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

Plaintiffs' primary argument is that the data breach made them easier targets for identity thieves. In *Remijas v. Neiman Marcus Group, LLC*, the Seventh Circuit recognized that a substantial risk of identity theft qualifies as an injury-in-fact. 794 F.3d 688 (7th Cir. 2015). There, "hackers deliberately targeted Neiman Marcus in order to obtain [shoppers'] credit card information." *Id*. at 693. All told, the attackers absconded with about 300,000 credit and debit card numbers. *Id*. at 690. They promptly placed fraudulent charges on 9,000 of the stolen cards. *Id*. Under those conditions, the Court of Appeals held that all of the shoppers had pleaded an injury-in-fact sufficient to survive a Rule 12(b)(1) motion. *Id*. at 693.

Whether a data breach exposes consumers to a material threat of identity theft turns on two factors that derive from *Remijas*: (1) the sensitivity of the data in question, see, e.g., *In re Vtech Data Breach Litig.*, No. 15 C 10889, 2017 WL 2880102, at *4 (N.D. Ill. July 5, 2017), and (2) the incidence of "fraudulent charges" and other symptoms of identity theft, see *Lewert v. P.F. Chang's China Bistro, Inc.*, 819 F.3d 963, 967 (7th Cir. 2016).[2]

Particularly relevant here, *Vtech* applied these factors to a breach that exposed children's data. In that case, a toy company disclosed millions of "children's names, genders, birthdates" along with their parents' "email and mailing addresses,

[2] At times, Plaintiffs seem to suggest that any data breach, no matter the sensitivity of the stolen information or the incidence of identity theft, satisfies Article III. But courts in this circuit have repeatedly refused to recognize standing when hackers gained access to low-risk information. *See, e.g.*, *Vtech*, 2017 WL 2880102, at *4 ("Plaintiffs have not shown an increased risk of identity theft due to a data breach because they do no allege how the stolen data would aid identity thieves[.]"); *Unchageri v. Carefirst of Maryland, Inc.*, No. 16 C 1068, 2016 WL 8255013, at *3 (C.D. Ill. Nov. 14, 2016) (same).

IP addresses, download and purchase histories" and other account information. *Vtech*, 2017 WL 2880102, at *2. Distinguishing *Remijas*, the court reasoned that "the data stolen here did not include credit-card or debit-card information, or any other information that could easily be used in fraudulent transactions." *Id.* at *3–4. At the same time, the court also found it significant that the breach had not "resulted in fraudulent charges" or any other "fallout." *Id.* "With respect to this data breach," the court concluded, "plaintiffs have not plausibly alleged a substantial risk of harm sufficient to confer standing."[3] *Id.* at *4.

Similar logic explains why Plaintiffs' identity-theft theory fails in this case. What matters most is that the data disclosed here is far less likely to facilitate identity theft than the credit and debit card numbers at issue in *Remijas*. As the Seventh Circuit has observed, "the information stolen from payment cards can be used to open new cards in the consumer's name." *Lewert*, 819 F.3d at 967 (citing *Remijas*, 794 F.3d at 692–93). Here, by contrast, the names, emails, and dates of birth of registered students cannot "easily be used in fraudulent transactions." *Vtech*, 2017 WL 2880102, at *4. If anything, the data at issue here is less sensitive than in *Vtech*, which featured "passwords" and "secret questions and answers" that might be used to access other online accounts. *Id.*

This is not to say that the data taken from Pearson's servers could never enable identity theft. In a tactic that cybersecurity experts call "social engineering,"

[3] The *Vtech* court went on to identify an injury-in-fact based on "benefit-of-the-bargain damages resulting from [plaintiffs'] breach of contract claim, because the products they received were worth less than the products they were promised." *Id.* at *5. Given that Plaintiffs never paid for Pearson's services, that theory is not implicated here, and Plaintiffs do not argue otherwise.

hackers sometimes collect relatively benign information about consumers and contact "IT help desk [personnel]" at various companies in an effort to obtain more sensitive information, such as credit card or social security numbers. Am. Compl. ¶ 24. Under the circumstances alleged in the complaint, however, any theory that the data would facilitate social engineering depends on a "highly attenuated chain of possibilities" that "does not satisfy [Article III]." *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 410 (2013).

