATION OF CALIFORNIA**
2 **UNFAIR COMPETITION LAW (CAL. BUS. & PROF. CODE §§ 17200, ET**
3 **SEQ.)**

4 **(On behalf of Plaintiff, the Nationwide Class and the California Class)**

5 118. The Plaintiff repeats, reiterates and realleges each and every allegation
6 set forth in the preceding paragraphs above as if set forth in full herein.

7 119. Defendant engaged in deceptive, unfair, and unlawful trade acts or
8 practices in the conduct of trade or commerce and furnishing of services, in violation
9 of Cal. Bus. & Prof. Code §§17200, *et. seq.*, including but not limited to the
10 following:

- 11 (a) Defendant misrepresented material facts to Plaintiff, the
12 Nationwide Class and California Class Members by representing
13 that they would maintain adequate data privacy and security
14 practices and procedures to safeguard Plaintiff, the Nationwide
15 Class and California Class members' Private Information and other
16 data from unauthorized disclosure, release, data breaches, and
17 theft;
- 18 (b) Defendant misrepresented material facts to Plaintiff, the
19 Nationwide Class and California Class Members by representing
20 that they did and would comply with the requirements of federal
21 and state laws pertaining to the privacy and security of Plaintiff,
22 the Nationwide Class and California Class Members' Private
23 Information and other data;
- 24 (c) Defendant omitted, suppressed, and concealed material facts of the
25 inadequacy of its privacy and security protections for Plaintiff, the
26 Class and California Class Members' Private Information and
27 other data;
- 28

- 1 (d) Defendant misrepresented material facts to Plaintiff, the
2 Nationwide Class and California Class Members by representing
3 that they would maintain adequate data privacy and security
4 practices and procedures to safeguard Plaintiff, the Nationwide
5 Class and California and Class Members' Private Information and
6 other data from unauthorized disclosure, release, data breaches,
7 and theft;
- 8 (e) Defendant misrepresented material facts to Plaintiff, the
9 Nationwide Class and California Class Members by representing
10 that they did and would comply with the requirements of federal
11 and state laws pertaining to the privacy and security of Plaintiff,
12 the Nationwide Class and California Class Members' Private
13 Information and other data;
- 14 (f) Defendant omitted, suppressed, and concealed material facts of the
15 inadequacy of its privacy and security protections for Plaintiff, the
16 Nationwide Class and California Class Members' Private
17 Information and other data;
- 18 (g) Defendant engaged in deceptive, unfair, and unlawful trade acts or
19 practices by failing to maintain the privacy and security of
20 Plaintiff, the Nationwide Class and California Class Members'
21 Private Information and other data, in violation of duties imposed
22 by and public policies reflected in applicable federal and state
23 laws, resulting in the Data Breach. These unfair acts and practices
24 violated duties imposed by laws including the Federal Trade
25 Commission Act (15 U.S.C. § 45);
- 26 (h) Defendant engaged in deceptive, unfair, and unlawful trade acts or
27 practices by failing to disclose the Data Breach to Plaintiff, the
28 Nationwide Class and California Class Members in a timely and

1 accurate manner, contrary to the duties imposed by various federal
2 and state statutes and regulations.

3 119. Defendant’s failure constitutes false and misleading representations,
4 which have the capacity, tendency, and effect of deceiving or misleading consumers
5 (including Plaintiff, the Nationwide Class and California Class Members) regarding
6 the security of its network and aggregation of Private Information and other data.

7 120. The misrepresentations upon which consumers (including Plaintiff, the
8 Nationwide Class and California Class Members) relied were material
9 misrepresentations (*e.g.*, as to Defendant’s adequate protection of Private Information
10 and other data), and consumers (including Plaintiff, the Nationwide Class and
11 California Class Members) relied on those representations to their detriment.

12 121. Defendant’s conduct is unconscionable, deceptive, and unfair, as it is
13 likely to, and did, mislead consumers acting reasonably under the circumstances. As a
14 direct and proximate result of Defendant’s conduct, Plaintiff, the Nationwide Class
15 and California Class Members have been harmed, in that they were not timely notified
16 of the data breach, which resulted in profound vulnerability of their Private
17 Information and other data.

18 122. As a direct and proximate result of Defendant’s unconscionable, unfair,
19 and deceptive acts and omissions, Plaintiff, the Class and California Class Members’
20 Private Information and other data were disclosed to third parties without
21 authorization, causing and will continue to cause Plaintiff, the Nationwide Class and
22 California and Class Members damages.

23 123. As a direct and proximate result of Defendant’s violation of Cal. Bus. &
24 Prof. Code §§17200, *et. seq.*, Plaintiff, the Nationwide Class and California and Class
25 Members have suffered, and continue to suffer, injuries, damages arising from identify
26 theft; from their needing to contact agencies administering benefits; potentially
27 defending themselves from legal action base upon fraudulent applications for benefits
28 made in their name; contacting their financial institutions; loss of use of funds; closing

1 or modifying financial accounts; damages from lost time and effort to mitigate the
2 actual and potential impact of the data breach on their lives; closely reviewing and
3 monitoring their accounts for unauthorized activity which is certainly impending;
4 placing credit freezes and credit alerts with credit reporting agencies; and damages
5 from identify theft, which may take months or years to discover and detect.

