

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

ELAINE MALINOWSKI, KRISTAL MIZE,
MICHELLE PETTIFORD, VANESSA HAYS,
DANIEL ROBERT BRAWNER, ROWDY JAMES
ALDRIDGE, JOSEPH TYLER HALEY, MARY
LEA KIRBY, MICHAEL WRIGHT, ANTHONY
HANNA, PATRICK CALHOUN, ANDREW ROSE,
individually, and on behalf of all other similarly
situated,

Plaintiffs,

-against-

INTERNATIONAL BUSINESS MACHINES
CORPORATION and JOHNSON & JOHNSON
HEALTH CARE SYSTEMS, INC.,

Defendants.

No. 23-CV-8421 (NSR)

OPINION & ORDER

NELSON S. ROMÁN, United States District Judge:

Plaintiffs Elaine Malinowski (“Malinowski”), Kristal Mize (“Mize”), Michelle Pettiford (“Pettiford”), Vanessa Hays (“Hays”), Daniel Robert Brawner (“Brawner”), Rowdy James Aldridge (“Aldridge”), Joseph Tyler Haley (“Haley”), Mary Lea Kirby (“Kirby”), Michael Wright (“Wright”), Anthony Hanna (“Hanna”), Patrick Calhoun (“Calhoun”) and Andrew Rose (“Rose”) (together, “Plaintiffs”) bring this action against Defendants International Business Machines Corporation (“IBM”) and Johnson & Johnson Health Care Systems, Inc., (“J&J”) (together, “Defendants”). Plaintiffs bring claims of negligence, negligence *per se*, breach of implied contract, breach of fiduciary duty, breach of third-party beneficiary contract, unjust enrichment, violations of the Illinois Consumer Fraud and Deceptive Business Practices Act, violations of the California Consumer Privacy Act, violations of the California Confidentiality of Medical Information Act,

and violations of the California Unfair Competition Law.

Presently before the Court is Defendants' Motion to Dismiss Plaintiffs' Amended Consolidated Complaint (the "ACC") pursuant to Federal Rule of Civil Procedure 12(b)(6). For the following reasons, Defendants' Motion is GRANTED.

BACKGROUND¹

I. Factual Background

The following facts are derived from the ACC and are taken as true and construed in the light most favorable to Plaintiffs at this stage.

Defendant IBM is an information technology company that provides consulting, software, IT infrastructure, and other administrative and technical services to a wide range of clients, including Janssen. (ACC ¶ 32.) Janssen is owned and operated by Defendant J&J. (*Id.* ¶ 31.) Janssen CarePath ("CarePath") is a patient-support platform that helps patients research, manage, and find financial assistance for prescription medications. (*Id.*) IBM manages the CarePath application and the third-party database that supports it. (*Id.* ¶ 32.) To obtain medical services from Janssen, Defendants require that patients provide CarePath personally identifying information ("PII") consisting of names, contact information, and dates of birth, as well as personal health information ("PHI") consisting of health insurance information, and information about medications and medical conditions. (*Id.* ¶ 33.) PII and PHI are collectively referred to herein as "Personal Information."

In 2023, Janssen became "aware of a technical method by which unauthorized access to the [CarePath] database could be obtained" and notified IBM. (ECF No. 71-2, the "Notice

¹ The parties' briefs will be referred to herein as follows: Defendants' Memorandum of Law in Support of their Motion to Dismiss ("Dfts. Mem.," ECF No. 72); Plaintiffs' Memorandum of Law in Opposition to Defendants' Motion to Dismiss ("Pltfs. Opp. to Dfts.," ECF No. 73); Defendants' Reply in Support of their Motion to Dismiss ("Dfts. Reply," ECF No. 74).