To see why this is so, it is helpful to put oneself in the shoes of the hackers responsible for the Pearson breach. They now have a list of students' names, birthdays, and email addresses. But they have no way of knowing which students hold bank or credit card accounts at which company. And, even if the hackers guess that a specific student patronizes a particular financial institution, they will need to persuade that institution's IT staff that they represent the student. Given that names, birthdays, and emails are not usually viewed as reliable indicators of identity in and of themselves, that will be a difficult task. Should the hackers succeed, IT staff may still refuse to disclose sensitive information over the phone, preferring to send it to the students' email or physical addresses, over which the hackers have no control.

As this example illustrates, Plaintiffs' social engineering theory involves a "long sequence of uncertain contingencies involving multiple independent actors." *Attias v. Carefirst, Inc.*, 865 F.3d 620, 629 (D.C. Cir. 2017). In other words, social engineering only poses a threat if exceptionally determined hackers encounter

especially credulous IT personnel. While that combination is theoretically possible, nothing in the complaint establishes that it exposes Plaintiffs to a substantial risk. *See Whitmore v. Ark.*, 495 U.S. 149, 158 (1990) ("Allegations of possible future injury do not satisfy the requirements of Art[icle] III.").

Plaintiffs' inability to identify any consequences of the data breach reinforces that conclusion. More than a year after the breach, Plaintiffs cannot point to a single instance of identity theft affecting any of the 900,000 members of the putative class. Am. Compl. ¶ 1. By comparison, the *Remijas* plaintiffs alleged that thousands of shoppers had reported fraudulent charges on their credit card statements. 794 F.3d at 690. And, although Plaintiffs cite an FBI warning that "collection of student data could have . . . safety implications" for children, they do not spotlight any safety incident attributable to the Pearson breach. Am. Compl. ¶ 32. Nor do they "allege that the hacker is a predator, or that the hacker disseminated the information broadly, to predators or anyone else who would harm the children." *Vtech*, 2017 WL 2880102, at *4. Ultimately, Plaintiffs' failure to describe any "fallout" underscores the relatively minimal danger posed by the data breach. *Id.* at *3–4.

In resisting that conclusion, Plaintiffs make much of Pearson's offer to supply students with free credit monitoring services in the wake of the breach. In *Remijas*, the court interpreted a similar offer as an admission that the risk of identity theft was not "so ephemeral that it can safely be disregarded." 794 F.3d at 694. Seizing on that language, Plaintiffs read *Remijas* as holding that a firm's provision of

identity protection services is enough to establish that a breach poses a material danger.

But neither Seventh Circuit case law nor common sense support that conclusion. When the *Remijas* court analyzed the risk of identity theft, it repeatedly highlighted the sensitive nature of the compromised data and the actual incidences of fraudulent charges, much more so than the fact that the defendant had offered credit monitoring services to its customers. *See, e.g.*, *id.* at 690, 691, 692. And in subsequent opinions, the Court of Appeals has assessed the threat posed by data breaches without even mentioning the presence or absence of any offers to provide credit monitoring. *See Lewert*, 819 F.3d at 967; *Tierney v. Advocate Health & Hosps. Corp.*, 797 F.3d 449, 451 (7th Cir. 2015). At most, Seventh Circuit precedent suggests that the provision of credit monitoring plays a minor part in standing analysis, not the decisive role Plaintiffs' envision.

Two practical considerations confirm the wisdom of that approach. First, the availability of free credit monitoring is an unreliable indicator of risk. The premise underlying Plaintiffs' argument is that firms only offer post-breach services when identity theft poses a serious threat. But firms may have other incentives to offer such services even when a data breach presents little or no risk, such as the need to placate and retain customers. According to a report cited in the complaint, for example, engaging those services has emerged as the "standard" response to data breaches in some industries. Am. Compl. ¶ 29 n.8 (citing Government Accountability Office, *Data Breaches—Range of Consumer Risks Highlights*

Limitations of Identity Theft Services, at *11, https://www.gao.gov/assets/700/697985.pdf.). It follows that the provision of free services reveals relatively little about the degree of risk created by a breach.

