IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF SOUTH CAROLINA
AIKEN DIVISION

Lataveia Allen, on behalf of herself and all others similarly situated, Plaintiff, v. SRP Federal Credit Union, Defendant.	Case No. 1:24-cv-07476-CMC
Norman Black, on behalf of himself and all others similarly situated, Plaintiff, v. SRP Federal Credit Union, Defendant.	Case No. 1:24-cv-07519-CMC
Ge-Quoia Whitfield, on behalf of herself and all others similarly situated, Plaintiff, v. SRP Federal Credit Union, Defendant.	Case No. 1:24-cv-07537-CMC

Rosemary Ortiz, on behalf of herself and all others similarly situated, Plaintiff, v. SRP Federal Credit Union, Defendant.	Case No. 1:24-cv-07671-CMC
Theresa McGrier, on behalf of herself and all others similarly situated, Plaintiff, v. SRP Federal Credit Union, Defendant.	Case No. 1:24-cv-07695-CMC
Shannon Dunn, on behalf of herself and all others similarly situated, Plaintiff, v. SRP Federal Credit Union, Defendant.	Case No. 1:25-cv-00210-CMC

Ricky Chase, on behalf of himself and all others similarly situated, Plaintiff, v. SRP Federal Credit Union, Defendant.	Case No. 1:25-cv-00312-CMC

ORDER DISMISSING PLAINTIFFS' CONSOLIDATED COMPLAINT WITHOUT PREJUDICE AND WITH LEAVE TO AMEND

Plaintiffs in these consolidated actions are seven members of SRP Federal Credit Union ("SRP") whose personally identifiable information ("PII") was compromised in a 2024 data breach. They assert various tort and contract claims against SRP, claiming SRP failed to safeguard their PII, delayed notifying them of the breach, and understated both the scope of the breach and the risks it posed.

Now before the court is SRP's motion to compel arbitration or, in the alternative, to dismiss the consolidated complaint under Federal Rules of Civil Procedure 12(b)(1) and 12(b)(6). ECF No. 29.[1] SRP first asks the court to compel arbitration of Plaintiffs' claims based on an arbitration provision in its membership agreement and to stay the case pending the outcome of arbitration. Alternatively, it argues the complaint should be dismissed because Plaintiffs lack Article III standing and have failed to state a claim upon which relief can be granted.

[1] Citations to docket entries refer to those in the lead case, No. 1:24-cv-07476-CMC.

As explained below, the court's analysis begins and ends with standing. Although three Plaintiffs have adequately alleged an injury in fact based on fraudulent charges, the complaint, as currently pleaded, does not plausibly allege those injuries are fairly traceable to SRP's conduct. Accordingly, the court will grant SRP's motion and dismiss the complaint without prejudice for lack of standing. But the court will grant Plaintiffs leave to amend to allow them an opportunity to cure the traceability defects identified below.

I. BACKGROUND

SRP is a federally insured credit union with branches in Georgia and South Carolina. ECF No. 19 ¶ 20. It holds over $1.8 billion in assets and serves more than 195,000 members, including the seven Plaintiffs. *Id.* ¶¶ 11, 20.

On December 12, 2024, SRP notified its members "of a recent incident that may have involved some of [their] personal information." ECF No. 19-1 at 2. SRP explained that "an unknown, unauthorized third party accessed [its] computer systems" between September 5, 2024, and November 4, 2024, and "potentially acquired certain files from [its] network during that time." *Id.* Plaintiffs were informed that the "files potentially acquired by the third party" contained their names, dates of birth, Social Security numbers, and financial account numbers.[2] ECF No. 19-2 at 2–5, 9–11. SRP assured those affected it had "no evidence that [their] personal information ha[d] been misused" but encouraged them to enroll in a complimentary one-year credit monitoring

[2] Two Plaintiffs were also advised their credit card numbers were potentially compromised. ECF No. 19-2 at 9, 10.

service and to "remain vigilant" against "potential fraud and/or identity theft." ECF No. 19-1 at 2, 5.

According to the complaint, the data breach was perpetrated by a ransomware group called Nitrogen. ECF No. 19 ¶ 38. Ransomware is a type of malicious software, or "malware," that encrypts a victim's data and prevents access until a ransom payment is made. *Id.* ¶ 42. Ransomware actors also frequently employ "double extortion" tactics in which they not only encrypt the victim's data but also steal it and threaten to publicly release or sell it if the ransom is not paid. *Id.* ¶ 44; *see also* Cybersecurity & Infrastructure Sec. Agency, *#StopRansomware Guide*, https://www.cisa.gov/stopransomware/ransomware-guide (last visited Oct. 3, 2025). "Once the data is exfiltrated from a network," the complaint alleges, "it should be assume[d] it will be traded to other threat actors, sold, or held for a second/future extortion attempt." ECF No. 19 ¶ 44 (internal quotation marks omitted).

