United States District Court
Eastern District of New York

Sarah Chung, individually and on behalf of all others similarly situated, Plaintiff, - against - Illuminate Education, Inc., Defendant.	No.: 1:22-cv-3110 Class Action Complaint

Plaintiff Sarah Chung ("Plaintiff") alleges upon information and belief, except for allegations pertaining to Plaintiff, which are based on personal knowledge:

1. Illuminate Education, Inc. ("Defendant" or "Illuminate") failed to secure and safeguard personally identifiable information ("PII" or "Private Information") it collected, maintained, and stored in its Pupilpath online and app platform.

2. Defendant failed to timely and adequately notify Plaintiff that her information had been subject to unauthorized access by an unknown third party and inform her what specific type of information was accessed (the "Data Breach").

3. Due to Defendant's negligence, the PII that it collected and maintained is now an open book in the hands of unknown crooks.

4. Reports indicate that if a company takes reasonable, industry-standard steps and follows "best practices" associated with hiring and retention of personnel and contractors, either this data breach incident would not have occurred or it would not have lasted as long as it did, and the harm to Plaintiff would have been mitigated.

5. It is expected that the private information obtained on Plaintiff is now for sale on the "dark web" and will be utilized for nefarious and mischievous ends, which will harm Plaintiff.

Jurisdiction and Venue

6. Jurisdiction is in this Court pursuant to 28 U.S.C. §1332(d)(2) because the parties are citizens of different states, the aggregate amount in controversy, exclusive of interests and costs, exceeds $5 million, and there are greater than 100 members of the proposed class.

7. This Court has personal jurisdiction over Defendant because it is authorized to do business in this District and regularly conduct business in this District, and has sufficient minimum contacts with this state, through its promotion, sales, licensing and marketing within this state.

8. Venue is proper because Plaintiff and many Class members reside in this District and Defendant does business in this District and State.

9. A substantial part of the events and omissions giving rise to the claims occurred in this District.

Parties

10. Defendant Illuminate Education, Inc., is a California corporation with a principal place of business in Irvine, California.

11. Defendant provides educational software applications and technology support to schools.

12. Schools use Illuminate's software to store year-end assessment test results and final grades from kindergarten through 12th grade, track assignments and in-class exam grades, communicate with students and families with assigned email address, track student attendance and help with other administrative work.

13. On information and belief, Defendant also stored students' photographs, physical attributes such as height and weight and physical performance levels, such as the ability to do number of sit-ups, push-ups and squats.

14. Plaintiff Sarah Chung is a resident of Queens County, New York, and a student in geographic district 28 in Queens County.

15. Plaintiff's PII was believed to have been stolen in connection with the Data Breach.

16. Plaintiff suffered harm as a result of the Data Breach, including, but not limited to, (i) the theft of her PII; (ii) the time and costs associated with dealing with the Data Breach, such as the prevention of future identity theft and the inconvenience, nuisance, and annoyance of dealing with all other issues resulting from the Data Breach; (iii) the imminent heightened risk of identity theft; (iii) invasion of her privacy; and (iv) damage to the PII that Defendant failed to safeguard.

Allegations

17. The Data Breach occurred as a result of Defendant's failure to secure and protect Plaintiff's PII.

18. Defendant's Pupilpath platform is licensed to 5,000 schools nationally with total enrollment of about 17 million students.

19. Plaintiff and Class members utilizing the Pupilpath system, as required by their schools' curricula, were required to provide Defendant with valuable and sensitive PII, including their facial photographs, first and last names, dates of birth, email addresses, and unique identification numbers.

20. Plaintiff and Class members relied on Defendants to keep their PII confidential and secure, to be used solely for educational purposes, and to protect against unauthorized disclosure of the PII.

21. On January 8, 2022, Illuminate became aware of suspicious activity in applications within their programs and launched an investigation.

22. On March 24, 2022, the investigation revealed that unauthorized access to certain

databases, containing protected student information had taken place between December 28, 2021, and January 8, 2022.

23. The Illuminate Data Breach is known to have impacted nearly two million students in five states.

24. In NY state alone, 820,000 current students in 567 schools are known to be impacted by the breach. The number of former students impacted are estimated to be many folds higher than the number of current students.