Letter.”)² On August 2, 2023, IBM identified that “there was unauthorized access to personal information in the database” but they were “unable to determine the scope of that access” (the “Data Breach”). (*Id.*) On September 15, 2023, IBM notified Plaintiffs about “a recent incident that may have involved unauthorized access to your personal information stored in Janssen CarePath.” (Notice Letter) The Notice Letter stated, “[y]our Social Security number and financial account information were not contained in the database or affected.” (*Id.*)

Plaintiffs allege that, as a result of the Data Breach, they have suffered unauthorized disclosure of their Personal Information; actual, imminent and substantial risk of current and future identity theft and fraud; and other concrete harms resulting from the Data Breach, including mitigation expenses, lost time, and emotional damages. (ACC ¶ 111.) Plaintiffs additionally attribute a number of adverse events (the “Post-Breach Adverse Events”) to the Data Breach. For example, Plaintiffs Malinowski, Mize, Hays, Brawner, Aldridge, Haley, Kirby, Pettiford, Wright, Hanna, Calhoun also allege receiving spam calls, texts and/or emails, which they attribute to the Data Breach. (*Id.* ¶¶ 169, 181, 193, 205, 217, 229, 241, 253, 265, 277, 289.) Plaintiff Malinowski alleges that her credit reports reflected attempts to open store and credit cards in her name. (*Id.* ¶ 169.) Plaintiff Haley alleges that accounts were opened using his email address at Victoria’s Secret and Walmart, that someone accessed and used his UPS account to send a package to an unknown address, and that he discovered several charges to his accounts originating from locations he does not frequent. (*Id.* ¶ 229.) Plaintiffs Kirby, Wright and Calhoun allege that they experienced fraudulent credit-card charges. (*Id.* ¶ 241, 265, 289.) Plaintiffs Mize, Pettiford, Wright and Calhoun allege that they were informed that their PII had been published on the dark web. (*Id.* ¶¶ 181, 253,

² Though Plaintiffs do not include a copy of the Notice Letter in the ACC, the Second Circuit “deem[s] a complaint to include any written instrument attached to it as an exhibit or any statements or documents incorporated in it by reference.” *Rothman v. Gregor*, 220 F.3d 81, 88 (2d Cir. 2000) (internal citations omitted). As the Notice Letter is mentioned throughout the ACC, the Court deems the Notice Letter to be incorporated by reference.

265, 289.) Plaintiffs Wright and Calhoun allege receiving threatening emails identifying their health insurer and medical conditions. (*Id.* ¶¶ 265, 289.)

II. Procedural History

Plaintiffs commenced this action on September 22, 2023. (ECF No. 1.) Thereafter, on January 18, 2024, Plaintiffs filed a Consolidated Complaint. (ECF No. 22.) On April 30, 2024, Defendants filed their motion to dismiss Plaintiffs' Consolidated Complaint and their memorandum of law in support (ECF Nos. 50, 52.) On the same day, Plaintiffs filed their opposition to Defendants' motion to dismiss, and Defendants filed their reply in further support of their motion to dismiss (ECF Nos. 53, 54.) On March 31, 2025, the Court dismissed Plaintiffs' claims for lack of standing, but granted Plaintiffs leave to file an amended pleading. (ECF No. 60.)

On May 15, 2025, Plaintiffs filed the ACC, which is the operative pleading. (ECF No. 61.) On September 2, 2025, Defendants filed their motion to dismiss, supporting memorandum of law, and reply papers. (ECF Nos. 70, 72, 74.) That same day, Plaintiffs filed their opposition to Defendants' motion. (ECF No. 73.)

LEGAL STANDARD

I. Rule 12(b)(1)

Under Federal Rule of Civil Procedure 12(b)(1), “[a] case is properly dismissed for lack of subject matter jurisdiction . . . when the district court lacks the statutory or constitutional power to adjudicate it.” *Nike, Inc. v. Already, LLC*, 663 F.3d 89, 94 (2d Cir. 2011) (citation and internal quotations omitted). “A plaintiff asserting subject matter jurisdiction has the burden of proving by a preponderance of the evidence that it exists.” *Morrison v. Nat’l Australia Bank Ltd.*, 547 F.3d 167, 170 (2d Cir. 2008) (quoting *Makarova v. U.S.*, 201 F.3d, 110, 113 (2d Cir. 2000)). In assessing whether subject matter jurisdiction exists, the Court must accept as true all material facts alleged

in the complaint. *Conyers v. Rossides*, 558 F.3d 137, 143 (2d Cir. 2009). Nevertheless, even “on a motion to dismiss, courts ‘are not bound to accept as true a legal conclusion couched as a factual allegation.’” *Sharkey v. Quarantillo*, 541 F.3d 75, 83 (2d Cir. 2008).