In December 2024 and January 2025, Plaintiffs Allen, Black, Whitfield, Ortiz, McGrier, Dunn, and Chase each filed separate lawsuits against SRP. After the court consolidated the cases pursuant to Federal Rule of Civil Procedure 42(a), Plaintiffs filed the operative consolidated complaint on April 7, 2025. ECF Nos. 14, 19. The complaint asserts claims for negligence, negligence per se, breach of implied contract, violation of S.C. Code Ann. § 39-1-90, breach of confidentiality, breach of fiduciary duty, unjust enrichment, and recovery of litigation expenses under Ga. Code Ann. § 13-6-11. ECF No. 19 ¶¶ 198–289. The complaint also seeks to certify a class "of at least 240,000 former and current [SRP] customers . . . whose data was compromised in the [d]ata [b]reach." *Id.* ¶¶ 185–197.

On May 22, 2025, SRP filed the instant motion to compel arbitration or, in the alternative, to dismiss for lack of standing under Rule 12(b)(1) and for failure to state a claim under Rule 12(b)(6). ECF No. 29. Plaintiffs responded in opposition on June 23, 2025, ECF No. 40, and SRP replied on July 14, 2025, ECF No. 46. SRP's motion is fully briefed and ripe for resolution.

II. LEGAL STANDARD

A motion to dismiss for lack of subject-matter jurisdiction under Rule 12(b)(1) "addresses whether [the plaintiff] has a right to be in the district court at all and whether the court has the power to hear and dispose of [its] claim." *Holloway v. Pagan River Dockside Seafood*, 669 F.3d 448, 452 (4th Cir. 2012). "Challenges to subject-matter jurisdiction can be presented either facially or factually." *Hutton v. Nat'l Bd. of Exam'rs in Optometry, Inc.*, 892 F.3d 613, 620 (4th Cir. 2020). A facial challenge argues the complaint "fails to allege facts upon which subject matter jurisdiction can be based," while a factual challenge contends "the jurisdictional allegations of the complaint [are] not true." *Kerns v. United States*, 585 F.3d 187, 192 (4th Cir. 2009) (quoting *Adams v. Bain*, 697 F.2d 1213, 1219 (4th Cir. 1982)). When, as here, a defendant raises a facial challenge, the plaintiff "is afforded the same procedural protection as he would receive under a Rule 12(b)(6) consideration." *Adams*, 697 F.2d at 1219. That means "the facts alleged in the complaint are taken as true, and the motion must be denied if the complaint alleges sufficient facts to invoke subject matter jurisdiction." *Kerns*, 585 U.S. at 192.

III. DISCUSSION

Article III of the United States Constitution limits the jurisdiction of federal courts to "Cases" and "Controversies." U.S. Const. art. III, § 2. A necessary component of the case-or-

controversy limitation is that a plaintiff must have standing to sue — that is, a "personal stake" in the outcome of the lawsuit. *TransUnion LLC v. Ramirez*, 594 U.S. 413, 423 (2021). To establish the "irreducible constitutional minimum of standing," a plaintiff must show "(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*, 578 U.S. 330, 338 (2016) (internal quotation marks omitted). This case concerns the first two elements: injury in fact and traceability.

A. Injury in Fact

Injury in fact is "the '[f]irst and foremost' of standing's three elements." *Spokeo*, 578 U.S. at 338 (quoting *Steel Co. v. Citizens for Better Environment*, 523 U.S. 83, 103 (1998)). It requires a plaintiff to demonstrate an injury that is "concrete," "particularized," and "actual or imminent." *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560 (1992) (internal quotation marks omitted).

A "concrete" injury is one that "actually exist[s]"; in other words, it is "real, and not abstract." *Spokeo*, 578 U.S. at 340 (internal quotation marks omitted). The "most obvious" kind of concrete injuries are "traditional tangible harms, such as physical harms and monetary harms." *TransUnion*, 594 U.S. at 425. But "intangible harms" may also qualify, provided they bear "a close relationship to harms traditionally recognized as providing a basis for lawsuits in American courts." *Id.* (listing "reputational harms," "disclosure of private information," "intrusion upon seclusion," and "harms specified by the Constitution itself" as examples). The second component — "particularity" — requires that "the injury must affect 'the plaintiff in a personal and individual way' and not be a generalized grievance." *FDA v. All. for Hippocratic Med.*, 602 U.S. 367, 381

(2024) (quoting *Lujan*, 504 U.S. at 560 n.1)). Finally, an injury is "actual or imminent" if the harm has "already occurred or [is] likely to occur soon." *Id.* Allegations of future harm may suffice, but 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, 409, 414 n.5 (2013)).

Two additional principles from the Supreme Court's standing cases are particularly relevant in the data-breach context. First, although "a material risk of future harm" can give rise to standing for injunctive relief if the risk is "sufficiently imminent and substantial," *TransUnion*, 594 U.S. at 435, the "mere risk of future harm" cannot support a backwards-looking claim for damages, *id.* at 436. Rather, when the remedy sought is retrospective, the threat must have either "materialize[d]" into the anticipated harm or caused "a *separate* concrete harm." *Id.* at 436 (emphasis in original). Second, a plaintiff "cannot manufacture standing by choosing to make expenditures based on hypothetical future harm that is not certainly impending." *Clapper*, 568 U.S. at 402. Put differently, costs incurred to minimize the risk of a "non-imminent harm" cannot confer standing. *Id.* at 422.