6 124. Plaintiff, the Nationwide Class and California Class Members seek all
7 monetary and non-monetary relief allowed by law, including restitution of all profits
8 stemming from Defendant’s unfair, unlawful, and fraudulent business practices or use
9 of their Private Information; declaratory relief; reasonable attorneys’ fees and costs
10 under California Code of Civil Procedure § 1021.5; injunctive relief; and other
11 appropriate equitable relief.

12 125. The above constitutes violation of Cal. Bus. & Prof. Code §§17200, *et.*
13 *seq.*

14 **EIGHTH CAUSE OF ACTION FOR VIOLATION OF CALIFORNIA**
15 **CUSTOMER RECORDS ACT (CAL. CIV. CODE § 1798.80, ET SEQ.)**
16 **(On behalf of Plaintiff, the Nationwide Class and the California Class)**

17 126. The Plaintiff repeats, reiterates and realleges each and every allegation
18 set forth in the preceding paragraphs above as if set forth in full herein.

19 127. Cal. Civ. Code §1798.81.5 requires that any business that “owns,
20 licenses, or maintains Personal Information about a California resident shall
21 implement and maintain reasonable security procedures and practices appropriate to
22 the nature of the information, to protect the Personal Information from unauthorized
23 access, destruction, use, modification, or disclosure.”

24 128. Defendant committed violations of Cal. Civ. Code §1798.81.5, including
25 but not limited to by failing to design, adopt, implement, control, direct, oversee,
26 manage, monitor, and audit appropriate data security processes, controls, policies,
27 procedures, protocols, and software and hardware systems to safeguard and protect the
28

1 Private Information and other data entrusted to it, including Plaintiff, the Nationwide
2 Class and California Class Members' Private Information and other data as aforesaid.

3 129. As a direct and proximate result of Defendant's violation of Cal. Civ.
4 Code §1798.81.5, Plaintiff, the Nationwide Class and California and Class Members'
5 Private Information and other data were disclosed to third parties without
6 authorization, causing and will continue to cause Plaintiff, the Nationwide Class and
7 California Class Members damages.

8 130. As a direct and proximate result of Defendant's violation of Cal. Civ.
9 Code §1798.81.5, Plaintiff, the Nationwide Class and California Class Members have
10 suffered, and continue to suffer, injuries, damages arising from identify theft; from
11 their needing to contact agencies administering benefits; potentially defending
12 themselves from legal action base upon fraudulent applications for benefits made in
13 their name; contacting their financial institutions; loss of use of funds; closing or
14 modifying financial accounts; damages from lost time and effort to mitigate the actual
15 and potential impact of the data breach on their lives; closely reviewing and
16 monitoring their accounts for unauthorized activity which is certainly impending;
17 placing credit freezes and credit alerts with credit reporting agencies; and damages
18 from identify theft, which may take months or years to discover and detect.

19 131. The above constitutes violation of Cal. Civ. Code §1798.81.5.

20 132. Plaintiff, the Nationwide Class and California Class Members seek relief
21 under Cal. Civ. Code § 1798.84, including actual damages and injunctive relief.

22 **NINTH CAUSE OF ACTION FOR VIOLATION OF CALIFORNIA**
23 **CONSUMER PRIVACY ACT (CAL. CIV. CODE §§ 1798.150, ET SEQ.)**
24 **(On behalf of Plaintiff, the Nationwide Class and the California Class)**

25 133. The Plaintiff repeats, reiterates and realleges each and every allegation
26 set forth in the preceding paragraphs above as if set forth in full herein.

27 134. Defendant violated to California Consumer Privacy Act by failing to
28 exercise reasonable care in safeguarding and protecting Plaintiff, the Nationwide

1 Class and California Class Members' Private Information and other data by failing to
2 design, adopt, implement, control, direct, oversee, manage, monitor, and audit
3 appropriate data security processes, controls, policies, procedures, protocols, and
4 software and hardware systems to safeguard and protect the Private Information and
5 other data entrusted to it, including Plaintiff, the Nationwide Class and California
6 Class Members' Private Information and other data as aforesaid. It was reasonably
7 foreseeable to Defendant that its failure to exercise reasonable care in safeguarding
8 and protecting Plaintiff, the Nationwide Class and California Class Members' Private
9 Information and other data by failing to design, adopt, implement, control, direct,
10 oversee, manage, monitor, and audit appropriate data security processes, controls,
11 policies, procedures, protocols, and software and hardware systems would result in the
12 unauthorized release, disclosure, and dissemination of Plaintiff, the Nationwide Class
13 and California Class Members' Private Information and other data.

14 135. As a direct and proximate result of Defendant's violation of Cal. Civ.
15 Code §1798.150, et seq., Plaintiff, the Nationwide Class and California Class
16 Members' Private Information and other data were disclosed to third parties without
17 authorization, causing and will continue to cause Plaintiff, the Nationwide Class and
18 California Class Members damages.

19 136. As a direct and proximate result of Defendant's violation of Cal. Civ.
20 Code §1798. 150, et seq., Plaintiff, the Nationwide Class and California Class
21 Members have suffered, and continue to suffer, injuries, damages arising from identify
22 theft; from their needing to contact agencies administering benefits; potentially
23 defending themselves from legal action base upon fraudulent applications for benefits
24 made in their name; contacting their financial institutions; loss of use of funds; closing
25 or modifying financial accounts; damages from lost time and effort to mitigate the
26 actual and potential impact of the data breach on their lives; closely reviewing and
27 monitoring their accounts for unauthorized activity which is certainly impending;
28

1 placing credit freezes and credit alerts with credit reporting agencies; and damages
2 from identify theft, which may take months or years to discover and detect.

