

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

-----X	
	:
BRADLEY COOPER, <i>on behalf of himself and all others</i>	:
<i>similarly situated,</i>	:
	:
Plaintiff,	:
	:
-v-	:
	:
BONOBOS, INC.,	:
	:
Defendant.	:
	:
-----X	

21-CV-854 (JMF)

OPINION AND ORDER

JESSE M. FURMAN, United States District Judge:

To bring a lawsuit in federal court, a plaintiff must have standing, which requires a showing that he or she suffered an “injury in fact.” At a minimum, that means a plaintiff must allege and prove that, as a result of the defendant’s actions, he or she faces a “substantial risk” of some harm. The question presented in this putative class action — brought by Plaintiff Bradley Cooper against Defendant Bonobos, Inc., a men’s clothing store — is one with which many courts have grappled in recent years: whether and when someone whose personal information was stolen as part of a data breach can demonstrate a sufficiently “substantial” risk of identity theft or fraud to bring a lawsuit in federal court. In general, the answer to that question turns on evaluation of several factors: whether the data was intentionally stolen or otherwise compromised; whether any of the stolen data has already been misused; and whether the stolen data is of a “sensitive” nature and presents a high risk of identity theft or fraud, the paradigmatic example being a Social Security number. Applying these factors here, the Court concludes that Cooper lacks standing to bring claims against Bonobos relating to a 2020 data breach. Put simply, given the age and nature of the data, the risk of identity theft or fraud is too remote to

constitute injury in fact. Accordingly, and for the reasons that follow, the Court must and does dismiss this case.

BACKGROUND

The following facts are drawn from the Amended Complaint, except where noted, and assumed to be true for purposes of this motion. *See Amidax Trading Grp. v. S.W.I.F.T. SCRL*, 671 F.3d 140, 145 (2d Cir. 2011) (“In reviewing a facial attack to the court’s jurisdiction, we draw all facts — which we assume to be true unless contradicted by more specific allegations or documentary evidence — from the complaint.”).

Bonobos owns and operates a chain of men’s clothing stores that does business both online and through brick-and-mortar stores throughout the United States. ECF No. 28 (“Am. Compl.”), ¶¶ 15, 17. On June 28, 2013, Cooper purchased approximately \$170 of items through Bonobos’s website. *Id.* ¶ 25. To complete the order, he was required to enter his billing and shipping information, including his name, address, email address, telephone number, and credit card information. *Id.* Over six years later, in August 2020, a group of hackers known as “Shiny Hunters” accessed Bonobos’s cloud backup database and stole the personal information of some or all of Bonobos’s seven million online customers. *Id.* ¶ 1. Thereafter, the hackers posted the stolen information to a “hacker website forum.” *Id.* The leaked information included customers’ addresses, telephone numbers, email addresses, order history, Internet Protocol (“IP”) addresses, encrypted passwords, and partial credit card numbers (that is, the last four digits). *Id.* ¶¶ 1, 4, 23.

In January 2021, Bonobos sent notices to affected customers, including Cooper, stating that “an unauthorized third party may have been able to view some of your account details, including your contact information and encrypted password.” *Id.* ¶ 4. The notice explained that the user’s “encrypted password was protected so your actual password was not visible” and that

“[p]ayment card information was not affected by this issue.” *Id.* The notice further advised that Bonobos was “resetting your password and [had] logged you out of your account.” *Id.* In response to the message, Cooper changed the password to his Bonobos account, placed a security freeze on his credit through Experian, purchased credit repair and protection services for \$85.00 per month, and purchased a robocall-blocking subscription for \$19.99. *Id.* ¶¶ 27-28. Cooper alleges that he has also “spent time dealing with the increased and unwanted spam, text[s], telephone calls, and emails that he continues to receive after the [d]ata [b]reach.” *Id.* ¶ 29.