With these standing principles in mind, the court turns to the case at hand. Plaintiffs' injury-in-fact allegations can be grouped into seven categories of harm: (1) unauthorized charges; (2) risk of future identity theft; (3) time, money, and effort spent mitigating the effects of the breach; (4) loss of privacy; (5) emotional distress; (6) diminished value of their PII; and (7) increased spam communications. The court addresses each in turn below.

1. Unauthorized Charges

Three Plaintiffs — Plaintiffs McGrier, Chase, and Black — expressly allege they have incurred fraudulent charges on their SRP accounts. ECF No. 19 ¶¶ 90, 104, 118. Financial harm readily satisfies the injury-in-fact requirement. *Air Evac EMS, Inc. v. Cheatham*, 910 F.3d 751, 760 (4th Cir. 2018) ("[F]inancial harm is a classic and paradigmatic form of injury in fact." (internal quotation marks omitted)); *Penegar v. Liberty Mut. Ins. Co.*, 115 F.4th 294, 302 (4th Cir. 2024) ("[P]ast monetary loss is a quintessential injury in fact."); *see also, e.g.*, *Jenkins v. Associated Wholesale Grocers, Inc.*, No. 24-4039-DDC-GEB, 2025 WL 708574, at *7 (D. Kan. Mar. 5, 2025) ("Unauthorized purchases are actual misuses of a plaintiff's PII constituting injuries in fact.") Therefore, Plaintiffs McGrier, Chase, and Black will have standing to seek damages if the complaint contains plausible allegations that these charges are "fairly traceable" to the SRP breach. *Spokeo*, 578 U.S. at 338.

2. Risk of Future Identity Theft and Mitigation Costs

The four remaining Plaintiffs, Plaintiffs Dunn, Allen, Whitfield, and Ortiz — whom the court will refer to as the Non-Misuse Plaintiffs — each allege they face a "present and continuing risk of fraud, identity theft, and misuse resulting from [their] PII being placed in the hands of unauthorized third parties." ECF No. 19 ¶¶ 78, 134, 148, 160. They also allege they have "spent time and made reasonable efforts to mitigate the impact of the [d]ata [b]reach," such as conducting research, reviewing account statements, changing passwords, freezing their credit, and purchasing credit monitoring. *Id.* ¶¶ 76, 132, 146, 158.

As noted, "risk of future harm . . . cannot, by itself, establish concrete injury to have standing to seek damages." *Penegar*, 115 F.4th at 302 (4th Cir. 2024) (emphasis omitted) (citing *TransUnion*, 594 U.S. at 436). But "costs stemming from a potential future harm" *can* support standing for damages if "the underlying future harm" is "a non-speculative one." *Sommerville v. Union Carbide Corp.*, 149 F.4th 408, 429 (4th Cir. 2025) (Diaz, C.J., dissenting) (emphasis omitted); *Hutton*, 892 F.3d at 622 ("[T]he [Supreme] Court has recognized standing to sue on the basis of costs incurred to mitigate or avoid harm when a substantial risk of harm actually exists."). So, for purposes of evaluating the Non-Misuse Plaintiffs' mitigation costs, the court must determine, as a threshold matter, whether they have adequately alleged that future identity theft is "certainly impending" or that there is a "substantial risk" it will occur. *Clapper*, 568 U.S. at 409, 414 n.5.

The Fourth Circuit's decision in *Beck v. McDonald*, 848 F.3d 262 (4th Cir. 2017), is instructive on this point. *Beck* involved two consolidated appeals brought by veterans whose personal information had been compromised in separate data breaches at a Veterans Affairs ("VA") medical center. 848 F.3d at 266. In the first case, an unencrypted laptop containing the names, birth dates, last four digits of Social Security numbers, and physical descriptors of 7,400 patients was stolen. *Id.* at 267. The second case arose after VA officials discovered four boxes of pathology reports containing the names, Social Security numbers, and medical diagnoses of over 2,000 patients had gone missing. *Id.* at 268. The plaintiffs in both cases "sought to establish Article III standing based on the harm from the increased risk of future identity theft and the cost

of measures to protect against it." *Id.* at 266–67. Applying *Clapper*, the Fourth Circuit rejected both theories of standing.

The plaintiffs' first theory was "too speculative to constitute an injury-in-fact," the court explained, because it required the court to "assume that the thie[ves] targeted the stolen items for the personal information they contained" and that "the thieves [would] then select, from thousands of others, the personal information of the named plaintiffs and attempt successfully to use that information to steal their identities." *Id.* at 274, 275. The court then rejected the plaintiffs' second theory of standing as "a repackaged version" of the first, noting that "costs . . . incurred in response to a speculative threat" cannot confer standing. *Id.* at 276–77 (quotation marks omitted).

