

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

-----	X	
	:	
ROBIN STEVEN et al.,	:	
	:	
Plaintiffs,	:	
	:	18-CV-6500 (JMF)
-v-	:	
	:	<u>MEMORANDUM</u>
CARLOS LOPEZ & ASSOCIATES, LLC, and	:	<u>OPINION AND ORDER</u>
CARLOS LOPEZ, individually,	:	
	:	
Defendants.	:	
	:	
-----	X	

JESSE M. FURMAN, United States District Judge:

In June 2018, an employee of Defendant Carlos Lopez & Associates, LLC (“CLA”), a provider of mental and behavioral health services to veterans and others, accidentally sent an email containing personal information about approximately 130 current and former CLA employees to a distribution list of current CLA employees (a group numbering about sixty five). ECF No. 18 (“Compl.”), ¶¶ 1, 19-20; see also Nov. 14, 2019 Tr. (“Tr.”) 10. Although there is no evidence that the personal information contained in the email was shared with anyone outside of CLA, let alone misused, several people whose information had been shared sued on behalf of a class of all those whose information had been shared, alleging negligence and violations of several states’ laws. Compl. ¶¶ 21-23, 64-101. Defendants CLA and Carlos Lopez moved to dismiss for, among other things, lack of Article III standing, see ECF Nos. 24-25, but before Plaintiffs filed any opposition to that motion, the parties reached a class-wide settlement, see ECF No. 33. Plaintiffs now move, pursuant to Rule 23(e) of the Federal Rules of Civil Procedure, for approval of the parties’ settlement and an award of attorney’s fees.

Although unopposed, Plaintiffs’ motion is denied. It is axiomatic that “federal courts are

courts of limited jurisdiction and, as such, lack the power to disregard such limits as have been imposed by the Constitution or Congress.” *Purdue Pharma L.P. v. Kentucky*, 704 F.3d 208, 213 (2d Cir. 2013) (internal quotation marks omitted). One critical limit set forth in Article III of the United States Constitution is that all suits filed in federal court must be “cases and controversies of the sort traditionally amenable to, and resolved by, the judicial process.” *Steel Co. v. Citizens for a Better Env’t*, 523 U.S. 83, 102 (1998). And “[the] case-or-controversy requirement is satisfied only where a plaintiff has standing” to bring suit. *Sprint Commc’ns Co., L.P. v. APCC Servs., Inc.*, 554 U.S. 269, 273 (2008) (emphasis added). Thus, a federal court has “an obligation to assure [itself] of litigants’ standing under Article III.” *Frank v. Gaos*, 139 S. Ct. 1041, 1046 (2019) (internal quotation marks omitted). Most relevant here, as the Supreme Court emphasized only this year, “[t]hat obligation extends to court approval of proposed class action settlements” because “the ‘claims, issues, or defenses of a certified class — or a class proposed to be certified for purposes of settlement — may be settled, voluntarily dismissed, or compromised only with the court’s approval.’ A court is powerless to approve a proposed class settlement if it lacks jurisdiction over the dispute, and federal courts lack jurisdiction if no named plaintiff has standing.” *Id.* (quoting Fed. R. Civ. P. 23(e)). Thus, although the parties have reached a settlement — and, in light of that settlement, Defendants have apparently agreed not to press their arguments about standing (despite remaining of the view that Plaintiffs do not actually have standing, see ECF No. 58; Tr. 14) — the Court is not free to stick its head in the sand. Instead, it must confirm for itself that Plaintiffs have standing.¹

¹ *Whitehead v. Advance Stores Co.*, 16-CV-250 (M.D. Fl. 2017), cited by the parties, see ECF No. 58, at 1; ECF No. 57 (“Pls.’ Standing Mem.”), at 5, does not suggest otherwise. First, contrary to the parties’ suggestion, the Court in that case made an explicit finding in its order approving the settlement that it had subject-matter jurisdiction. See *Whitehead v. Advance Stores Co.*, 16-CV-250, ECF No. 60, ¶ 2. And even if that were not the case, the Court is bound by the