25. For weeks after the cyberattack took place, Illuminate failed to notify New York City schools that personal information had been compromised back in January.

26. Finally, on or about March 25, 2022, Defendant notified the NYC Department of Education ("DOE") that its system had been breached.

27. The DOE notified the police department and other law enforcement agencies although the FBI was already involved in the investigation.

28. Defendant's delayed reaction violates the New York's Education Law §2-d, strengthened to protect student data privacy in 2019, which requires that affected schools must be notified of any data breach "without unreasonable delay but no more than seven calendar days from the date of discovery of such breach."

29. The school, in turn, must notify affected individuals without unreasonable delay but in no case no more than 14 calendar days from the date of discovery.

30. Defendant has yet to directly inform the students and their parents that the PII has been compromised.

31. Instead, current students, former students and some parents in New York City, received letters dated May 19, 2022, from the DOE that a data security incident took place.

32. The investigation revealed that Defendant's failure to encrypt student data may have been a contributing factor in theft of the unauthorized information.

33. According to sources, Illuminate had told the DOE that it was meeting the legal requirements for data protection including data encryption.

34. Defendant failed to appreciate the gravity of the data breach which heightened the risk that additional damage might follow the Data Breach.

35. Defendant negligently and unlawfully failed to safeguard students' PII and failed to timely notify them and any guardians when it was compromised.

36. Accordingly, students now face an increased risk of fraud, identity theft, tracking, or other adverse effects.

37. According to Doug Levin, a national director at K12 Security Information Exchange, the identity information of a younger person is worth more than an established adult.

38. Levin stated that a younger person's identity information can be abused, and their credit record can be hijacked for five to ten years before anyone figures out the identity has been compromised, whereas an adult will figure it out usually within a month or two.

39. Now, current and former students, parents and guardians must spend years living in fear that unscrupulous actors may utilize their ill-gotten information.

40. As a direct and proximate result of Defendant's conduct, Plaintiff and Class members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud, identity theft, tracking and other adverse effects.

41. Plaintiff and Class members have an interest in ensuring that their PII, which is believed to remain in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that

the storage of data or documents containing personal and financial information is not accessible online and that access to such data is password-protected.

42. As a result of Defendant's misconduct, the Data Breach has potentially made Plaintiff's and Class members' PII available to criminals for misuse.

43. The Data Breach directly resulted in injuries such as theft of personal information, costs of identity theft detection and further protection, costs to mitigate the future consequences of the Data Breach, including but not limited to, time taken from life, extra trips to places like banks to resolve issues, loss of enjoyment, inconvenience, nuisance, annoyance, impending injury resulting from fraud and identify theft due to PII for sale on the dark web and loss of privacy.

44. As a result of Defendant's conduct, Plaintiff and Class members are forced to live with the anxiety that their private information, including their academic records, are disclosed to the entire world depriving them of the right to privacy.

Class Allegations

45. Plaintiff seeks to represent a class of New York persons pursuant to Fed. R. Civ. P. 23, who used the Products or Services of Defendant during the statutes of limitation.

46. Common questions of law or fact predominate and include whether Plaintiff's and class members' personal information was compromised, causing them harm, and if Defendant took reasonable measures to prevent or mitigate the harm, and whether Plaintiff and Class members are entitled to damages.

47. Plaintiff's claims and the basis for relief are typical to other Class members because all were subjected to the same representations.

48. Plaintiff is an adequate representative because her interests do not conflict with other Class members.

49. No individual inquiry is necessary since the focus is only on Defendant's practices and the Class is definable and ascertainable.

50. Individual actions would risk inconsistent results, be repetitive and are impractical to justify, as the claims are modest.

51. Plaintiff's counsel is competent and experienced in complex class action litigation and intends to adequately and fairly protect Class members' interests.

CAUSES OF ACTION

New York General Business Law ("GBL") §§ 349 & 350

52. Plaintiff repeats and re-alleges each and every factual allegation contained in all previous paragraphs as if fully set forth herein.

53. New York General Business Law ("GBL") §§ 349 & 350 *et seq*., prohibits the use of unfair or deceptive business practices in the conduct of trade or commerce.

54. Defendant's acts, practices, representations and omissions related to their adherence to data protection practices that purportedly would safeguard the information of Plaintiff and class members are not unique to the parties and have a broader impact on the public.