II. Rule 12(b)(6)

Under Federal Rule of Civil Procedure 12(b)(6), dismissal is proper unless the complaint “contain[s] sufficient factual matter, accepted as true, to ‘state a claim to relief that is plausible on its face.’” *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007)). When there are well-pled factual allegations in the complaint, “a court should assume their veracity and then determine whether they plausibly give rise to an entitlement to relief.” *Id.* at 679. While the Court must take all material factual allegations as true and draw reasonable inferences in the non-moving party’s favor, the Court is “not bound to accept as true a legal conclusion couched as a factual allegation,” or to credit “mere conclusory statements” or “[t]hreadbare recitals of the elements of a cause of action.” *Id.* at 678 (quoting *Twombly*, 550 U.S. at 555). The critical inquiry is whether the Plaintiff has pled sufficient facts to nudge the claims “across the line from conceivable to plausible.” *Twombly*, 550 U.S. at 570. A motion to dismiss will be denied where the allegations “allow[] the court to draw the reasonable inference that the Defendant is liable for the misconduct alleged.” *Iqbal*, 556 U.S. at 678.

DISCUSSION

In the ACC, Plaintiffs bring claims of negligence, negligence *per se*, breach of implied contract, breach of fiduciary duty, breach of third-party beneficiary contract, unjust enrichment, violations of the Illinois Consumer Fraud and Deceptive Business Practices Act, violations of the California Consumer Privacy Act, violations of the California Confidentiality of Medical

Information Act, and violations of the California Unfair Competition Law.³ The Court finds that Plaintiffs lack standing to prosecute such claims and therefore confines its discussion to the Article III standing analysis.⁴

I. Standing

Standing is “the threshold question in every federal case” and implicates the Court’s subject matter jurisdiction. *Ross v. Bank of America, N.A.*, 524 F.3d 217, 222 (2d Cir. 2008) (“Standing is the threshold question in every federal case, determining the power of the court to entertain the suit.”) (citing *Denney v. Deutsche Bank AG*, 443 F.3d 253, 263 (2d Cir. 2006)). “[T]he irreducible constitutional minimum of standing [in federal court] contains three elements”: injury, traceability, and redressability. *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 560 (1992). “First, the plaintiff must have suffered an ‘injury in fact’— an invasion of a legally protected interest which is (a) concrete and particularized, and (b) actual or imminent, not conjectural or hypothetical.” *Id.* (internal quotations and citations omitted). “Second, there must be a causal connection between the injury and the conduct complained of—the injury has to be ‘fairly . . . trace[able] to the challenged action of the defendant, and not . . . th[e] result [of] the independent action of some third party not before the court.’” *Id.* at 560–61 (quoting *Simon v. Eastern Ky. Welfare Rights Org.*, 426 U.S. 26, 41–42, (1976)). “Third, it must be likely, as opposed to merely speculative, that the injury will be redressed by a favorable decision.” *Lujan*, 504 U.S. at 561 (internal quotation and citation omitted).

Plaintiffs advance three principal categories of injury: “(1) unauthorized access and

³ Although the ACC asserts a claim under the Florida Unfair and Deceptive Trade Practices Act, Plaintiffs withdraw the claim in their opposition brief. (Pltfs. Opp. to Dfts. at 24, n. 3.)

⁴ Plaintiffs’ addition of a new Plaintiff, Andrew Rose, who brings claims under the California Consumer Privacy Act, the California Confidentiality of Medical Information Act, and the California Unfair Competition Law does not warrant a separate standing analysis. “For standing purposes, . . . an important difference exists between (i) a plaintiff’s statutory cause of action to sue a defendant over the defendant’s violation of federal law, and (ii) a plaintiff’s suffering concrete harm because of the defendant’s violation of federal law . . . an injury in law is not an injury in fact.” *TransUnion LLC v. Ramirez*, 594 U.S. 413, 426-27 (2021). Plaintiffs must still show they have suffered a concrete injury, and Plaintiffs have not done so in the instant case.

disclosure of their Personal Information; (2) actual, imminent and substantial risk of current and future identity theft and fraud; and (3) other concrete harms resulting from the Data Breach, including mitigation expenses, lost time, and emotional damages.” (Pltfs. Opp. to Dfts. at 4.) Although the Court’s prior Order dismissed the Consolidated Complaint for failure to adequately plead traceability, (ECF No. 60), the Court’s past analysis principally addressed whether certain Post-Breach Adverse Events—including unauthorized accounts, fraudulent charges, dark-web publication, threatening emails, and increased spam—could plausibly be attributed to the Data Breach. (*Id.*) The ACC and the parties’ briefing now place that question before the Court. Accordingly, the Court considers each of Plaintiffs’ principal theories of injury in turn and, where necessary, whether the asserted injury is fairly traceable to Defendants.