To be sure, this case differs from *Beck* in that the Non-Misuse Plaintiffs were victims of a ransomware attack, meaning there is no need to speculate whether their PII was "intentionally targeted." *Id.* at 274. Even so, the court concludes their risk of future injury depends on a similarly "attenuated chain of possibilities," *Clapper*, 568 U.S. at 410, and "speculation about the decisions of independent actors," *id.* at 414. The risk of the Non-Misuse Plaintiffs becoming victims of identity theft rests on speculation that Nitrogen will carry out its threat to sell or release the stolen data; that another wrongdoer will locate the data on the dark web and acquire it; that this unknown third party will decide to misuse the data rather than merely trade or sell it; and that this actor — or someone else who later acquires the data — will single out these four Plaintiffs' information

from among the 240,000 victims, attempt to commit identity theft, and actually succeed.[3] Only if all these contingencies occur would the harm the Non-Misuse Plaintiffs fear materialize.

The complaint implicitly acknowledges this uncertainty. It notes "[s]tolen PII trades on the black market for years," ECF No. 19 ¶ 167, and asserts "fraudulent activity resulting from the [d]ata [b]reach may not come to light for years," *id.* ¶ 50; *see also id.* ¶ 169 ("It can take victims years to spot identity or PII theft."). The court struggles to see how an injury that may or may not occur years from now, depending on the actions of third parties, can be described as "certainly impending." *See, e.g.*, *Green v. eBay Inc.*, No. 14–1688, 2015 WL 2066531, at *5 (E.D. La. May 4, 2015) (finding no "certainly impending" risk of harm where the complaint stated the bad actor who possessed the plaintiff's personal information "may hold the information for later use[] or continue to sell it between identity thieves" and the plaintiff and other class members would need to "be vigilant for many years in checking for fraud" (emphasis omitted)); *In re Zappos.com, Inc.*, 108 F. Supp. 3d 949, 959 (D. Nev. 2015) ("The possibility that the alleged harm could transpire in the as-of-yet undetermined future relegates Plaintiffs' injuries to the realm of speculation."); *see also Dinerstein v. Google, LLC*, 73 F.4th 502, 512 (7th Cir. 2023) ("[A] plaintiff who has not suffered a past harm cannot simply rest on allegations that he may suffer some 'possible future

[3] The complaint does not allege Nitrogen, a known ransomware group, has used or is likely to use Plaintiffs' PII to commit identity theft itself. Rather, it asserts Nitrogen "issued a ransom demand to [SRP]" and "intends to release all stolen information obtained from the [b]reach on its data leak page." ECF No. 19 ¶¶ 39–40. The complaint also attaches a screenshot of a webpage purportedly associated with Nitrogen that lists data acquired in the SRP breach for sale for $400,000. *Id.* ¶ 39.

injury,' 'at some indefinite future time.' (citation omitted) (first quoting *Whitmore v. Arkansas*, 495 U.S. 149, 158 (1990); and then quoting *Lujan*, 504 U.S. at 564 n.2)).

Nor is the court convinced the Non-Misuse Plaintiffs have plausibly alleged a "substantial risk" of future identity theft. *Clapper*, 568 U.S. at 414 n.5. The *Beck* court dismissed the allegation that "33% of health-related data breaches result in identity theft" as "insufficient to establish a 'substantial risk' of harm." 848 F.3d at 275. "Even if we credit the Plaintiffs' allegation that 33% of those affected by [the] data breaches will become victims of identity theft," the court reasoned, "it follows that over 66% of veterans affected will suffer no harm. This statistic falls far short of establishing a 'substantial risk' of harm." *Id.* at 275–76. If a 33% risk of identity theft was insufficient in *Beck*, then the Non-Misuse Plaintiffs' failure to allege any facts quantifying the likelihood of harm they face is necessarily fatal here. *See Podroykin v. Am. Armed Forces Mut. Aid Ass'n*, 634 F. Supp. 3d 265, 271 (E.D. Va. 2022) (finding no "substantial risk" of harm because the plaintiff did "not proffer any statistics to allege a high risk of identity theft following a ransomware attack" and "even if [he] did allege statistics regarding the chance of identity theft after a ransomware attack, a 33% chance would be insufficient").

In sum, the complaint does not plausibly plead that the Non-Misuse Plaintiffs face a "substantial risk" of future identity theft or that such harm is "certainly impending."[4]

[4] The court does not credit the Non-Misuse Plaintiffs' "on information and belief" allegation that their "PII has already been published — or will be published imminently — by cybercriminals on the Dark Web." ECF No. 19 ¶¶ 71, 127, 141, 153. "Pleading on the basis of information and belief is generally appropriate" when the information at issue is "particularly within [the defendant's] knowledge and control." *Boykin v. KeyCorp.*, 521 F.3d 202, 215 (2d Cir.
(Continued)

Consequently, their mitigation efforts and expenses cannot satisfy the injury-in-fact requirement. *See, e.g.*, *Beck*, 848 F.3d at 276–77; *Remijas v. Neiman Marcus Grp., LLC*, 794 F.3d 688, 694 (7th Cir. 2015) ("Mitigation expenses do not qualify as actual injuries where the harm is not imminent."); *Tsao v. Captiva MVP Rest. Partners, LLC*, 986 F.3d 1332, 1345 (11th Cir. 2021) ("Tsao cannot conjure standing here by inflicting injuries on himself to avoid an insubstantial, non-imminent risk of identity theft.").