3 137. In accordance with Cal. Civ. Code § 1798.150(b), on or about June 10,
4 2022, Plaintiff's counsel served Defendant with notice of these CCPA violations via
5 First-Class U.S. Mail.

6 138. On behalf of Plaintiff, the Nationwide Class and California Class
7 Members, Plaintiff, the Nationwide Class and California Class Members seek
8 injunctive relief in the form of an order enjoining Defendant from continuing to
9 violate the CCPA. If Defendant fails to respond to Plaintiff's notice letter or agree to
10 rectify the violations detailed above, Plaintiff will amend this Complaint and seek
11 actual, punitive, and statutory damages, restitution, attorneys' fees and costs, and any
12 other relief the Court deems proper as a result of Defendant's CCPA violations.

13 139. Plaintiff, the Nationwide Class and California Class Members seek
14 statutory damages of between \$100 and \$750 per customer per violation or actual
15 damages, whichever is greater, as well as all monetary and non-monetary relief
16 allowed by law, including actual financial losses; injunctive relief; and reasonable
17 attorneys' fees and costs.

18 140. The above constitutes violation of Cal. Civ. Code §1798.150, et. seq.

19 **TENTH CAUSE OF ACTION FOR VIOLATION OF CALIFORNIA**
20 **CONSUMER LEGAL REMEDIES ACT (CAL. CIV. CODE §§ 1750, ET SEQ.)**
21 **(On behalf of Plaintiff, the Nationwide Class and the California Class)**

22 141. The Plaintiff repeats, reiterates and realleges each and every allegation
23 set forth in the preceding paragraphs above as if set forth in full herein.

24 142. Defendant's acts and practices were intended to and did result in the sales
25 of products and services to Plaintiff, the Nationwide Class and California Class
26 Members in violation of Civil Code § 1770, including:

- 27 (a) Representing that goods or services have characteristics that they
28 do not have;

- 1 (b) Representing that goods or services are of a particular standard,
2 quality, or grade when they were not;
- 3 (c) Advertising goods or services with intent not to sell them as
4 advertised; and
- 5 (d) Representing that the subject of a transaction has been supplied in
6 accordance with a previous representation when it has not.

7 141. Defendant's representations and omissions were material because they
8 were likely to deceive reasonable consumers about the adequacy of its data security
9 and ability to protect the confidentiality of consumers' Private Information and other
10 data.

11 142. As a direct and proximate result of Defendant's violation of Cal. Civ.
12 Code §1750, *et seq.*, Plaintiff, the Nationwide Class and California Class Members'
13 Private Information and other data were disclosed to third parties without
14 authorization, causing and will continue to cause Plaintiff, the Nationwide Class and
15 California Class Members damages.

16 143. As a direct and proximate result of Defendant's violation of Cal. Civ.
17 Code §1750, *et seq.*, Plaintiff, the Nationwide Class and California and Class
18 Members have suffered, and continue to suffer, injuries, damages arising from identify
19 theft; from their needing to contact agencies administering benefits; potentially
20 defending themselves from legal action base upon fraudulent applications for benefits
21 made in their name; contacting their financial institutions; loss of use of funds; closing
22 or modifying financial accounts; damages from lost time and effort to mitigate the
23 actual and potential impact of the data breach on their lives; closely reviewing and
24 monitoring their accounts for unauthorized activity which is certainly impending;
25 placing credit freezes and credit alerts with credit reporting agencies; and damages
26 from identify theft, which may take months or years to discover and detect.

1 144. In accordance with Cal. Civ. Code § 1750, on or about June 10, 2022,
2 Plaintiff’s counsel served Defendant with notice of these CLRA violations via First-
3 Class U.S. Mail.

4 145. On behalf of Plaintiff, the Nationwide Class and California Class
5 Members, Plaintiff seeks injunctive relief in the form of an order enjoining Defendant
6 from continuing to violate the CLRA. If Defendant fails to respond to Plaintiff’s
7 notice letter or agree to rectify the violations detailed above, Plaintiff will amend this
8 Complaint and seek actual, punitive, and statutory damages, restitution, attorneys’ fees
9 and costs, and any other relief the Court deems proper as a result of Defendant’s
10 CLRA violations.

11 146. Plaintiff, the Nationwide Class and California Class Members seek all
12 monetary and non-monetary relief allowed by law, including damages, an order
13 enjoining the acts and practices described above, attorneys’ fees, and costs under the
14 CLRA.

15 147. The above constitutes violation of Cal. Civ. Code §1750, *et. seq.*

16 **ELEVENTH CAUSE OF ACTION FOR VIOLATION OF THE CALIFORNIA**
17 **CONFIDENTIALITY OF MEDICAL INFORMATION ACT,**
18 **CAL. CIV. CODE § 56, ET SEQ.**
19 **(On Behalf of Plaintiff, the Nationwide Class and the California Class)**

20 148. The Plaintiff repeats, reiterates and realleges each and every allegation
21 set forth in the preceding paragraphs above as if set forth in full herein.