Cooper brings suit on behalf of a putative class of “[a]ll residents of the United States of America whose [p]rivate [i]nformation was compromised in the [d]ata [b]reach and who made purchases from Defendant prior to June 2018.” *Id.* ¶ 67. He brings claims for negligence, *see id.* ¶¶ 77-93, violations of Section 349 of the New York General Business Law, *see id.* ¶¶ 94-110, and unjust enrichment, *see id.* ¶¶ 111-19. Bonobos now moves, pursuant to Rule 12(b)(1) and (6) of the Federal Rules of Civil Procedure, to dismiss the Complaint for lack of subject-matter jurisdiction and for failure to state a claim. *See* ECF No. 34.

DISCUSSION

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 such limit 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). That requirement “is satisfied only where a plaintiff has standing.” *Sprint Commc’ns Co., L.P. v. APCC Servs., Inc.*, 554 U.S. 269, 273 (2008). In a class

action, that means that at least one named plaintiff must have standing. *See, e.g., Frank v. Gaos*, 139 S. Ct. 1041, 1046 (2019); *Lewis v. Casey*, 518 U.S. 343, 357 (1996).

It is well established that “the irreducible constitutional minimum of standing contains three elements”: (1) injury in fact, (2) causation, and (3) redressability. *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 560-61 (1992). An injury in fact is “an invasion of a legally protected interest which is (a) concrete and particularized, and (b) actual or imminent, not conjectural or hypothetical.” *Id.* at 560 (cleaned up). The element of causation requires that the injury be “fairly traceable to the challenged action of the defendant, and not the result of the independent action of some third party not before the court.” *Id.* (cleaned up). Finally, to establish redressability, “it must be likely, as opposed to merely speculative, that the injury will be redressed by a favorable decision.” *Id.* at 561 (internal quotation marks omitted).

An injury “need not be actualized” to satisfy Article III. *Davis v. Fed. Election Comm’n*, 554 U.S. 724, 734 (2008). But 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 v. Driehaus*, 573 U.S. 149, 158, (2014) (quoting *Clapper v. Amnesty Int’l USA*, 568 U.S. 398, 414 n.5 (2013)). Significantly, no Article III standing exists if a plaintiff’s theory of injury rests on an “attenuated chain of inferences necessary to find harm.” *Clapper*, 568 U.S. at 414 n.5. Moreover, where a plaintiff fails to demonstrate a substantial risk that harm will occur, the plaintiff “cannot manufacture standing” by incurring costs to monitor or protect against the harm. *Id.* at 416. 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).

Last year, the Second Circuit addressed how these principles apply in the (increasingly common) context of data breaches such as the one in this case. *See McMorris v. Carlos Lopez & Assocs., LLC*, 995 F.3d 295 (2d Cir. 2021). Specifically, the Court held that “plaintiffs may establish standing based on an increased risk of identity theft or fraud following the unauthorized disclosure of their data,” and identified three non-exhaustive “factors” that “bear on whether the risk . . . is sufficiently concrete, particularized, and imminent”:

(1) whether the plaintiffs’ data has been exposed as the result of a targeted attempt to obtain that data; (2) whether any portion of the dataset has already been misused, even if the plaintiffs themselves have not yet experienced identity theft or fraud; and (3) whether the type of data that has been exposed is sensitive such that there is a high risk of identity theft or fraud.

Id. at 301, 303 (cleaned up). With respect to the third factor, the Court explained: “Naturally, the dissemination of high-risk information such as Social Security numbers and dates of birth — especially when accompanied by victims’ names — makes it more likely that those victims will be subject to future identity theft or fraud. By contrast, less sensitive data, such as basic publicly available information, or data that can be rendered useless to cybercriminals does not pose the same risk of future identity theft or fraud to plaintiffs if exposed.” *Id.* at 302 (citation omitted).¹

Applying these factors here, the Court concludes that Cooper has not, and cannot, establish standing based on an increased risk of identity theft or fraud. To be sure, the first