3. Loss of Privacy

Plaintiffs also allege they have suffered "actual injury from the exposure of [their] PII — which violates [their] rights to privacy." ECF No. 19 ¶¶ 74, 88, 102, 116, 130, 144, 156. As mentioned, an intangible harm can qualify as a concrete injury if it bears "a 'close relationship' to a harm traditionally recognized as providing a basis for a lawsuit in American courts." *TransUnion*, 594 U.S. at 417 (citing *Spokeo*, 578 U.S. at 340–41). Although an "exact duplicate" is not required, "plaintiffs [must] identif[y] a close historical or common-law analogue for their asserted injury." *Id.* at 424.

Here, Plaintiffs rely on a generalized "invasion of privacy" theory. ECF No. 40 at 17 (arguing only that their "loss of privacy is a cognizable injury"). But "an 'invasion of privacy' is not a standalone tort." *Dinerstein*, 73 F.4th at 513. Rather, "the term encompasse[s] four theories

2008); *Lincoln Benefit Life Co. v. AEI Life, LLC*, 800 F.3d 99, 107 n.31 (3d Cir. 2015) ("Several Courts of Appeals accept allegations 'on information and belief' when the facts at issue are peculiarly within the defendant's possession."). But here, there is no reason why SRP would be in a unique position to know whether a particular Plaintiff's PII has been posted for sale on the dark web.

of wrongdoing: intrusion upon seclusion, appropriation of a person's name or likeness, publicity given to private life, and publicity placing a person in a false light." *Id.* (internal quotation marks and emphasis omitted); *Popa v. Microsoft Corp.*, __ F.4th __, 2025 WL 2448824, at *6 (9th Cir. Aug. 26, 2025) ("[T]here existed no free-roaming privacy right at common law but rather four discrete torts that protected specific kinds of privacy-related harms."); Restatement (Second) of Torts § 652A cmt. b ("As it has developed in the courts, the invasion of the right of privacy has been a complex of four distinct wrongs . . . .").

Because Plaintiffs have not identified which of these four torts their alleged injury most closely resembles, they have failed to carry their burden of establishing standing based on a loss of privacy. Without a proposed common-law analogue, the court cannot properly assess whether their asserted privacy injury supports standing. *See, e.g.*, *Dinerstein*, 73 F.4th at 513 ("*TransUnion* requires us to nail down a particular common-law analogue . . . ."); *Popa*, 2025 WL 2448824, at *5 ("*TransUnion* contemplates a standing inquiry particularized to a plaintiff's circumstances and benchmarked to a specific tort . . . ."); *see also TransUnion*, 594 U.S. at 434 n.6 (explaining a theory that "circumvents a fundamental requirement" of an analogous common-law tort "does not bear a sufficiently 'close relationship'" to the comparator tort).

4. Emotional Distress

Next, Plaintiffs allege they have experienced "feelings of anxiety, stress, fear, and frustration because of the [d]ata [b]reach." ECF No. 19 ¶¶ 77, 91, 105, 119, 133, 147, 159. The Supreme Court has not yet taken a "position on whether or how . . . an emotional or psychological harm could suffice for Article III purposes." *TransUnion*, 594 U.S. at 436 n.7. The Fourth Circuit,

however, has spoken on the issue. In *Beck*, it held that claims of "emotional upset" and "fear [of] identity theft and financial fraud" stemming from the data breaches were insufficient to establish Article III standing. 848 F.3d at 272–73 (rejecting "the proposition that bare assertions of emotional injury are sufficient to confer Article III standing"). Consistent with *Beck*, Plaintiffs' allegations of emotional distress cannot give rise to standing. *See Stuart v. Kyocera Avx Components Corp.*, 769 F. Supp. 3d 476, 489 (D.S.C. 2025); *Holmes v. Elephant Ins. Co.*, No. 3:22cv487, 2023 WL 4183380, at *5 (E.D. Va. June 23, 2023).

5. Decreased Value of PII

Plaintiffs further allege they have suffered "actual injury in the form of damages to and diminution in the value of [their] PII" as a result of the data breach. ECF No. 19 ¶¶ 75, 89, 103, 117, 131, 145, 157.

This theory of standing also fails because, even assuming there exists some legitimate market that gives PII intrinsic economic value, Plaintiffs allege no facts showing they ever intended to sell their PII or that such information would now fetch a lower price. *See, e.g.*, *Chambliss v. CareFirst, Inc.*, 189 F. Supp. 3d 564, 572 (D. Md. 2016) (finding no injury in fact where plaintiffs "ha[d] not alleged that they ha[d] attempted to sell their personal information" or that "the data breach forced them to accept a decreased price for that information"); *In re Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig.*, 45 F.Supp.3d 14, 30 (D.D.C. 2014) ("Plaintiffs do not contend that *they* intended to sell [their personal and medical] information on the cyber black market in the first place, so it is uncertain how they were injured by this alleged

loss. Even if the service members did intend to sell their own data — something no one alleges — it is unclear whether or how the data has been devalued by the breach.").