Second, recognizing an injury-in-fact whenever firms supply identity protection services would create perverse incentives. Most of the time, courts "exclude[ ] evidence of subsequent remedial measures as proof of an admission of fault." Fed. R. Evid. 407, advisory committee's notes. A contrary rule would "discourag[e] [defendants] from taking steps in furtherance of added safety." *Id.* As the Third and Fourth Circuits have recognized, similar logic militates against placing substantial weight on a firm's decision to offer post-breach services. *See In re Horizon Healthcare Servs. Inc. Data Breach Litig.*, 846 F.3d 625, 634 n.12 (3d Cir. 2017); *Beck v. McDonald*, 848 F.3d 262, 276 (4th Cir. 2017). To do otherwise risks "disincentiviz[ing] companies from offering [free] services in the wake of a breach." *Horizon*, 946 F.3d at 634 n.12.

In short, Plaintiffs' theory fails because the disclosed data is not sensitive enough to materially increase the risk of identity theft. That none of the affected students seems to have suffered adverse consequences from the breach confirms this diagnosis, and Pearson's provision of credit monitoring services is not a reliable enough indicator of risk to undermine it. The result is that Plaintiffs cannot demonstrate Article III standing on this basis.[4]

[4] The complaint also predicts that Plaintiffs will incur mitigation expenses in responding to the data breach. Am. Compl. ¶ 66. While that is sometimes sufficient to support standing, see *Remijas*, 794 F.3d at 694, Plaintiffs do not press this argument in their response brief, so the Court does not consider it.

B. Diminution in Value of Personal Data

In the alternative, Plaintiffs assert that the data breach reduced the market value of their personal information. "[A]n economic market existed for Plaintiffs' and Class Members' [data]," their theory goes, and "the value of that data decreased as a result of its availability on the black market." Pls.' Resp. at 12, ECF No. 33. What is missing from the complaint, however, are any allegations that the Pearson hackers have attempted to trade the compromised data for anything of value. *See, e.g.*, *In re Yahoo! Inc. Customer Data. Sec. Breach Litig.*, No. 16-MD-02752-LHK, 2017 WL 3727318, at *14 (N.D. Cal. Aug. 30, 2017) (identifying an injury-in fact because the complaint "include[d] several examples of hackers selling [personal identification information] from Yahoo accounts on the dark web"). Nor do Plaintiffs plead that they have ever sold their data or that they would even consider doing so. *See* Am. Compl. ¶ 26; *Khan v. Children's Nat'l Health Sys.*, 188 F. Supp. 3d 524, 533 (D. Md. 2016). Those deficiencies make this theory "too speculative" to confer standing. *See Clapper*, 568 U.S. at 401.

C. Standing Based on Statutory Violations

Finally, Plaintiffs insist that certain statutes establish that any disclosure of student data counts as an injury, regardless of whether it leads to economic loss. As a general rule, legislatures "have the power to enact statutes creating legal rights, the invasion of which creates standing, even though no injury would exist without the statute." *Gaylor v. Mnuchin*, 919 F.3d 420, 426 (7th Cir. 2019) (citing *Sterk v. Redbox Automated Retail, LLC*, 770 F.3d 618, 623 (7th Cir. 2014)). For a statute to confer standing, however, a claimant must clear two hurdles. First, he must "allege[ ] a violation of a legally protected interest" established by the statute. *Sterk*, 770 F.3d at 623. Second, he must show that the statute protects a "substantive" rather than a "procedural" interest. *Bryant v. Compass Grp., USA, Inc.*, No. 20-1443, 2020 WL 2121463, at *6 (7th Cir. May 5, 2020).

In analyzing the first step, the Seventh Circuit distinguishes between statutes that award "statutory damages" and those that "require[ ] an actual injury." *Diedrich v. Ocwen Loan Servicing, LLC*, 839 F.3d 583, 589 (7th Cir. 2016). If the relevant legislation grants statutory damages, courts generally proceed to the second step. *See CS Wang & Assoc. v. Wells Fargo Bank, N.A.*, 305 F. Supp. 3d 864, 880 (N.D. Ill. 2018) ("[It is] telling, though not dispositive, that [a statute] gives injured persons the right to sue for . . . statutory damages"). But if the statute calls for "actual injury," then "the injury requirement for standing overlaps with the injury requirement under the statute," and there is "no need to perform a separate [analysis]" of statutory standing. *Diedrich*, 839 F.3d at 589.

Plaintiffs falter at the first step. In claiming that they retain a legally-protected interest in the compromised records, Plaintiffs invoke the Family Education Rights and Privacy Act ("FERPA"), 20 U.S.C. § 1232g, and the Illinois School Student Records Act ("ISSRA"), 105 Ill. Comp. Stat. § 10/1 *et seq*. At a minimum, however, statutory standing demands that the claimant plead a violation of the cited statute. *See Sterk*, 770 F.3d at 623. And, while the complaint elaborates a dozen different causes of action, it does not allege that Pearson ran afoul of FERPA or ISSRA.