55. Plaintiff was directed by Defendant to entrust it with their PII and assured it would not be disclosed to unauthorized persons and that best practices would be employed to prevent or mitigate such disclosure.

56. The representations and omissions were relied on by Plaintiff, causing damages.

57. As a result, Plaintiff and class members seek all monetary and non-monetary relief allowed by law, including injunctive relief and reasonable attorneys' fees.

Breach of Contract

58. Plaintiff entered into contracts with Defendant that included its promise to protect

non-public personal information given to it or that it gathered on its own, from disclosure.

59. Plaintiff performed her obligations under the contract when she engaged and used the Pupilpath platform.

60. Defendant breached the contractual obligation to protect her non-public personal information when the information was accessed as part of the Data Breach.

61. As a direct and proximate result of the breach, Plaintiff has been harmed and suffered, and will continue to suffer, damages and injuries.

Negligence and Negligence Per Se

62. Defendant violated N.Y. Gen. Bus. Law § 899-aa and similar laws of the other states, which is based upon the safeguarding certain confidential data.

63. Plaintiff and class members are within the class of persons that these laws were intended to protect because they are residents of these states.

64. The harm which occurred due to Defendant's Data Breach is the type of harm that these laws were intended to protect.

65. Specifically, this is the harm of the unauthorized access or disclosure of personal information due to a failure to maintain reasonable security procedures.

66. Defendant had a duty of reasonable care to safeguard the privacy, confidentiality, and security of Plaintiff's personal information and documents and comply with the terms of its own privacy and security policy.

67. Defendant had, and continues to have, a duty to timely disclose that Plaintiff and Class members' Private Information within their possession was compromised and disclose precisely the type(s) of information that were compromised.

68. Defendant breached this duty of care by failing to adequately safeguard the private

and confidential personal information and records of Plaintiff and Class members.

69. Defendant unlawfully breached its duty to timely disclose to Plaintiff and Class members that the Private Information within Defendant's possession might have been compromised and precisely the type of information compromised.

70. As a result of Defendant's ongoing failure to notify Plaintiff and Class members regarding specifically what type of Private Information has been compromised, Plaintiff and Class members are unable to take the necessary precautions to mitigate damages to prevent future fraud.

71. Defendant's breaches of duty caused Plaintiff and Class members to suffer from identity theft, loss of time and money to monitor their finances for fraud, and loss of control over their Private Information.

72. As a result of Defendant's negligence and breach of duties, Plaintiff and Class members are in danger of imminent harm in that their PII, which is still in the possession of third parties, will be used for fraudulent purposes.

73. As a direct and proximate result of Defendant's breach of their duty of care, Plaintiff and the Class suffered injury.

Unjust Enrichment

74. Plaintiff incorporates by references all preceding paragraphs.

75. Defendant obtained benefits and monies because the Services or Products were not as represented and expected, they were not accompanied by adequate, industry-standard security protocols, to the detriment and impoverishment of Plaintiff and Class members, who seek restitution and disgorgement of inequitably obtained profits.

Jury Demand and Prayer for Relief

Plaintiff demands a jury trial on all issues.

WHEREFORE, Plaintiffs prays for judgment:

1. Declaring this a proper class action, certifying Plaintiff as representatives and the undersigned as counsel for the class;
2. Entering preliminary and permanent injunctive relief by directing Defendant to correct the challenged practices to comply with the law;
3. Injunctive relief to remove and/or refrain from the challenged representations, restitution and disgorgement for members of the State Subclasses pursuant to the consumer protection laws of their States;
4. Awarding monetary damages and interest, including treble and punitive damages, pursuant to the common law and consumer protection law claims, and other statutory claims;
5. Awarding costs and expenses, including reasonable fees for Plaintiff's attorneys and experts; and
6. Other and further relief as the Court deems just and proper.

Dated: May 26, 2022

Respectfully submitted,

Sheehan & Associates, P.C.
/s/Spencer Sheehan
Spencer Sheehan
60 Cuttermill Road, Suite 412
Great Neck, NY 11021
(516) 268-7080
spencer@spencersheehan.com

Law Office of James Chung
James Chung
43-22 216th Street
Bayside, NY 11361
(718) 461-8808
Jchung_77@msn.com