Accordingly, Plaintiffs have failed to plausibly allege an injury in fact based on any diminution of the value of their personal information.

6. Increased Spam Communications

Finally, Plaintiffs (with the exception of Plaintiff Whitfield) contend they have experienced "a significant increase" in spam calls, text messages, and emails since the data breach. ECF No. 19 ¶¶ 79, 93, 107, 121, 135, 161.

"Spam calls, texts, and e-mails have become very common in this digitized world, and a number of courts have declined to confer standing when considering an increase in spam communications." *McCombs v. Delta Grp. Elecs., Inc.*, 676 F. Supp. 3d 1064, 1074 (D.N.M. 2023) (collecting cases); *see also, e.g.*, *Jenkins*, 2025 WL 708574, at *6 ("Spam calls are annoying. But an annoyance isn't an actual and concrete injury."); *Williams v. Bienville Orthopaedic Specialists, LLC*, 737 F. Supp. 3d 411, 421 (S.D. Miss. 2024) ("Fendley's allegation of an increase in spam phone calls is insufficient to establish an injury in fact."); *Johnson v. Yuma Reg'l Med. Ctr.*, 769 F. Supp. 3d 936, 950 (D. Ariz. 2024) ("On its own, receiving spam or mass mail does not constitute an injury." (internal quotation marks omitted)).

Even if the court were to depart from this consensus and conclude the receipt of unwanted spam communications constitutes an injury in fact, Plaintiffs still fail to show traceability. None of the data-breach notices sent to Plaintiffs indicate their phone numbers or email addresses were compromised, and they acknowledge "their contact information was not included in the PII

accessed." ECF No. 40 at 20. For this reason, Plaintiffs cannot establish standing based on an alleged increase in spam communications. *See, e.g.*, *Negron v. Ascension Health*, No. 4:24-CV-00669-JAR, 2025 WL 2710014, at *6 (E.D. Mo. Sept. 23, 2025) (holding "alleged injuries in the form of spam calls, texts, and emails [were] not fairly traceable to [the defendant]" because "[p]hone numbers and email addresses weren't identified in the pleadings or public notices as types of PII compromised in the breach").

* * *

Of the seven Plaintiffs, only Plaintiffs McGrier, Chase, and Black have plausibly alleged an injury in fact sufficient to support a claim for damages. The court next considers whether these injuries can be fairly traced to the SRP data breach.

B. Traceability

The traceability element of standing "examines the causal connection between the assertedly unlawful conduct and the alleged injury." *Allen v. Wright*, 468 U.S. 737, 753 n.19 (1984). It "asks whether the [plaintiff's] injury is 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." *Steel Co.*, 523 U.S. at 106 n.7 (cleaned up). Article III does not demand "a tort-like showing of proximate causation," *Conservation L. Found., Inc. v. Acad. Express, LLC*, 129 F.4th 78, 90 (1st Cir. 2025) (citing *Lexmark Int'l, Inc. v. Static Control Components, Inc.*, 572 U.S. 118, 134 n.6 (2014)), but "[a] plaintiff must at least demonstrate *factual* causation between his injuries and the defendant's misconduct," *Walters v. Fast AC, LLC*, 60 F.4th 642, 650 (11th Cir. 2023) (emphasis in original); *see, e.g.*, *Warth v. Seldin*, 422 U.S. 490, 505 (1975) (holding Article III requires

plaintiffs "to establish that, in fact, the asserted injury was the consequence of the defendants' actions"); *Duke Power Co. v. Carolina Env't Study Grp., Inc.*, 438 U.S. 59, 74–78 (1978) (holding "a 'but for' causal connection" satisfies the traceability requirement).

The "fact-dependent" nature of the traceability requirement can make it difficult to evaluate at the motion-to-dismiss stage. *All. for Hippocratic Med.*, 602 U.S. at 384. This is especially true in the data-breach context. As one district court has observed, "[A]n individual's [personal information] can be stolen in myriad ways, often without the individual's knowledge. Data breaches and other forms of data theft are so prevalent that it is seemingly impossible to trace the misuse of personal information to one particular breach." *Williams*, 737 F. Supp. 3d at 425. Still, a review of standing decisions in data-breach cases reveals a few guiding principles.

First, because traceability "logically requires a temporal element," *Hulse v. Acadian Ambulance Serv. Inc.*, No. 6:24-CV-01011, 2025 WL 1453847, at *10 (E.D. La. May 19, 2025), a plaintiff must, at the very least, allege when his or her PII was misused in relation to the breach. Most obviously, "allegations of actual misuse that predate the disclosure of the stolen information" cannot satisfy the traceability requirement. *In re MOVEit Customer Data Sec. Breach Litig.*, MDL No. 1:23-md-03083-ADB-PGL, 2024 WL 5092276, at *12 (D. Mass. Dec. 12, 2024). Similarly, "the more time that passes between a data breach and an instance of identity theft, the more latitude a defendant has to argue that the identity theft is not 'fairly traceable' to the defendant's data breach." *Remijas*, 794 F.3d at 693 (quoting *In re Adobe Sys., Inc. Privacy Litig.*, 66 F. Supp. 3d 1197, 1215 n.5 (N.D. Cal. 2014)). By contrast, courts are more likely to find standing when there is a close temporal connection between a data breach and the misuse of a plaintiff's PII. *See, e.g.*,