¹ In a supplemental letter, Bonobos argues that *TransUnion LLC v. Ramirez*, 141 S. Ct. 2190 (2021), in which the Supreme Court held that a “mere risk of future harm” is insufficient to support standing, *id.* at 2211, “calls into question” whether *McMorris* remains good law. ECF No. 43. That may well be so, but it is the task of the Second Circuit, not this Court, to determine if *McMorris* should be overturned. *See, e.g., United States v. Diaz*, 122 F. Supp. 3d 165, 179 (S.D.N.Y. 2015) (observing that a district court must follow a precedential opinion of the Second Circuit “unless and until it is overruled . . . by the Second Circuit itself or unless a subsequent decision of the Supreme Court so undermines it that it will almost inevitably be overruled by the Second Circuit” (internal quotation marks omitted)), *aff’d*, 854 F.3d 197 (2d Cir. 2017). In any event, the Court need not and does not decide the issue because, for the reasons that follow, Cooper lacks standing even if *McMorris* remains good law.

McMorris factor favors Cooper because the data was stolen by a known “threat actor,” Shiny Hunters. Am. Compl. ¶ 23. But the second factor — “whether any portion of the dataset has already been misused,” 995 F.3d at 303 — cuts the other way. In arguing otherwise, Cooper points to allegations that hackers have engaged in “credential stuffing,” a technique in which they enter credentials gained from a hack into third-party websites, hoping that they will match an existing account because the consumer has reused the same password elsewhere. Am. Compl. ¶¶ 2 & n.3, 23. But conspicuously, Cooper does not allege that any of his accounts, or the accounts of other Bonobos consumers for that matter, were compromised in this manner. Nor does he allege that, in August 2020 when the Bonobos hack occurred, he even used the password that he had used for Bonobos in June 2013 on other websites.

Cooper also contends that the data “has already been misused by criminals” insofar as it was posted to a “hacker website forum.” ECF No. 39 (“Pl.’s Opp’n”), at 12; *see* Am. Compl. ¶ 23. There he is on firmer ground as the Second Circuit has held that allegations of a similar nature can help support a finding of standing based on future risk. *See McMorris*, 995 F.3d at 302 (“[A]llegations that the plaintiffs’ [personally identifiable information] was available for sale on the Dark Web following a data breach — and could therefore be purchased by cybercriminals at any moment to commit identity theft or fraud — provide[] strong support for the conclusions that those plaintiffs [have] established an Article III injury in fact.” (citing *Fero v. Excellus Health Plan, Inc.*, 304 F. Supp. 3d 333, 341, 344-45 (W.D.N.Y. 2018))). But that ground crumbles where, as here, the type of data that was exposed is not susceptible to misuse — that is, not “sensitive.” Put differently, the third *McMorris* factor dooms Cooper’s ability to establish standing based on an increased risk of identity theft or fraud. *See id.* at 304 n.6 (observing that

“there may be situations in which the nature of the data itself reveals that plaintiffs are *not* substantially at risk of identity theft as a result of the exposure”).

That is because the stolen and posted information was all “less sensitive data, such as basic publicly available information, or data that can be rendered useless to cybercriminals.” *Id.* at 302. First, it included customers’ contact information, namely “addresses, phone numbers, . . . email addresses, and IP addresses.” Am. Compl. ¶ 23. But Cooper does not allege that his contact information in August 2020, when the hack occurred, was the same as it was in June 2013, when he shared it with Bonobos. In any event, contact information is generally publicly available and, thus, “does not pose the same risk of future identity theft or fraud to plaintiffs if exposed.” *McMorris*, 995 F.3d at 302. Indeed, as Bonobos notes, Cooper’s own contact information, including his email address and phone number, is publicly available on his employer’s website. *See* ECF No. 35, at 11 (citing <http://rcc-ventures.com/team/>).² Nor does the Amended Complaint explain how disclosure of Cooper’s IP address increased the risk of identity theft or fraud. Cooper posits some hypotheticals in his opposition to Bonobos’s motion — for instance, that the hackers could use his IP address to “hack [his] device” or “hit [him] with a DDoS attack” or even “frame [him] for illegal activity by downloading illegal content they do not want traced back to them,” Pl.’s Opp’n 16 — but these hypotheticals are entirely speculative, if not fanciful, and thus insufficient to support standing. *See Clapper*, 568 U.S. at 409.