22 149. The California’s Confidentiality of Medical Information Act (“CMIA”)
23 prohibits, among other things, unauthorized disclosure of private medical information.
24 Cal. Civ. Code §§ 56, *et seq.*

25 150. Plaintiff, the Nationwide Class and California Class Members provided
26 their PHI to Defendant which is a “health care practitioner” is a “provider of health
27 care” as defined by Cal. Civ. Code § 56.05(j).

1 151. Plaintiff, the Nationwide Class and California Class Members are
2 “patients” as defined by Cal. Civ. Code § 56.05(k).

3 152. Illuminate is a “provider of health care” subject to the CMIA because it is
4 a “business that offers software or hardware to consumers, . . . that is designed to
5 maintain medical information” in order to make the information available to an
6 individual or an educational entity to which Plaintiff, the Nationwide Class and
7 California Class Members provided their PHI. Cal. Civ. Code § 56.06(b).

8 153. Illuminate stored in electronic form on its computer system Plaintiff, the
9 Nationwide Class and California Class Members’ “medical information” as defined by
10 Cal. Civ. Code § 56.05(j).

11 154. Illuminate’s systems were designed, in part, to make information
12 available to the educational entities by providing cloud-based computing solutions
13 through which those educational entities could store, access, and manage current and
14 former students’ Private Information including PHI.

15 155. Plaintiff, the Nationwide Class and California Class Members did not
16 provide Illuminate authorization nor was Illuminate otherwise authorized to disclose
17 Plaintiff, the Nationwide Class and California Class Members’ PHI to an unauthorized
18 third-party.

19 156. As described throughout this Complaint, Illuminate negligently
20 maintained, disclosed and released Plaintiff, the Nationwide Class and California
21 Class Members’ PHI inasmuch as it did not implement adequate security protocols to
22 prevent unauthorized access to medical information, maintain an adequate electronic
23 security system to prevent data breaches, or employ industry standard and
24 commercially viable measures to mitigate the risks of any data the risks of any data
25 breach or otherwise comply with HIPAA data security requirements.

26 157. As a direct and proximate result of Illuminate’s negligence, it disclosed
27 and released Plaintiff, the Nationwide Class and California Class Members’ PHI to an
28 unauthorized third-party.

1 158. Illuminate’s unauthorized disclosure of PHI has caused injury to the
2 Plaintiff, the Nationwide Class and California Class Members.

3 159. Upon information and belief, Plaintiff, the Nationwide Class and
4 California Class Members’ PHI was viewed by an unauthorized third party.

5 160. Accordingly, Plaintiff, individually and on behalf of the Nationwide
6 Class and California Class Members seek to recover actual, nominal (including \$1000
7 nominal damages per disclosure under § 56.36(b)), and statutory damages (including
8 under § 56.36(c)) where applicable, together with reasonable attorneys’ fees and costs.

9 **TWELFTH CAUSE OF ACTION FOR VIOLATION OF COLORADO**
10 **SECURITY BREACH NOTIFICATION ACT,**
11 **Colo. Rev. Stat. §§ 6-1-716, et seq.**
12 **(On behalf of Plaintiff and the Colorado Class)**

13 161. The Plaintiff repeats, reiterates and realleges each and every allegation set
14 forth in the preceding paragraphs above as if set forth in full herein.

15 162. Defendant is required to accurately notify Plaintiff and Colorado Class
16 Members if it becomes aware of a breach of its data security system in the most
17 expedient time possible and without unreasonable delay under Colo. Rev. Stat. § 6-1-
18 716(2).

19 163. Because Defendant was aware of a breach of its security system, it had an
20 obligation to disclose the data breach in a timely and accurate fashion as mandated by
21 Colo. Rev. Stat. § 6-1-716(2).

22 164. By failing to disclose the Illuminate Data Breach in a timely and accurate
23 manner, Defendant violated Colo. Rev. Stat. § 6-1-716(2).

24 165. As a direct and proximate result of Defendant’s violation of Colo. Rev.
25 Stat. § 6-1-716(2), Plaintiff and Colorado Class Members’ Private Information and
26 other data were disclosed to third parties without authorization, causing and will
27 continue to cause Plaintiff and Colorado Class Members damages.

1 166. As a direct and proximate result of Defendant's violation of Colo. Rev.
2 Stat. § 6-1-716(2), Plaintiff and Colorado Class Members have suffered, and continue
3 to suffer, injuries, damages arising from identify theft; from their needing to contact
4 agencies administering benefits; potentially defending themselves from legal action
5 base upon fraudulent applications for benefits made in their name; contacting their
6 financial institutions; loss of use of funds; closing or modifying financial accounts;
7 damages from
8 lost time and effort to mitigate the actual and potential impact of the data breach on
9 their lives; closely reviewing and monitoring their accounts for unauthorized activity
10 which is certainly impending; placing credit freezes and credit alerts with credit
11 reporting agencies; and damages from identify theft, which may take months or years
12 to discover and detect.

13 167. Plaintiff and Colorado Class Members seek relief under Colo. Rev. Stat.
14 § 6-1-716(4), including actual damages and equitable relief.

15 168. The above constitutes violation of Colo. Rev. Stat. § 6-1-716(2).

16 **THIRTEENTH CAUSE OF ACTION FOR VIOLATION OF COLORADO**
17 **CONSUMER PROTECTION ACT,**
18 **Colo. Rev. Stat. §§ 6-1-101, et seq.**
19 **(On behalf of Plaintiff and the Colorado Class)**

20 169. The Plaintiff repeats, reiterates and realleges each and every allegation
21 set forth in the preceding paragraphs above as if set forth in full herein.