Webb v. Injured Workers Pharm., LLC, 72 F.4th 365, 374 (1st Cir. 2023) (finding "an obvious temporal connection" between a January 2021 data breach and the filing of a false tax return a year later); *Roper v. Rise Interactive Media & Analytics, LLC*, No. 23 CV 1836, 2023 WL 7410641, at *5 (N.D. Ill. Nov. 9, 2023) (finding traceability adequately pled where one plaintiff alleged that "an unknown party attempted to use her personal information to open a bank account" within three months of a data breach).[5]

Second, to establish traceability, a plaintiff must also allege that the type of information misused "matches" the type of information exposed in the breach. *Santos-Pagan v. Bayamón Med. Ctr.*, No. 20-1237 (BJM), 2024 WL 4350990, at *6 (D.P.R. Sept. 30, 2024). That is, "they must allege facts that indicate that the information stolen . . . is the same type of information used to commit their injuries." *Welborn v. Internal Revenue Serv.*, 218 F. Supp. 3d 64, 79 (D.D.C. 2016). Courts consistently "reject[] traceability arguments when the information needed to commit the alleged identity theft was not obtained in the data breach." *In re Samsung Data Sec. Breach Litig.*, 761 F. Supp. 3d 781, 800 (D.N.J. 2024); *see, e.g.*, *DiPierro v. Fla. Health Scis. Ctr., Inc.*, 737 F. Supp. 3d 1314, 1330 (M.D. Fla. 2024) ("Without additional factual allegations to bridge the gap,

[5] *But see, e.g.*, *Williams*, 737 F. Supp. 3d at 425 ("The mere fact that [plaintiffs] experienced misuse of their PII or learned that some of their PII had been stolen after the data breach is insufficient to show that the misuse of their PII is fairly traceable to the Bienville data breach."); *Masterson v. IMA Fin. Grp., Inc.*, No. 2:23-cv-02223-HLT-ADM, 2023 WL 8647157, at *4 (D. Kan. Dec. 14, 2023) ("The only link between the data breach and the claimed misuse is that the misuse came after the data breach. This does not allege a 'substantial likelihood' that the data breach caused the misuse."); *Malinowski v. Int'l Bus. Machs. Corp.*, 23-cv-8421 (NSR), 2025 WL 965812, at *4 (S.D.N.Y. Mar. 31, 2025) (finding no traceability where plaintiffs "only offer[ed] a correlation — that is, after the Data Breach [they] experienced the adverse actions").

James has not plausibly alleged how any of the potentially stolen information could fairly cause the $2,600 unauthorized charge to his bank account or the two $400 ATM withdrawals."); *Blood v. Labette Cnty. Med. Cntr.*, No. 5:22-cv-04036-HLT-KGG, 2022 WL 11745549, at *5 (D. Kan. Oct. 20, 2022) ("The Bloods allege they suffered unauthorized charges to their bank account. But they do not plead any facts suggesting how the mere possession of their Social Security numbers and names would enable someone to make unauthorized charges on an existing account (instead of, for example, opening a new account)."); *Burger v. Healthcare Mgmt. Sols., LLC*, No. RDB-23-1215, 2024 WL 473735, at *6 (D. Md. Feb. 7, 2025) ("[E]ven taking Burger's allegations as true, unauthorized charges on her credit card cannot be fairly traced to either of the defendants. Burger does not allege that her credit card information itself was disclosed; she alleges only that her bank account information was disclosed.").

Applying these principles here, the court concludes the complaint, as currently pleaded, fails to adequately allege traceability. According to the complaint, Plaintiff McGrier "suffered a number of fraudulent charges on her SRP account," which "forc[ed] her to open a new account and get a new card," ECF No. 19 ¶ 90; Plaintiff Chase "has flagged multiple unauthorized charges on his accounts associated with SRP," *id.* ¶ 104; and Plaintiff Black "ultimately clos[ed] his SRP account and open[ed] another due to various fraudulent charges," *id.* ¶ 118. For all three Plaintiffs, however, the complaint does not specify when the charges were made, leaving it unclear whether they are plausibly linked to the SRP breach.

Further, the complaint does not provide sufficient detail to "allow[] the court to draw the reasonable inference" that the disclosed information could have facilitated the fraudulent charges.

Ashcroft v. Iqbal, 556 U.S. 662, 678 (2009). The complaint does not allege what type of accounts were affected (e.g., checking, savings, or credit card), and although the data-breach notices sent to the three Plaintiffs indicate their "financial account number" was possibly exposed, ECF No. 19-2 at 3, 4, 9, an account number alone — without an associated routing number, debit card number, or PIN — generally cannot be used to initiate unauthorized withdrawals. Plaintiff McGrier's notice also indicates her credit card number may have been compromised, *id.* at 9, but the complaint does not specify whether the fraudulent charges were made on that card or on some other account.