Second, the hack compromised “partial credit card numbers (including the last four digits).” Am. Compl. ¶ 23. Once again, however, Cooper fails to allege that his credit card number remained unchanged in the nearly seven years between his Bonobos purchase and the

² The Court may consider evidence beyond the pleadings in evaluating Bonobos’s motion to dismiss for lack of subject-matter jurisdiction. *See, e.g., Libertarian Party of Erie Cnty. v. Cuomo*, 970 F.3d 106, 120-21 (2d Cir. 2020).

hack. Moreover, assuming *arguendo* that the number did remain the same, Cooper could have taken the simple step upon receiving notice of the hack of canceling the card, “effectively eliminating the risk of credit card fraud in the future.” *McMorris*, 995 F.3d at 302 (quoting *Tsao v. Captiva MVP Rest. Partners, LLC*, 986 F.2d 1332, 1344 (11th Cir. 2021)). In *Whalen v. Michaels Stores, Inc.*, 689 F. App’x 89 (2d Cir. 2017) (summary order), the Second Circuit concluded that a plaintiff lacked standing where her credit card number was stolen as part of a data breach, but she promptly canceled her card “and no other personally identifying information — such as her birth date or Social Security number — is alleged to have been stolen,” *id.* at 90. If anything, Cooper’s argument for standing is even weaker because the hack did not compromise his full credit card number; it merely compromised the last four digits of his credit card, and he does not allege — let alone allege plausibly — that criminals could use that limited information to cause him harm.

Finally, the Complaint alleges that the exposed information included consumers’ “password histories.” Am. Compl. ¶ 23. But that is not entirely accurate. As the Bonobos notice makes clear (and Cooper does not dispute), the breach merely exposed a consumer’s “*encrypted password*. Your encrypted password was protected so your actual password was not visible.” *Id.* ¶ 4 (emphasis added). Thus, Cooper’s theory of future harm depends on an assumption — not supported by any allegations in the Amended Complaint — that the hackers or others could and would decrypt his password. In any event, Cooper alleges that after receiving notice of the hack, he immediately changed his Bonobos password (which, according to the notice, had already been “reset[]” by Bonobos itself), *see* Am. Compl. ¶¶ 4, 27, and he does not allege that he used the same password for other accounts. *Cf. B.J.F. v. PNI Digital Media*, No. 15-CV-1643 (MJP), 2016 WL 4014113, at *2 (W.D. Wash. July 27, 2016) (finding

no standing even where the plaintiff alleged that she had used the same password because she did not “describe the nature of the accounts that she used the same password for” or “explain how she would be harmed if those other accounts were accessed by hackers”). In these circumstances, Cooper cannot plausibly claim a risk of future harm.

Even taken together, the data stolen in the Bonobos data breach is, absent plausible allegations of misuse, insufficient to demonstrate that Cooper is at a substantial risk of identity theft or fraud. Put simply, given the nature and age of the data, the likelihood that its exposure would result in harm to Cooper is too remote to support standing. *See Whitmore v. Arkansas*, 495 U.S. 149, 158 (1990) (“Allegations of possible future injury do not satisfy the requirements of Art[icle] III.”); *see also, e.g., In re SuperValu, Inc.*, 870 F.3d 763, 770 (8th Cir. 2017) (finding no substantial risk of identity theft where the stolen data did “not include any personally identifying information, such as social security numbers, birth dates, or driver’s license numbers”); *Jackson v. Loews Hotels, Inc.*, No. 18-CV-827 (DMG), 2019 WL 6721637, at *4 (C.D. Cal. July 24, 2019) (concluding that exposure of name, phone number, email address, mailing address, and credit card number was not sufficient to allege standing); *cf. In re Zappos.com, Inc.*, 888 F.3d 1020, 1027 (9th Cir. 2018) (finding standing with respect to the exposure of data similar to that in this case, but where one group of plaintiffs had already suffered identity theft and noting that that fact “undermine[d] [the defendant’s] assertion that the data stolen in the breach cannot be used for fraud or identity theft”).³ Thus, Cooper does not, and cannot, establish standing for his claims based on the increased risk of identity theft or fraud.