The Court concludes that they do not. To establish Article III standing, a plaintiff must allege, among other things, “injury in fact.” *Susan B. Anthony List v. Driehaus*, 134 S. Ct. 2334, 2341 (2014). An injury-in-fact is “an invasion of a legally protected interest that is concrete and particularized and actual or imminent, not conjectural or hypothetical.” *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1548 (2016) (internal quotation marks omitted). “Although imminence is concededly a somewhat elastic concept, it cannot be stretched beyond its purpose, which is to ensure that the alleged injury is not too speculative for Article III purposes.” *Clapper v. Amnesty Int’l USA*, 133 S. Ct. 1138, 1147 (2013) (quoting *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 564 n.2 (1992)). Accordingly, an allegation of threatened injury in the future is sufficient to establish standing only “if the threatened injury is ‘certainly impending,’ or there is a ‘substantial risk’ that the harm will occur.” *Susan B. Anthony List*, 134 S. Ct. at 2341 (quoting *Clapper*, 133 S. Ct. at 1147, 1150 n.5). Although Supreme Court precedent does not “uniformly require plaintiffs to demonstrate that it is literally certain that the harms they identify will come about” — hence, the “substantial risk” standard — no Article III standing exists if a plaintiff’s theory of injury rests on an “attenuated chain of inferences necessary to find harm.” *Clapper*, 133 S. Ct. at 1150 n. 5. Ultimately, the purpose of the imminence requirement is “to ensure that the court avoids deciding a purely hypothetical case in which the projected harm may ultimately fail to occur.” *Baur v. Veneman*, 352 F.3d 625, 632 (2d Cir. 2003).

Applying these principles, many courts have held that plaintiffs alleging the theft of personal identifying information in a “data breach” have standing to bring claims against the entity that had held their data based on an increased risk of future identity theft. See, e.g., *In re*

Supreme Court’s decision in *Frank*, not by the district court’s decision in *Whitehead*.

U.S. Office of Pers. Mgmt. Data Sec. Breach Litig., 928 F.3d 42, 55-61 (D.C. Cir. 2019) (“OPM”); *Attias v. Carefirst, Inc.*, 865 F.3d 620, 628-29 (D.C. Cir. 2017); *Galaria v. Nationwide Mut. Ins. Co.*, 663 F. App’x 384, 387-89 (6th Cir. Sept. 12, 2016) (unpublished); *Lewert v. P.F. Chang’s China Bistro, Inc.*, 819 F.3d 963, 967-68 (7th Cir. 2016); *Remijas v. Neiman Marcus Grp., LLC*, 794 F.3d 688, 692, 694-95 (7th Cir. 2015); *Fero v. Excellus Health Plan, Inc.*, 304 F. Supp. 3d 333, 338-40 (W.D.N.Y. 2018); *Sackin v. TransPerfect Glob., Inc.*, 278 F. Supp. 3d 739, 746 (S.D.N.Y. 2017). The Second Circuit has not yet ruled on the issue, but it did cite some of these cases, arguably with approval, in a summary order. See *Whalen v. Michaels Stores, Inc.*, 689 F. App’x 89, 91 & n.1 (2d Cir. 2017) (summary order). On that basis, some district courts within the Circuit have predicted — as Plaintiffs do here — that the Second Circuit would adopt the same approach. See, e.g., *Fero*, 304 F. Supp. 3d at 339 (“Whalen’s favorable citations to *Galaria*, *Remijas*, and *Lewert* suggest that the Second Circuit would follow the approach to the standing issue adopted by the Sixth and Seventh Circuits, which have both found standing based on increased risk of identity theft.”); accord *Sackin*, 278 F. Supp. 3d at 746; see also Pls.’ Standing Mem. at 1-2.

That may be so, but it would be of no help to Plaintiffs in this case. Indeed, if anything, the cases cited above demonstrate why their “increased risk” theory — upon which their claim of standing depends — is too speculative to survive scrutiny. In several of these cases, at least one named plaintiff alleged actual misuse of his or her personal information by the suspected data thief. See, e.g., *OPM*, 928 F.3d at 56 (noting that “several” plaintiffs “allege that unauthorized charges have appeared on their existing credit card and bank account statements since the breaches”); *Lewert*, 819 F.3d at 967 (noting that one plaintiff “asserts that he already has experienced fraudulent charges”); *Remijas*, 794 F.3d at 690 (noting that 9,200 of the 350,000

credit cards potentially exposed to malware “were known to have been used fraudulently”). And in all of them, the data was stolen by hackers or cyber criminals who had intentionally targeted the data. See *OPM*, 928 F.3d at 50; *Attias*, 865 F.3d at 623; *Galaria*, 663 F. App’x at 386; *Lewert*, 819 F.3d at 965; *Remijas*, 794 F.3d at 690; *Fero*, 304 F. Supp. 3d at 335; *Sackin*, 278 F. Supp. 3d at 744. Notably, when pressed on the point at oral argument, Plaintiffs’ counsel could not name a single case in which a court had found standing based on the risk of future identity theft that did not arise from such an intentional act. See Tr. 14-15.