In short, without allegations specifying when the charges were made and linking the information misused to the information disclosed in the breach, the court cannot say "it is both plausible and likely that [the] breach of [SRP's systems] resulted in the fraudulent use of the Plaintiff's personal information." *Hutton*, 892 F.3d at 623. Accordingly, Plaintiffs McGrier, Chase, and Black, like the four Non-Misuse Plaintiffs, lack standing to pursue money damages.

C. Standing for Injunctive Relief

Although not addressed by the parties in their briefing, the court next considers whether Plaintiffs have standing to seek injunctive relief. *See Davis v. Fed. Election Comm'n*, 554 U.S. 724, 734 (2008) ("Standing is not dispensed in gross. Rather, a plaintiff must demonstrate standing . . . for each form of relief that is sought." (cleaned up)). The complaint first seeks an injunction requiring SRP to "strengthen its data security systems and monitoring procedures" and to "conduct

periodic audits of those systems."[6] ECF No. 19 ¶ 218. "Naturally, an injunction requiring [SRP] to improve its cybersecurity systems cannot protect [Plaintiffs] from future misuse of their PII by the individuals they allege now possess it. Any such relief would safeguard only against a future breach." *Webb*, 72 F.4th at 378; *see also In re Progressive Leasing Breach Litig.*, No. 2:23-cv-00783-DBB-CMR, 2025 WL 213744, at *13 (D. Utah Jan. 16, 2025) ("Here, the complained of harm supporting an injunction is that Prog will experience another data breach and further compromise Plaintiffs' PII.").

Plaintiffs, however, offer no allegations to suggest the risk of a future data breach involving SRP's systems is "sufficiently imminent and substantial." *TransUnion*, 594 U.S. at 435. "The most that can be reasonably inferred from [their] allegations regarding the likelihood of another data breach . . . is that [they] *could* be victimized by a future data breach. That alone is not enough." *Beck*, 848 F.3d at 277–78 (emphasis in original).

Plaintiffs also request the court "[e]njoin[] [SRP] from further deceptive practices and making untrue statements about the [d]ata [b]reach and the stolen PII." ECF No. 19, Prayer for Relief. "But nowhere do [Plaintiffs] allege that [SRP] is likely to make deceptive statements about that past breach in the future or that any such statements would harm [them], particularly now that

[6] Paragraph 218 also requests the court order SRP to provide Plaintiffs with "lifetime credit monitoring and identity theft insurance." ECF No. 19 ¶ 218. But because this relief would entail no "more than an exchange of money," it cannot be considered "injunctive in nature." *Thomas v. FAG Bearings Corp.*, 846 F. Supp. 1400, 1404 (W.D. Mo. 1994); *see also Barraza v. C.R. Bard Inc.*, 322 F.R.D. 369, 387 (D. Ariz. 2017) ("[A] remedy requiring Defendants to do nothing more than write a check can[not] properly be viewed as an injunction.").

they know about the breach." *Webb*, 72 F.4th at 378. Thus, this "requested injunction would have no chance of redressing any alleged injury, and [Plaintiffs] lack standing to pursue it." *Id.*

D. Leave to Amend

When a district court finds it lacks subject-matter jurisdiction over a complaint for want of Article III standing, "it is within the trial court's power to allow . . . the plaintiff to supply, by amendment to the complaint or by affidavits, further particularized allegations of fact deemed supportive of . . . standing." *Warth*, 422 U.S. at 501. Because the traceability defects identified above could be cured through the pleading of additional facts, the court will grant Plaintiffs leave to amend their complaint. *See, e.g.*, *Hoang v. Bank of Am., N.A.*, 910 F.3d 1096, 1102–1103 (9th Cir. 2018) (explaining "[l]eave to amend can and should generally be given, even in the absence of such a request by the party," unless "the pleading could not possibly be cured by the allegation of other facts" (internal quotation marks omitted)); *see also United States ex rel. Nicholson v. Medcom Carolinas, Inc.*, 42 F.4th 185, 197 (4th Cir. 2022) ("[W]e have often described our Fourth Circuit policy as one to 'liberally allow amendment.'" (quoting *Galustian v. Peter*, 591 F.3d 724, 729 (4th Cir. 2010)).

IV. CONCLUSION

For the foregoing reasons, the court grants SRP's motion to dismiss (ECF No. 29) and dismisses the complaint without prejudice. *See S. Walk at Broadlands Homeowner's Ass'n v. OpenBand at Broadlands, LLC*, 713 F.3d 175, 185 (4th Cir. 2013) ("A dismissal for lack of standing . . . must be one without prejudice[.]"). Plaintiffs shall have thirty days from entry of this order to file an amended consolidated complaint. If they fail to do so, the court will enter a final

order at the end of the thirty-day period. *See Britt v. DeJoy*, 45 F.4th 790, 798 (4th Cir. 2022) (en banc) ("where the district court has indicated how much time the plaintiff has to amend her complaint — the district court shall issue a final order upon the expiration of that deadline").

IT IS SO ORDERED.

s/Cameron McGowan Currie
CAMERON MCGOWAN CURRIE
Senior United States District Judge

Columbia, South Carolina
October 9, 2025