³ *Peiran Zheng v. Live Auctioneers LLC*, No. 20-CV-9744 (JGK), 2021 WL 2043562 (S.D.N.Y. May 21, 2021), upon which Cooper relies, *see* Pl.’s Opp’n 14, also involved data similar to that here, but there the plaintiff’s personal information had been “sold multiple times.” *Id.* at *2. In any event, the defendant there did not challenge the plaintiff’s standing, and the court’s analysis is relegated to a single footnote. It thus warrants little, if any, weight.

That does not end the analysis, however, as Cooper also alleges several forms of actual, present-day injury. *See* Am. Compl. ¶ 29.⁴ First, he alleges that he spent time and money responding to the data breach. Specifically, he spent time self-monitoring his accounts for evidence of fraud or identity theft and freezing his accounts with Experian, *see id.* ¶¶ 27, 29, and he purchased both a credit repair and protection service as well as a subscription to a robocall blocking app, *see id.* ¶ 11. But the Supreme Court has held that plaintiffs “cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending.” *Clapper*, 568 U.S. at 416. Applying this rule in the data breach context, the Second Circuit has held that only “where plaintiffs have shown a substantial risk of future identity theft or fraud” may “any expenses they have reasonably incurred to mitigate that risk likewise qualify as injury in fact.” *McMorris*, 995 F.3d at 303 (quotation marks omitted). As Cooper does not show a substantial risk of future identity theft or fraud, it follows *a fortiori* that he cannot rely on his own expenses to secure standing. *See e.g., Muransky v. Godiva Chocolatier, Inc.*, 979 F.3d 917, 931 (11th Cir. 2020) (“[A]ny assertion of wasted time and effort necessarily rises or falls along with this Court’s determination of whether the risk posed . . . is itself a concrete harm.”).

Second, Cooper alleges as injury the “diminution in the value of his [p]rivate [i]nformation, a form of intangible information that he entrusted to Defendant for the purpose of making online purchases.” Am. Compl. ¶ 12. In support of this allegation, he references articles and other sources for the general proposition that personally identifiable information has inherent

⁴ The Amended Complaint alleges that Cooper and class members suffered “one or more of” various enumerated injuries, Am. Compl. ¶ 14, 66, but there are no allegations that Cooper suffered several of those listed: (1) the unauthorized use of his private information; (2) damages arising from the inability to use his private information; or (3) loss of privacy. *Id.* The Court does not address these theories further as they obviously do not support Cooper’s standing.

value. Am. Compl. ¶¶ 55-60. But courts have consistently “rejected allegations that the diminution in value of personal information can support standing,” *Fero*, 236 F. Supp. 3d at 755 (collecting cases); *see also Whalen*, 153 F. Supp. 3d at 581-82, particularly where the plaintiffs “have not alleged that they attempted to sell their personal information or that, if they have, the data breach forced them to accept a decreased price for that information,” *Chambliss v. Carefirst, Inc.*, 189 F. Supp. 3d 564, 572 (D. Md. 2016). That is the case here. Cooper does not “plausibly allege that [he] intended to sell [his] . . . personal information to someone else. Nor, in any event, do[es he] plausibly allege that someone else would have bought it as a stand-alone product.” *In re Facebook, Inc., Consumer Priv. User Profile Litig.*, 402 F. Supp. 3d 767, 784 (N.D. Cal. 2019).