22 170. Defendant engaged in deceptive trade practices in the course of its
23 business, in violation of Colo. Rev. Stat. § 6-1-105(1), including:

- 24 (a) Making a false representation as to the characteristics of products
25 and services;
- 26 (b) Representing that services are of a particular standard, quality, or
27 grade, though Defendant knew or should have known that there
28 were or another;

- 1 (c) Advertising services with intent not to sell them as advertised;
- 2 (d) Employing “bait and switch” advertising, which is advertising
- 3 accompanied by an effort to sell goods, services, or property other
- 4 than those advertised or on terms other than those advertised; and
- 5 (e) Failing to disclose material information concerning its services
- 6 which was known at the time of an advertisement or sale when the
- 7 failure to disclose the information was intended to induce the
- 8 consumer to enter into the transaction.

9 171. Defendant’s deceptive trade practices include:

- 10 (a) Failing to implement and maintain reasonable security and
- 11 privacy measures to protect Plaintiff and Colorado Class
- 12 Members’ Private Information and other data, which was a
- 13 direct and proximate cause of the Data Breach;
- 14 (b) Failing to identify and remediate foreseeable security and
- 15 privacy risks and adequately improve security and privacy
- 16 measures despite knowing the risk of cybersecurity incidents;
- 17 (c) Failing to comply with common law and statutory duties
- 18 pertaining to the security and privacy of Plaintiff and
- 19 Colorado Class Members’ Private Information and other
- 20 data, including duties imposed by the FTC Act, 15 U.S.C.
- 21 § 45, which was a direct and proximate cause of the Data
- 22 Breach;
- 23 (d) Misrepresenting that they would protect the privacy and
- 24 confidentiality of Plaintiff and Colorado Class Members’
- 25 Private Information and other data, including by
- 26 implementing and maintaining reasonable security measures;
- 27 (e) Misrepresenting that they would comply with common law
- 28 and statutory duties pertaining to the security and privacy of

1 Plaintiff and Colorado Class Members' Private Information
2 and other data, including duties imposed by the FTC Act, 15
3 U.S.C. § 45;

4 (f) Omitting, suppressing, and concealing the material fact that it
5 did not reasonably or adequately secure Plaintiff and
6 Colorado Class Members' Private Information and other
7 data; and

8 (g) Omitting, suppressing, and concealing the material fact that
9 they did not comply with common law and statutory duties
10 pertaining to the security and privacy of Plaintiff and
11 Colorado Class Members' Private Information and other
12 data, including duties imposed by the FTC Act, 15 U.S.C.
13 § 45.

14 172. Defendant's representations and omissions were material because they
15 were likely to deceive reasonable consumers about the adequacy of Illuminate's data
16 security and ability to protect the confidentiality of consumers' Private Information
17 and other data.

18 173. Defendant intended to mislead Plaintiff and Colorado Class Members and
19 induce them to rely upon its misrepresentations and omissions.

20 174. Defendant acted intentionally, knowingly, and maliciously to violate
21 Colorado's Consumer Protection Act, and recklessly disregarded Plaintiff and
22 Colorado Class Members' rights. Defendant was on notice that its security and privacy
23 protections were inadequate.

24 175. Defendant's deceptive trade practices significantly impact the public,
25 because many members of the public are actual or potential users of Defendant's
26 services and the Breach affected millions of students and former students, including
27 members of the Colorado Class.

28

1 176. As a direct and proximate result of Defendant's violation of Colo. Rev.
2 Stat. §§ 6-1-101, *et seq.*, Plaintiff and Colorado Class Members' Private Information
3 and other data were disclosed to third parties without authorization, causing and will
4 continue to cause Plaintiff and Colorado Class Members damages.

5 177. As a direct and proximate result of Defendant's violation of Colo. Rev.
6 Stat. §§ 6-1-101, *et seq.*, Plaintiff and Colorado Class Members have suffered, and
7 continue to suffer, injuries, damages arising from identify theft; from their needing to
8 contact agencies administering benefits; potentially defending themselves from legal
9 action base upon fraudulent applications for benefits made in their name; contacting
10 their financial institutions; loss of use of funds; closing or modifying financial
11 accounts; damages from lost time and effort to mitigate the actual and potential impact
12 of the data breach on their lives; closely reviewing and monitoring their accounts for
13 unauthorized activity which is certainly impending; placing credit freezes and credit
14 alerts with credit reporting agencies; and damages from identify theft, which may take
15 months or years to discover and detect.

16 178. Plaintiff and Colorado Class Members seek all monetary and non-
17 monetary relief allowed by law, including the greater of: (a) actual damages, or (b)
18 \$500, or (c) three times actual damages; injunctive relief; and reasonable attorneys'
19 fees and costs.

20 179. The above constitutes violation of Colo. Rev. Stat. §§ 6-1-101, *et seq.*

21 **FOURTEENTH CAUSE OF ACTION FOR VIOLATION OF CONNECTICUT**
22 **BREACH OF SECURITY REGARDING COMPUTERIZED DATA,**

23 **C.G.S.A. § 36a-701b**

24 **(On behalf of Plaintiff and the Connecticut Class)**

25 180. The Plaintiff repeats, reiterates and realleges each and every allegation
26 set forth in the preceding paragraphs above as if set forth in full herein.