Thus, “these cases have a common denominator. In each of them, the plaintiffs’ data actually had been [targeted and taken] by one or more unauthorized third parties.” *Katz v. Pershing, LLC*, 672 F.3d 64, 80 (1st Cir. 2012). That intentional act of theft gave rise, in turn, to a plausible inference that the stolen data would be misused. As the Seventh Circuit put it in *Remijas*, where data is intentionally stolen by a hacker “it is plausible to infer that the plaintiffs have shown a substantial risk of harm from the . . . data breach. Why else would hackers break into a store’s database and steal consumers’ private information? Presumably, the purpose of the hack is, sooner or later, to make fraudulent charges or assume those consumers’ identities.” 794 F.3d at 693; see, e.g., *Attias*, 865 F.3d at 628-29 (holding that where an “unauthorized party” has accessed personally identifying data “it is plausible . . . to infer that this party has both the intent and the ability to use that data for ill. . . . No long sequence of uncertain contingencies involving multiple independent actors has to occur before the plaintiffs in this case will suffer any harm; a substantial risk of harm exists already, simply by virtue of the hack and the nature of the data that the plaintiffs allege was taken.”); *Lewert*, 819 F.3d at 967 (“It is plausible to infer a substantial risk of harm from the data breach, because a primary incentive for hackers is sooner or later to make fraudulent charges or assume those consumers’ identities.” (internal quotation

marks omitted)); *Galaria*, 663 F. App'x at 388 (“There is no need for speculation where Plaintiffs allege that their data has already been stolen and is now in the hands of ill-intentioned criminals. . . . Where a data breach targets personal information, a reasonable inference can be drawn that the hackers will use the victims’ data for . . . fraudulent purposes . . .”).

By contrast, in the absence of an allegation or evidence that an unauthorized third party intentionally stole the data at issue, courts have concluded that the risk of identity theft is too speculative to support Article III standing. See, e.g., *Beck v. McDonald*, 848 F.3d 262 (4th Cir. 2017); *Katz*, 672 F.3d at 79-80; *Randolph v. ING Life Ins. & Annuity Co.*, 486 F. Supp. 2d 1, 7-8 (D.D.C. 2007); see also *Reilly v. Ceridian Corp.*, 664 F.3d 38, 40, 44 (3d Cir. 2011) (holding that employees lacked standing to bring claims where an unknown hacker had penetrated their company’s payroll system firewall because it was “not known whether the hacker read, copied, or understood” the system’s information and no evidence suggested past or future misuse of employee data or that the “intrusion was intentional or malicious”).² *Beck* is instructive. There, the plaintiffs brought claims based on two incidents: the theft of a laptop containing their personal data and the theft or loss of boxes containing their personal data. On appeal, the Fourth Circuit held that “the mere theft of these items, without more, cannot confer Article III standing.” 848 F.3d at 275. “[F]or the Plaintiffs to suffer the harm of identity theft that they fear,” the Court explained, “we must engage with the same ‘attenuated chain of possibilities’ rejected by the Court in *Clapper*. . . . [W]e must assume that the thief targeted the stolen items for the personal

² Although some courts have suggested that these cases are in conflict with the cases finding standing cited above, see, e.g., *Fero*, 304 F. Supp. 3d at 338, others have concluded that they are distinguishable on their facts and thus reconcilable, see, e.g., *OPM*, 928 F.3d at 58-59; *Beck*, 848 F.3d at 274-75; *Galaria*, 663 F. App'x at 389. Whether there is a genuine split among the courts of appeals on this issue is irrelevant for purposes of this case.

information they contained. And . . . the thieves must then select, from thousands of others, the personal information of the named plaintiffs and attempt successfully to use that information to steal their identities. This ‘attenuated chain’ cannot confer standing.” *Id.* (quoting *Clapper*, 133 S. Ct. at 1147-48); see also *Randolph*, 486 F. Supp. 2d at 7-8 (deeming the plaintiffs’ allegation “that at some unspecified point in the indefinite future they will be the victims of identity theft” too speculative because, although their information had been stolen by a burglar, they did “not allege that the burglar who stole the laptop did so in order to access their [i]nformation, or that their [i]nformation ha[d] actually been accessed since the laptop was stolen”).

The present case falls comfortably on the Beck side of the line. Plaintiffs make no allegation that their data was actually viewed, downloaded, copied, or shared, let alone misused. In fact, they affirmatively concede that there is no evidence that “any class member’s identity” was “stolen as a result of the breach.” ECF No. 52, at 19. And, of course, they do not allege that their data was compromised as a result of a hack or some other criminal act. Instead, they allege only that their data was compromised by an errant email sent within CLA (a company, for what it is worth, whose employees obviously deal with sensitive information of all kinds).³ If anything, the case for standing in this case is considerably weaker than it was in Beck. In Beck, the data was (or might have been) compromised as the result of a criminal act, yet the court still found the risk of future injury too speculative because there was no indication that the thief had intentionally targeted the data itself. Here, by contrast, there is no allegation of any criminal act

