NOT FOR PUBLICATION

FILED

SEP 8 2025

MOLLY C. DWYER, CLERK
U.S. COURT OF APPEALS

UNITED STATES COURT OF APPEALS

FOR THE NINTH CIRCUIT

ANASTASIYA KISIL; LUCAS CRANOR; SARAH CHUNG; KRISTEN WEILAND; LORRAINE DENIZ; TARA CHAMBERS; JANENE VITRO, Plaintiffs - Appellants, v. ILLUMINATE EDUCATION, INC., doing business as Pupil Path, Defendant - Appellee.	No. 23-4114 D.C. No. 8:22-cv-01164-JVS-ADS MEMORANDUM*

Appeal from the United States District Court
for the Central District of California
James V. Selna, District Judge, Presiding

Argued and Submitted January 16, 2025
Pasadena, California

Before: RAWLINSON and M. SMITH, Circuit Judges, and RAKOFF, District Judge.**

Plaintiffs, parents of schoolchildren whose data was subject to unauthorized

* This disposition is not appropriate for publication and is not precedent except as provided by Ninth Circuit Rule 36-3.

** The Honorable Jed S. Rakoff, United States District Judge for the Southern District of New York, sitting by designation.

access during a data breach targeting Defendant Illuminate Education, Inc. (Illuminate), appeal an order of the district court granting Illuminate's motion to dismiss Plaintiffs' putative class action suit. We have appellate jurisdiction pursuant to 28 U.S.C. § 1291, and we affirm.

Because the parties are familiar with the facts and background of this case, we provide only the information necessary to give context to our ruling. Illuminate is a software company that services millions of students across the nation. Between December 28, 2021, and January 8, 2022, Illuminate suffered a data breach affecting over three million students. While the data that was compromised varies by child, it potentially included information such as grades, socio-economic disadvantage status, and special education information. Illuminate informed parents that Social Security numbers and financial information were not at risk, and none of the breached information has yet been released.

Plaintiffs filed a putative class action against Illuminate, seeking damages and injunctive relief. The district court dismissed for lack of standing but allowed Plaintiffs leave to amend. Plaintiffs then filed an amended complaint, which is the operative pleading. The district court again dismissed for lack of standing and did not allow plaintiffs further leave to amend. Plaintiffs appealed. We review a district court's dismissal for lack of standing de novo. *Hong Kong Supermarket v. Kizer*, 830 F.2d 1078, 1080 (9th Cir. 1987). Plaintiffs must demonstrate standing

for each form of relief sought. *See TransUnion LLC v. Ramirez*, 594 U.S. 413, 431 (2021).

1. Plaintiffs have not demonstrated that they have suffered intangible harms sufficient to support standing. As an initial matter, *TransUnion*'s requirement that an intangible harm can be a basis for standing only where the asserted injury has a "close relationship to harms traditionally recognized as providing a basis for lawsuits in American courts," 594 U.S. at 425, applies to state statutory and common law claims. It is not—as Plaintiffs seemingly assert—only applicable to claims based on federal statutes. *See Popa v. Microsoft Corp.*, No. 24-14, 2025 WL 2448824, at *4–7 (9th Cir. Aug. 26, 2025) (applying *TransUnion*'s requirement of a common law analogue to claims based on a Pennsylvania statute and Pennsylvania common law). Moreover, contrary to Plaintiffs' assertions otherwise, a plaintiff cannot simply assert statutory or common law actions that are supposedly "injuries in themselves" to obtain standing; they must still demonstrate how the intangible harm from the statutory violation or tortious conduct is sufficiently closely related to a traditionally recognized harm. *Id.* at *4.

Although Plaintiffs appear to argue that, regardless, they have standing for all their claims because the intangible harms from the breach are closely related to the general common law injury of "intrusion upon personal privacy," we do not recognize a "free-roaming" common law right to privacy. *See id.* at *6. Rather,

both common law and statutory claims based on intangible harm from an invasion of privacy must be "benchmarked" to one of four distinct privacy torts. *Id.* at *4–6. And although Plaintiffs *also* appear to argue that, regardless, their harms are similar to those from the specific privacy tort of intrusion upon seclusion and non-privacy tort of defamation, they have waived these arguments by failing to raise them sufficiently for the trial court to rule on them.[1] *See In re Mercury Interactive Corp. Sec. Litig.*, 618 F.3d 988, 992 (9th Cir. 2010).

2. Plaintiffs have not demonstrated that they have suffered tangible harms or a risk of future harm sufficient to support standing, either. Plaintiffs allege the data breach exposed them to "further imminent and substantial risk of future harm in the form of identity theft," which can support standing for injunctive relief and damages based on (1) the cost of monitoring, (2) emotional distress from the risk, and (3) the imminent and substantial risk itself. The district court rejected these arguments, explaining that there has been no actual identity theft, the information at issue does not create an imminent and substantial risk of identity theft, and the harms resulting from the knowledge of a risk of identity theft cannot support

[1] To the extent Plaintiffs also imply that they are relying on the common law analogue of intentional infliction of emotional distress, that argument is waived as well. And their argument that, regardless, they have suffered a concrete harm of emotional distress from the potential exposure of their data fails for the same reason as their identity theft arguments below: they have not shown that there is a substantial and imminent risk that their data will be misused.

standing where the risk is not imminent or substantial.

We agree with the district court. Plaintiffs have not shown that identity theft has occurred, so Plaintiffs cannot assert standing for damages based on the risk of future harm of identity theft. *See Bock v. Washington*, 33 F.4th 1139, 1144–45 (9th Cir. 2022). Additionally, Plaintiffs have not demonstrated that the breach created an "imminent and substantial" risk of identity theft sufficient to support injunctive relief. *TransUnion*, 594 U.S. at 435. It has been more than three years since the breach, and no fraud has occurred, nor is the kind of information at issue the kind that this court normally considers sufficient to find a credible threat of identity theft. *See, e.g.*, *Krottner v. Starbucks Corp.*, 628 F.3d 1139, 1140–41, 1143 (9th Cir. 2010) (Social Security numbers were compromised). Also, although Illuminate provided access to monitoring services, it did so as "an added precaution" and did not indicate that fraud was likely to occur. Plaintiffs' assertion that they have standing for damages based on the derivative harms of emotional distress and mitigation costs from the risk of future harm therefore fail as well. *See Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 402 (2013) (a plaintiff "cannot manufacture standing by choosing to make expenditures based on hypothetical future harm that is not certainly impending.").

AFFIRMED.