A more fundamental problem is that neither statute treats the disclosure of student data as an injury unless the plaintiff suffers actual damages. To be sure, ISSRA empowers "[a]ny person injured by a . . . violation of this Act [to] institute an action for damages[.]" 105 Ill. Comp. Stat. § 10/9(b). But it goes on to clarify that "[i]n the case of any successful action . . . [the defendant] is liable to the plaintiff for the plaintiff's damages, the costs of the action and reasonable attorneys' fees," and nothing more. *Id.* § 10/9(c). Because ISSRA limits recovery to "the plaintiff's damages," *id.*, and makes no provision for statutory or nominal damages, the Court concludes that an claim brought under ISSRA "requires an actual injury." *Diedrich*, 839 F.3d at 589.

FERPA is similarly unhelpful to Plaintiffs. Nearly two decades ago, the Supreme Court held that FERPA's "nondisclosure provisions fail to confer enforceable rights." *Gonzaga Univ. v. Doe*, 536 U.S. 273, 287 (2002). That means that FERPA does not "creat[e] legal rights, the invasion of which creates standing."

Gaylor, 919 F.3d at 426; *see Kyles v. J.K. Guardian Sec. Servs., Inc.*, 222 F.3d 289, 294 (7th Cir. 2000) (explaining that statutory standing "depends in great measure on the particular rights conferred").

Perhaps anticipating these problems, Plaintiffs have submitted a supplemental memorandum. *See* Supp. Not. at 1–2, ECF No. 55. Although that memorandum purports to alert this Court to the Seventh Circuit's recent decision in *Bryant*, 2020 WL 2121463, at *5–7, Plaintiffs also use it as an opportunity to raise arguments they left out of their response brief. Specifically, they claim that Illinois's Personal Information Protection Act ("PIPA"), see 815 Ill. Comp. Stat. § 530/1, *et seq*., and Colorado's Security Breach Notification Act, see Colo. Rev. Stat. § 6-1-716, *et seq*., confer standing.

Putting aside the procedural dodginess of the filing, neither statute saves Plaintiffs. For one thing, *Remijas* determined that PIPA fails to "provide the basis for finding an injury for Article III standing" because it "requires actual damages." 794 F.3d at 695–96 (citing *People ex rel. Madigan v. United Const. of Am., Inc.*, 981 N.E.2d 404, 411 (Ill. App. Ct. 2012)). And, like FERPA, the Colorado notification law does not create a private right of action. *See* Colo. Rev. Stat. § 6-1-716(g)(4).

Ultimately, then, the injury-in-fact element hinges on whether the breach caused economic loss by magnifying the danger of identity theft or diminishing the value of Plaintiffs' data. Because Plaintiffs have failed to sustain either of those theories, they cannot support Article III standing.[5] As a result, the complaint is

[5] As an aside, the Court notes that the District of Minnesota recently dismissed a similar case arising from the Pearson data breach because it concluded that the plaintiffs

dismissed without prejudice for lack of subject-matter jurisdiction. *See Remijas*, 794 F.3d at 690 ("Where federal subject matter jurisdiction does not exist, federal courts do not have the power to dismiss with prejudice.") (citation omitted). Given that Plaintiffs have only amended their complaint once, and that they may be able to introduce facts that establish standing, the Court will allow them to revise their allegations a second and final time.

IV. Conclusion

For the reasons stated above, the motion to dismiss is granted. Pearson's motion to strike the class claims [22] and Plaintiffs' motion to strike certain declarations submitted by Pearson [32] are denied as moot. If Plaintiffs choose, they may submit a second amended complaint by August 21, 2020. If they do not do so, the Court will assume that Plaintiffs no longer wish to pursue this litigation and will terminate the case.

IT IS SO ORDERED.

ENTERED 7/28/20

John Z. Lee
United States District Judge

lacked Article III standing. *See George v. Pearson et al.*, No. 19-cv-2814 (JRT/KMM), 2020 WL 3642325, at *4 (D. Minn. July 6, 2020) (relying on the Eighth Circuit's decision in *In Re Supervalu, Inc.*, 870 F.3d 763, 771 (8th Cir. 2017)).