³ For these reasons, it is arguably a misnomer to even call this case a “data breach” case. Cf. N.Y. Gen. Bus. Law § 899-aa(1)(c)(1)-(3) (listing the following as relevant factors to determining if a data breach occurred: “indications that the information is in the physical possession and control of an unauthorized person . . . , indications that the information has been downloaded or copied . . . , or indications that the information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported”). At best, the data was “misplaced.” Cf. *Randolph*, 486 F. Supp. 2d at 6-7 (collecting “lost data” cases).

whatsoever; instead, Plaintiffs speculate that one of the CLA employees who received the email in error — all of whom owed duties and responsibilities to CLA and presumably knew that they could be fired if they did anything untoward with the email — could misuse their data or provide it to a third party who could, in turn, misuse it. As in Beck, “[t]hese allegations are insufficient to establish a ‘substantial risk’ of harm.” Beck, 848 F.3d at 275. Put differently, “the risk of harm that [Plaintiffs] envision[] is unanchored to any actual incident of data breach. This omission is fatal” to their claim of substantial risk: “because [they] do[] not identify any incident in which [their] data has ever been accessed by an unauthorized person, [they] cannot satisfy Article III’s requirement of actual or impending injury.” Katz, 672 F.3d at 80.⁴

In their Complaint, Plaintiffs do allege species of current injury, namely in the form of the time and money spent monitoring or changing their financial information and accounts. See Compl. ¶ 50. Conspicuously, however, Plaintiffs did not rely on that theory when pressed by the Court to explain how they have standing — either in their supplemental memorandum of law on standing, see Pls.’ Standing Mem. 1-2 (arguing only that Plaintiffs have suffered an injury in fact “because they face an increased risk of future identity theft” (capitalization altered)), or at oral argument, see Tr. 8-16 (same). That is for good reason: Plaintiffs “cannot manufacture standing

⁴ At oral argument, Plaintiffs suggested that the Court could find a sufficiently imminent risk of future identity theft based solely on the sensitive nature of the data at issue. See Tr. 15-16. Admittedly, the Fero court read a passing remark in the Second Circuit’s unpublished decision in Whalen — to wit, that Whalen had not alleged how she could “plausibly face a threat of future fraud, because her stolen credit card was promptly canceled after the breach and no other personally identifying information — such as her birth date or Social Security number — [was] alleged to have been stolen,” Whalen, 689 F. App’x at 90-91 — to “impl[y]” that the Second Circuit would have held that the theft of “personally identifying information” alone would give rise to standing “based on a threat of future fraud.” Fero, 304 F. Supp. 3d at 339. The Court would be hesitant to follow even a clear “implication” in an unpublished Second Circuit decision. But here, the language in Whalen does not even support the Fero court’s reading, which would expand the law of standing in data breach cases well beyond the law in any other Circuit.

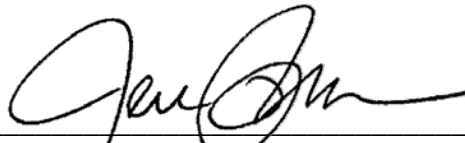
merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending.” *Clapper*, 133 S. Ct. at 1151; see, e.g., *In re Super Valu, Inc.*, 870 F.3d 763, 771 (8th Cir. 2017) (“Because plaintiffs have not alleged a substantial risk of future identity theft, the time they spent protecting themselves against this speculative threat cannot create an injury.”); *Beck*, 848 F.3d at 276-77 (rejecting the plaintiffs’ allegation that the cost of mitigating measures gave rise to standing on the ground that it was “merely ‘a repackaged version of [their] first failed theory of standing.’ Simply put, these self-imposed harms cannot confer standing.” (quoting *Clapper*, 133 S. Ct. at 1151)); *Reilly*, 664 F.3d at 46 (“[A]lleged time and money expenditures to monitor . . . financial information do not establish standing, because costs incurred to watch for a speculative chain of future events based on hypothetical future criminal acts are no more ‘actual’ injuries than the alleged ‘increased risk of injury’ . . .”).

In short, the Court is “powerless to approve” the parties’ proposed class settlement because “no named plaintiff has standing.” *Frank*, 139 S. Ct. at 1046. It follows that Plaintiffs’ motion for approval of the settlement must be and is DENIED and that this case must be DISMISSED. See Fed. R. Civ. P. 12(h)(3) (“If the court determines at any time that it lacks subject-matter jurisdiction, the court must dismiss the action.”).

The Clerk of Court is directed to terminate ECF Nos. 48 and 51 and to close this case.

SO ORDERED.

Dated: November 22, 2019
New York, New York



JESSE M. FURMAN
United States District Judge