Third, Cooper alleges that he has “spent time dealing with the increased and unwanted spam text[s], telephone calls, and emails that he continues to receive after the [d]ata [b]reach.” Am. Compl. ¶ 29. Courts have generally rejected the theory that unsolicited calls or emails constitute an injury in fact. *Cherny v. Emigrant Bank*, 604 F. Supp. 2d 605, 609 (S.D.N.Y. 2009) (“The receipt of spam by itself . . . does not constitute a sufficient injury entitling [the plaintiff] to compensable relief.”); *Jackson*, 2019 WL 6721637 *4 (“[R]eceiving spam or mass mail does not constitute an injury.”). And even if they did suffice, Cooper does not demonstrate that the spam texts, calls, and emails are “fairly traceable” to Bonobos’s actions. *Lujan*, 504 U.S. at 560-61. *In re Scientific Applications International Corp. (SAIC) Backup Tape Data Theft Litigation*, 45 F. Supp. 3d 14 (D.D.C. 2014), is illuminating on this score. There, the court contrasted two plaintiffs who alleged that they had received an increase in unsolicited calls due to the theft of a backup tape with their personal data. The first “simply alleged that he ha[d] received a number of unsolicited calls from telemarketers and scam artists.” *Id.* at 33 (quotation marks omitted).

The court found that “his harm” could not “plausibly be linked” to the defendants’ actions and that he “seem[ed] to simply be one among the many of us who are interrupted in our daily lives by unsolicited calls.” *Id.* The second plaintiff, by contrast, had an unlisted phone number and, after the theft, received calls for the first time that “targeted a specific medical condition listed in her medical records.” *Id.* This was enough to show a causal link. Cooper is like the first plaintiff. Without more, the mere allegation that he now receives more spam calls, texts, and emails does not support standing.

Finally, Cooper alleges, “[o]n information and belief, [that] the threat actors also turned the cracked passwords into a list used in credential stuffing attacks, which involves utilizing the log in information using the stolen credentials to access other websites.” Am. Compl. ¶ 23. Cooper provides extensive background information about credential stuffing but, as noted above, fails to plead that the technique was used *on him*, information that he would presumably know. He argues that he “does not need to show that he himself was the victim of credential stuffing, particularly where his data was stolen by a hacking group that is known for such tactics,” Pl.’s Opp’n 12, but that is not an accurate statement of the law, *see Warth v. Seldin*, 422 U.S. 490, 501 (1975) (“[T]he plaintiff still must allege a distinct and palpable injury to himself, even if it is an injury shared by a large class of other possible litigants”); *Shetiwy v. Midland Credit Mgmt.*, 15 F. Supp. 3d 437, 447 (S.D.N.Y. 2014) (finding no standing where the plaintiffs “failed to plead that such tactics were used *against them*, and lack standing to sue based on the injuries of others”).

CONCLUSION

In short, Cooper fails to allege any injuries that are “certainly impending” or based on a “substantial risk that the harm will occur.” *Clapper*, 568 U.S. at 409, 414 n.5 (quotation marks

omitted). Thus, Cooper's claims must be and are dismissed without prejudice for lack of subject-matter jurisdiction, and the Court need not — indeed, may not — address Bonobos's other arguments. *See, e.g., Hernandez v. Conriv Realty Assocs.*, 182 F.3d 121, 123 (2d Cir. 1999) (“Article III deprives federal courts of the power to dismiss a case with prejudice where federal subject matter jurisdiction does not exist.”). Moreover, although leave to amend should be freely given “when justice so requires,” Fed. R. Civ. P. 15(a)(2), it is “within the sound discretion of the district court to grant or deny leave to amend,” *Broidy Cap. Mgmt. LLC v. Benomar*, 944 F.3d 436, 447 (2d Cir. 2019) (internal quotation marks omitted). Here, Cooper already amended his pleadings once after Bonobos moved to dismiss, and he “fail[s] to show how amendment could . . . demonstrate[] a cognizable injury suffice to support Article III standing. Thus, any further amendment would [be] futile.” *Treiber v. Aspen Dental Mgmt., Inc.*, 635 F. App'x 1, 2 (2d Cir. 2016) (summary order).

The Clerk of Court is directed to terminate ECF No. 34, to enter judgment consistent with this Opinion and Order, and to close the case.

SO ORDERED.

Dated: January 19, 2022
New York, New York



JESSE M. FURMAN
United States District Judge