27 181. Defendant is required to accurately notify Plaintiff and Connecticut Class
28 Members if it becomes aware of a breach of its data security program in the most

1 expedient time possible and without unreasonable delay, not to exceed ninety days
2 after discovery of the breach under C.G.S.A. § 36a-701b(b).

3 182. Defendant is required to immediately notify Plaintiff and Connecticut
4 Class Members if it becomes aware of a breach of its data security program which
5 may have compromised personal information it stores, but which Plaintiff and
6 Connecticut Class Members own, under C.G.S.A. § 36a-701b(c).

7 183. Because Defendant was aware of a breach of its security system, it had an
8 obligation to disclose the data breach in a timely and accurate fashion as mandated by
9 C.G.S.A. §§ 36a-701b(b) and (c).

10 184. By failing to disclose the Data Breach in an accurate and timely manner,
11 Defendant failed to comply with C.G.S.A. §§ 36a-701b(b) and (c). Pursuant to
12 C.G.S.A. § 36a-701b(g), Defendant's failure to comply was an unfair trade practice
13 under the Connecticut Unfair Trade Practices Act, C.G.S.A. §§ 42-110a, *et seq.*

14 185. As a direct and proximate result of Defendant's violation of C.G.S.A. §
15 36a-701b(b), Plaintiff and Connecticut Class Members have suffered, and continue to
16 suffer, injuries, damages arising from identify theft; from their needing to contact
17 agencies administering benefits; potentially defending themselves from legal action
18 base upon fraudulent applications for benefits made in their name; contacting their
19 financial institutions; loss of use of funds; closing or modifying financial accounts;
20 damages from lost time and effort to mitigate the actual and potential impact of the
21 data breach on their lives; closely reviewing and monitoring their accounts for
22 unauthorized activity which is certainly impending; placing credit freezes and credit
23 alerts with credit reporting agencies; and damages from identify theft, which may take
24 months or years to discover and detect.

25 186. Plaintiff and Connecticut Class Members seek all monetary and non-
26 monetary relief allowed by law, including actual damages, punitive damages,
27 disgorgement of profits, reasonable costs, and attorney's fees.
28

1 187. In compliance with Connecticut General Statutes § 42-110g(c), a copy of
2 this Complaint is being contemporaneously mailed to the Attorney General of the
3 State of Connecticut and the Commissioner of Consumer Protection.

4 188. The above constitutes violation of C.G.S.A. § 36a-701b(b).

5 **FIFTEENTH CAUSE OF ACTION FOR VIOLATION OF NEW YORK**
6 **GENERAL BUSINESS LAW §349**
7 **(On behalf of Plaintiff and the New York Class)**

8 189. The Plaintiff repeats, reiterates and realleges each and every allegation
9 set forth in the preceding paragraphs above as if set forth in full herein.

10 190. Defendant engaged in deceptive, unfair, and unlawful trade acts or
11 practices in the conduct of trade or commerce and furnishing of services, in violation
12 of N.Y. Gen. Bus. Law § 349(a), including but not limited to the following:

- 13 (a) Defendant misrepresented material facts to Plaintiff and Class
14 Members by representing that they would maintain adequate data
15 privacy and security practices and procedures to safeguard Plaintiff
16 and New York Class members' Private Information and other data
17 from unauthorized disclosure, release, data breaches, and theft;
- 18 (b) Defendant misrepresented material facts to Plaintiff and New York
19 Class Members by representing that they did and would comply
20 with the requirements of federal and state laws pertaining to the
21 privacy and security of Plaintiff and New York Class Members'
22 Private Information and other data;
- 23 (c) Defendant omitted, suppressed, and concealed material facts of the
24 inadequacy of its privacy and security protections for Plaintiff and
25 New York Class Members' Private Information and other data;
- 26 (d) Defendant engaged in deceptive, unfair, and unlawful trade acts or
27 practices by failing to maintain the privacy and security of Plaintiff
28 and New York Class members' Private Information and other data,

1 in violation of duties imposed by and public policies reflected in
2 applicable federal and state laws, resulting in the Data Breach.

3 These unfair acts and practices violated duties imposed by laws
4 including the Federal Trade Commission Act (15 U.S.C. § 45);

5 (e) Defendant engaged in deceptive, unfair, and unlawful trade acts or
6 practices by failing to disclose the Data Breach to the Class in a
7 timely and accurate manner, contrary to the duties imposed by
8 N.Y. Gen. Bus. Law §§ 899-aa(2) and 899-bb (SHIELD Act).

9 191. Defendant's failure constitutes false and misleading representations,
10 which have the capacity, tendency, and effect of deceiving or misleading consumers
11 (including Plaintiff and New York Class Members) regarding the security of its
12 network and aggregation of Private Information and other data.

13 192. The misrepresentations upon which consumers (including Plaintiff and
14 New York Class Members) relied were material misrepresentations (e.g., as to
15 Defendant's adequate protection of Private Information and other data), and
16 consumers (including Plaintiff and New York Class Members) relied on those
17 representations to their detriment.

18 193. Defendant's conduct is unconscionable, deceptive, and unfair, as it is
19 likely to, and did, mislead consumers acting reasonably under the circumstances. As a
20 direct and proximate result of Defendant's conduct, Plaintiff and New York Class
21 Members have been harmed, in that they were not timely notified of the Data Breach,
22 which resulted in profound vulnerability of their Private Information and other data.

