IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

KYLIE S., ANTHONY P., ANNA S., and GENA W., on behalf of themselves and as parents and guardians of their minor children, K.S., J.P., K.P., D.C., M.C., J.C., Z.W., and C.W., and on behalf of all similarly-situated individuals,	)	
Plaintiffs,	)	
v.	)	**19 C 5936**
PEARSON PLC, NCS PEARSON, INC, and PEARSON EDUCATION, INC., d/b/a PEARSON CLINICAL ASSESSMENT,	)	**Judge John Z. Lee**
Defendants.	)	

MEMORANDUM OPINION AND ORDER

Pearson PLC, NCS Pearson, Inc., and Pearson Education, Inc. (collectively "Pearson") operate AIMSweb, an educational testing platform that stores students' names, emails, and birthdays, among other information. In 2018, hackers slipped past Pearson's defenses and gained access to the data hosted on AIMSweb. No credit cards, social security numbers, health records, or other sensitive information was compromised, and none of the affected students have reported fraudulent charges or other fallout attributable to the data breach.

Believing that Pearson neglected to implement security measures that would have thwarted the hackers, a group of Illinois and Colorado parents initiated this putative class action. At this stage, Pearson has moved to dismiss the complaint. Because Plaintiffs have not established Article III standing, the motion is granted.

I. Background[1]

A. The AIMSweb Platform

Pearson PLC publishes educational materials. Am. Compl. ¶ 13, ECF No. 11. Pearson Education, Inc., one of Pearson PLC's subsidiaries, supplies testing services. *Id.* ¶ 14. NCS Pearson, Inc., another subsidiary, develops educational software. *Id.* ¶ 15.

Working together, these entities oversee AIMSweb, a "digital education technology assessment platform licensed to schools and school districts." *Id.* ¶ 35. As part of the curriculum, schools that license the platform instruct their students to complete tests on AIMSweb. *Id.* ¶ 36. To do so, students must share "their first and last names, dates of birth, email addresses, unique student identification numbers, home addresses and telephone numbers." *Id.* ¶ 38. In a privacy policy that covers AIMSweb, Pearson accepted "full responsibility for the information we hold" and promised to "protect [student] privacy at all times." *Id.* ¶ 58.

B. The Data Breach

Sometime in late 2018, hackers penetrated AIMSweb's defenses and gained access to the data stored on the platform. Am. Compl. ¶ 1. But it was not until early 2019, when the FBI detected the incident, that Pearson realized that AIMSweb had been compromised. *Id.* ¶ 41.

---

[1] In analyzing a motion to dismiss, the court "accept[s] as true all well-pleaded factual allegations and draw[s] all reasonable inferences in favor of the plaintiff." *Heredia v. Capital Mgmt. Servs., L.P.*, 942 F.3d 811, 814 (7th Cir. 2019).

In a preliminary analysis, the FBI estimated that the intruders could have accessed information related to roughly 900,000 students at about 13,000 schools. *Id.* The disclosed data included "first name, last name, and in some instances . . . date of birth and/or email address," along with students' "unique student identification numbers." *Id.* ¶ 47.

About four months after the FBI discovered the problem, Pearson issued a public notice acknowledging that a data breach had occurred. *Id.* ¶¶ 43, 46. Pearson assured customers that it "do[es] "not have any evidence that th[e] information has been misused." *Id.* ¶ 48. "[A]s a precaution," however, it "offer[ed] to compensate victims in the form of one year of complimentary credit monitoring services." *Id.* ¶¶ 48–49.

C. Plaintiffs' Claims

Based on Pearson's failure to prevent the data breach, Plaintiffs assert a dozen different common law and statutory claims. They accuse Pearson of common law negligence, negligence per se, breach of an express contract, breach of an implied contract, unjust enrichment, and intrusion upon seclusion. They also allege that Pearson violated the Illinois Personal Information and Protection Act, 815 Ill. Comp. Stat. § 530/1 *et seq.*; Illinois Consumer Fraud and Deceptive Business Practices Act, 815 Ill. Comp. Stat. § 505/1, *et seq.*; Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/1, *et seq.*; Colorado Security Breach Notification Act, Colo. Rev. Stat. §§ 6-1-716, *et seq.*; Colorado Consumer Protection

Act, Colo. Rev. Stat. §§ 6-1-101, *et seq.*; and Colorado Student Data Transparency and Security Act, Colo. Rev. Stat. §§ 22-16-101, *et seq.*

For its part, Pearson maintains that the complaint should be dismissed for lack of subject-matter jurisdiction, want of personal jurisdiction, and failure to state a claim. The Court's analysis begins—and, in this case, ends—with the question of subject-matter jurisdiction.

II. Legal Standard

Under Federal Rule of Civil Procedure 12(b)(1), a defendant may move to dismiss claims over which a federal court lacks subject-matter jurisdiction. *See Apex Digital, Inc. v. Sears, Roebuck & Co.*, 572 F.3d 440, 443 (7th Cir. 2009); *Perry v. Vill. of Arlington Heights*, 186 F.3d 826, 829 (7th Cir. 1999). In analyzing a Rule 12(b)(1) motion, courts accept as true all well-pleaded facts, draw all reasonable inferences in the plaintiff's favor, and look beyond the jurisdictional allegations to evidence submitted on the issue of subject-matter jurisdiction. *See St. John's United Church of Christ v. City of Chi.*, 502 F.3d 616, 625 (7th Cir. 2007).

III. Analysis

Pearson contends that Plaintiffs lack standing to bring this suit. It is well-established that "[s]tanding is an essential component of Article III's case-or-controversy requirement." *Apex Digital, Inv. v. Sears, Roebuck & Co.*, 572 F.3d 440, 443 (7th Cir. 2009).

To support standing, a claimant must allege: "(1) an injury in fact, (2) that is fairly traceable to the challenged conduct of the defendant, and (3) that is likely to

be redressed by a favorable judicial decision." *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1547 (2016). "[A] plaintiff, as the party invoking federal jurisdiction, bears the burden of establishing these elements." *Id.* (citation omitted). At issue here is whether Plaintiffs have adequately pleaded an injury-in-fact.

An injury-in-fact refers to a particularized and concrete, actual or imminent invasion of a legally-protected interest. *See Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560 (1992). "For an injury to be 'particularized,' it 'must affect the plaintiff in a personal and individual way.'" *Spokeo*, 136 S Ct. at 1548 (citation omitted). For an injury to be "concrete," it must "actually exist." *Id.* "This does not mean, however, that [a] risk of real harm cannot satisfy the requirement of concreteness." *Id.* at 1549. So long as the plaintiff faces "a substantial risk" of injury, the concreteness component is present. *Hummel v. St. Joseph Cty. Bd. of Comm'rs*, 817 F.3d 1010, 1019–20 (7th Cir. 2016) (citation omitted).

In arguing that they suffered an injury-in-fact, Plaintiffs articulate three distinct theories. First, they submit that the data breach exacerbated their vulnerability to identity theft. Second, they suggest that the breach reduced the market value of their data. Finally, they contend that certain statutes dictate that any disclosure of student records is a legally-cognizable injury, even if no economic harm results.

A. Increased Risk of Identity Theft

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.