A. Unauthorized Access and Disclosure of Personal Information

Plaintiffs argue that “[t]he admitted unauthorized disclosure of Plaintiffs’ Personal Information is a concrete injury sufficient to confer Article III standing here.” (Pltfs. Opp. to Dfts. at 4.) In *TransUnion LLC v. Ramirez*, the Supreme Court identified the “disclosure of private information” as an intangible harm traditionally recognized as providing a basis for standing. 594 U.S. 413, 425 (2021). Applying *TransUnion* in the data-breach context, the Second Circuit in *Bohnak* held that exposure of a plaintiff’s private information to an unauthorized actor *may* itself constitute a concrete injury because that harm bears a close relationship to the traditionally recognized tort of public disclosure of private facts. *Bohnak v. Marsh & McLennan Companies, Inc.*, 79 F.4th 276, 285–86 (2d Cir. 2023) (emphasis added). Plaintiffs invoke that principle here, arguing that the alleged disclosure of their Personal Information establishes Article III injury. But *Bohnak* does not establish that the disclosure of information automatically confers standing. *See I.C. v. Zynga, Inc.*, 600 F. Supp. 3d 1034, 1050 (N.D. Cal. 2022) (“In data breach cases, courts

must examine the nature of the specific information at issue to determine whether privacy interests were implicated at all. Otherwise, every data breach (or any situation in which one loses control of information) would confer standing.”); *O’Leary v. TrustedID, Inc.*, 60 F.4th 240, 244 (4th Cir. 2023) (“Being subjected to a data breach isn’t in and of itself sufficient to establish Article III standing.”).

The information allegedly disclosed here is materially different from the information at issue in *Bohnak*. There, the Second Circuit emphasized that the plaintiff’s Social Security number had been exposed, describing Social Security numbers as “among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change.” *Bohnak*, 79 F.4th at 289. The other case Plaintiffs cite, *Miller*, also involved Social Security numbers and financial information. *Miller v. Syracuse*, 662 F.Supp.3d 338, 353 (N.D.N.Y. 2023). The information allegedly compromised here—names, dates of birth, health-insurance information, medications, and medical conditions—is undoubtedly personal. But Plaintiffs’ Social Security numbers and financial-account information were expressly not contained in the CarePath database. (ECF No. 71-2.) Plaintiffs therefore ask the Court to extend *Bohnak* beyond the particularly sensitive information at issue there and hold that unauthorized access to the materially different categories of information alleged here, standing alone, constitutes a concrete injury. Neither *Bohnak* nor the other authorities cited by Plaintiffs compel that conclusion. Accordingly, Plaintiffs have not established that the disclosure, without more, bears a sufficiently close relationship to the traditionally recognized harm identified in *Bohnak* to constitute a concrete injury in fact.

B. Actual Misuse of Stolen Information and Imminent Risk of Future Harm

Plaintiffs also allege “that they have suffered identity theft and fraud as a result of the Data

Breach and also allege that there is a real and substantial risk of the same harms occurring to Plaintiffs and putative class members in the future.” (Pltfs. Opp. to Dfts. at 6.) First, the ACC points to the Post-Breach Adverse Events as evidence that Plaintiffs already have suffered misuse of personal information: attempted openings of store or credit accounts; fraudulent credit-card charges; notices that certain Plaintiffs’ information appeared on the dark web; threatening emails purporting to know Plaintiffs’ health insurers and medical conditions; and increases in spam calls, texts, and emails. (ACC ¶¶ 169, 181, 193, 205, 217, 229, 241, 253, 265, 277, 289.)

Without reaching whether these alleged harms themselves constitute cognizable injuries in fact, the Post-Breach Adverse Events suffer from the same traceability defect the Court identified in dismissing the Consolidated Complaint. As the Court previously explained, “correlation is not tantamount to causation and, without more than mere correlation, a causal relationship cannot be established.” (ECF No. 60 at 8.) The Court suggested that “Plaintiffs can likely satisfy the traceability requirement of Article III standing if they only offer further factual averments that articulate a causal connection between the purported injuries and the Defendants’ conduct.” (*Id.* at 9.)