23 194. As a direct and proximate result of Defendant's unconscionable, unfair,
24 and deceptive acts and omissions, Plaintiff and New York Class Members' Private
25 Information and other data were disclosed to third parties without authorization,
26 causing and will continue to cause Plaintiff and New York Class Members damages.

27 195. As a direct and proximate result of Defendant's violation of NY GBL
28 §349, Plaintiff and New York Class Members have suffered, and continue to suffer,

1 injuries, damages arising from identify theft; from their needing to contact agencies
2 administering unemployment benefits; potentially defending themselves from legal
3 action base upon fraudulent applications for unemployment benefits made in their
4 name; contacting their financial institutions; loss of use of funds; closing or modifying
5 financial accounts; damages from lost time and effort to mitigate the actual and
6 potential impact of the data breach on their lives; closely reviewing and monitoring
7 their accounts for unauthorized activity which is certainly impending; placing credit
8 freezes and credit alerts with credit reporting agencies; and damages from identify
9 theft, which may take months or years to discover and detect.

10 196. Plaintiff and New York Class Members seek all monetary and non-
11 monetary relief allowed by law, injunctive relief, and reasonable attorneys' fees and
12 costs.

13 197. The above constitutes violation of NY GBL §349.

14 **SIXTEENTH CAUSE OF ACTION FOR VIOLATION**
15 **OF NEW YORK EDUCATION LAW §2-d**
16 **(On behalf of Plaintiff and the New York Class)**

17 198. The Plaintiff repeats, reiterates and realleges each and every allegation
18 set forth in the preceding paragraphs above as if set forth in full herein.

19 199. New York Education Law §2-d(5)(f) provides that:

20 (a) Each third party contractor that enters into a contract or other
21 written agreement with an educational agency under which
22 the third party contractor will receive student data or teacher
23 or principal data shall:

24 (i) limit internal access to education records to those
25 individuals that are determined to have legitimate
26 educational interests; not use the education records for any
27 other purposes than those explicitly authorized in its
28 contract;

- 1 (b) except for authorized representatives of the third party
2 contractor to the extent they are carrying out the contract, not
3 disclose any personally identifiable information to any other
4 party:
5 (i) without the prior written consent of the parent or eligible
6 student; or
7 (ii) unless required by statute or court order and the party
8 provides a notice of the disclosure to the department, district
9 board of education, or institution that provided the
10 information no later than the time the information is
11 disclosed, unless providing notice of the disclosure is
12 expressly prohibited by the statute or court order;
- 13 (c) maintain reasonable administrative, technical and physical
14 safeguards to protect the security, confidentiality and
15 integrity of personally identifiable student information in its
16 custody;
- 17 (d) uses encryption technology to protect data while in motion or
18 in its custody from unauthorized disclosure using a
19 technology or methodology specified by the secretary of the
20 United States department of health and human services in
21 guidance issued under Section 13402(H)(2) of Public Law
22 111-5.

23 200. New York Education Law §2-d(6)(a) provides that, in the case of the
24 breach and unauthorized release of Private Information:

- 25 (a) Each third party contractor that receives student data or teacher or
26 principal data pursuant to a contract or other written agreement
27 with an educational agency shall be required to notify such
28 educational agency of any breach of security resulting in an

1 unauthorized release of such data by the third party contractor or
2 its assignees in violation of applicable state or federal law, the
3 parents bill of rights for student data privacy and contractual
4 obligations relating to data privacy and security, *in the most*
5 *expedient way possible and without unreasonable delay* [emphasis
6 added].

7 201. New York Education Law §2-d(6)(a) provides that, in the case of the
8 breach and unauthorized release of Private Information:

9 (a) In the case of an unauthorized release of student data,
10 the educational agency shall notify the parent or
11 eligible student of the unauthorized release of student
12 data that includes personally identifiable information
13 from the student records of such student *in the most*
14 *expedient way possible and without unreasonable*
15 *delay* [emphasis added].

16 202. Defendant has violated New York Education Law §2-d by virtue of its
17 inordinate and unreasonable delay in notifying school districts and parents of Plaintiff
18 and New York Class members of its Data Breach, of which it was fully aware.

19 203. As a direct and proximate result of Defendant's violation of NY GBL
20 §349, Plaintiff and New York Class Members have suffered, and continue to suffer,
21 injuries, damages arising from identify theft; from their needing to contact agencies
22 administering unemployment benefits; potentially defending themselves from legal
23 action base upon fraudulent applications for unemployment benefits made in their
24 name; contacting their financial institutions; loss of use of funds; closing or modifying
25 financial accounts; damages from lost time and effort to mitigate the actual and
26 potential impact of the data breach on their lives; closely reviewing and monitoring
27 their accounts for unauthorized activity which is certainly impending; placing credit
28

1 freezes and credit alerts with credit reporting agencies; and damages from identify
2 theft, which may take months or years to discover and detect.

3 204. Plaintiff and New York Class Members seek all monetary and non-
4 monetary relief allowed by law, injunctive relief, and reasonable attorneys' fees and
5 costs.

6 205. The above constitutes violation of NY Education Law §2-d.

7
8 **SEVENTEENTH CAUSE OF ACTION FOR VIOLATION OF OKLAHOMA**
9 **CONSUMER PROTECTION ACT,**
10 **Okla. Stat. Tit. 15, §§ 751, et seq.**
11 **(On behalf of Plaintiff and the Oklahoma Class)**

12 206. The Plaintiff repeats, reiterates and realleges each and every allegation
13 set forth in the preceding paragraphs above as if set forth in full herein.

14 207. Defendant, in the course of its business, engaged in unlawful practices in
15 violation of Okla. Stat. tit. 15, § 753, including the following:

- 16 (a) Making false or misleading representations, knowingly or with
17 reason to know, as to the characteristics, uses, and benefits of the
18 subjects of its consumer transactions;
19 (b) Representing, knowingly or with reason to know, that the subjects
20 of its consumer transactions were of a particular standard when
21 they were of another;
22 (c) Advertising, knowingly or with reason to know, the subjects of its
23 consumer transactions with intent not to sell as advertised;
24 (d) Committing deceptive trade practices that deceived or could
25 reasonably be expected to deceive or mislead a person to the
26 detriment of that person as defined by section 752(13);
27 (e) Committing unfair trade practices that offend established public
28 policy and was immoral, unethical, oppressive, unscrupulous, and
substantially injurious to consumers as defined by section 752(14).

1 208. Defendant’s unlawful practices include:

- 2 (a) Failing to implement and maintain reasonable security and privacy
3 measures to protect Plaintiff and Oklahoma Class Members’
4 Private Information and other data, which was a direct and
5 proximate cause of the Data Breach;
- 6 (b) Failing to identify and remediate foreseeable security and privacy
7 risks and adequately improve security and privacy measures
8 despite knowing the risk of cybersecurity incidents, which was a
9 direct and proximate cause of the Data Breach;
- 10 (c) Failing to comply with common law and statutory duties pertaining
11 to the security and privacy of Plaintiff and Oklahoma Class
12 Members’ Private Information and other data, including duties
13 imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and
14 proximate cause of the Data Breach;
- 15 (d) Misrepresenting that they would protect the privacy and
16 confidentiality of Plaintiff and Oklahoma Class Members’ Private
17 Information and other data, including by implementing and
18 maintaining reasonable security measures;
- 19 (e) Misrepresenting that they would comply with common law and
20 statutory duties pertaining to the security and privacy of Plaintiff
21 and Oklahoma Class Members’ Private Information and other
22 data, including duties imposed by the FTC Act, 15 U.S.C. § 45;
- 23 (f) Omitting, suppressing, and concealing the material fact that it did
24 not reasonably or adequately secure Plaintiff and Oklahoma Class
25 Members’ Private Information and other data; and
- 26 (g) Omitting, suppressing, and concealing the material fact that they
27 did not comply with common law and statutory duties pertaining to
28 the security and privacy of Plaintiff and Oklahoma Class

1 Members' Private Information, including duties imposed by the
2 FTC Act, 15 U.S.C. §

3 209. Defendant's representations and omissions were material because they
4 were likely to deceive reasonable consumers about the adequacy of Illuminate's data
5 security and ability to protect the confidentiality of consumers' Private Information
6 and other data.

7 210. Defendant intended to mislead Plaintiff and Oklahoma Class Members
8 and induce them to rely on its misrepresentations and omissions.

9 211. As a direct and proximate result of Defendant's violation of the
10 Oklahoma Consumer Protection Act, Plaintiff and Oklahoma Class Members have
11 suffered, and continue to suffer, injuries, damages arising from identify theft; from
12 their needing to contact agencies administering unemployment benefits; potentially
13 defending themselves from legal action base upon fraudulent applications for
14 unemployment benefits made in their name; contacting their financial institutions; loss
15 of use of funds; closing or modifying financial accounts; damages from lost time and
16 effort to mitigate the actual and potential impact of the data breach on their lives;
17 closely reviewing and monitoring their accounts for unauthorized activity which is
18 certainly impending; placing credit freezes and credit alerts with credit reporting
19 agencies; and damages from identify theft, which may take months or years to
20 discover and detect.

21 212. Plaintiff and Oklahoma Class Members seek all monetary and non-
22 monetary relief allowed by law, injunctive relief, and reasonable attorneys' fees and
23 costs.

24 The above constitutes violation of Okla. Stat. tit. 15, § 753.

25 **PRAYER FOR RELIEF**

26 WHEREFORE, Plaintiff, individually and on behalf of the members of the
27 Classes defined above, respectfully request that this Court:
28

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

- A. Certify this case as a class action under Federal Rule of Civil Procedure 23, appoint Plaintiff as the Class representatives, and appoint the undersigned as Class counsel;
- B. Order appropriate relief to Plaintiff and the Classes; Enter injunctive and declaratory relief as appropriate under the applicable law;
- C. Award Plaintiff and the Classes pre-judgment and/or post-judgment interest as prescribed by law;
- D. Award reasonable attorneys’ fees and costs as permitted by law; and
- E. Enter such other and further relief as may be just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands a trial by jury of all claims so triable.

DATED: June 14, 2022

Respectfully submitted,

GREEN & NOBLIN, P.C.

By: /s/ Robert S. Green
Robert S. Green

James Robert Noblin
Emrah M. Sumer
2200 Larkspur Landing Circle, Ste. 101
Larkspur, CA 94939
Telephone: (415) 477-6700
Facsimile: (415) 477-6710

Counsel for Plaintiff and the Proposed
Class