While Plaintiffs may have amended the Consolidated Complaint, Plaintiffs have failed to remedy the traceability issue that the Court previously identified with respect to the Post-Breach Adverse Events. The ACC does not add any new factual allegations that connect the Post-Breach Adverse Events to the Data Breach. The only purportedly “new” causal connection concerns Plaintiffs Wright and Calhoun, as to whom the ACC now asserts that their threatening emails “plainly referenced” the compromised dataset (ACC ¶ 140); but the underlying facts—that Plaintiffs Wright and Calhoun received threatening emails claiming knowledge of their health insurers and medical conditions, and that CarePath housed that information—were already alleged

in the Consolidated Complaint and considered by the Court in its prior traceability analysis (*Compare* ECF No. 22 ¶¶ 247, 271 *with* ECF No. 60 at 6-7.)

Plaintiffs’ repeated attribution of the Post-Breach Adverse Events to the Data Breach does not supply the missing causal connection. The ACC seeks to provide the causal link between the spam, fraudulent activity, dark-web postings, and the Data Breach by stating Plaintiffs “attribute[] [them] to the Data Breach.” (*See, e.g.*, ¶¶ 169, 181, 193, 205, 217, 229, 241, 253, 265, 277, 289.) However, as the Court previously pointed out, what remains absent are “factual allegations as to why such attribution is justified.” (ECF No. 60 at 8.) Plaintiffs’ mere assertion that the injuries suffered are attributable to Defendants serves as a “legal conclusion couched as a factual allegation,” which the Court is not bound to accept as true. *Sharkey*, 541 F.3d at 83.

The failure to plausibly trace the Post-Breach Adverse Events to the Data Breach does not necessarily foreclose Plaintiffs’ theory that the Data Breach creates a substantial risk of future medical identity theft. That theory, however, presents a distinct injury-in-fact inquiry. Under *McMorris v. Carlos Lopez & Associates, LLC*, the Second Circuit considers three non-dispositive factors in assessing whether exposure of personal information creates a sufficiently substantial risk of future identity theft: (1) whether the data was exposed as the result of a targeted attempt to obtain the plaintiffs’ information; (2) whether at least some portion of the compromised dataset has already been misused, even if the particular plaintiff’s information has not yet been affected; and (3) whether the nature of the exposed data makes future identity theft or fraud more likely. 995 F.3d 295, 301–03 (2d Cir. 2021).

The first factor does not support Plaintiffs. Plaintiffs characterize the Data Breach as a targeted attack undertaken for the purpose of obtaining Personal Information. (ACC ¶¶ 44, 46.) Plaintiffs rely on *Bohnak*, 79 F.4th 276, 285–86 (2d Cir. 2023), *In re Unite Here Data Security*

Incident Litigation, 740 F. Supp. 3d 364, 374 (S.D.N.Y. 2024) and *Sackin v. TransPerfect Global, Inc.*, 278 F.Supp.3d 739, 746 (S.D.N.Y. 2017) to support that inference. But those authorities involved clearer allegations of an intentional attack directed at highly sensitive identifying information, such as Social Security numbers or financial information. No such information is involved in the instant case.

The second *McMorris* factor—actual misuse of some portion of the compromised dataset—likewise does not materially favor Plaintiffs. Plaintiffs contend that the Post-Breach Adverse Events constitute actual misuse sufficient to move the risk of future identity theft beyond the speculative. (Pltfs. Opp. to Dfts. at 9.) But the relevant question under *McMorris* is not simply whether Plaintiffs experienced suspicious activity following the Data Breach; it is whether information compromised in the Data Breach was actually misused. That is where the traceability defect identified in the Court’s prior order remains significant. As this Court previously explained, temporal sequence alone does not establish that the Post-Breach Adverse Events were caused by this particular Data Breach. (ECF No. 60.)

The passage of time further undermines the asserted imminence of the future medical identity theft. Indeed, the ACC does not merely fail to allege that any named Plaintiff has suffered medical identity theft; it also fails to identify anyone whose information was compromised in the Data Breach who has actually suffered medical identity theft in the nearly two years that have passed between the Data Breach and the filing of the ACC. (*See* Dfts. Mem. at 10.) In *In re Practicefirst Data Breach Litigation*, 2022 WL 354544, at *5 (E.D.N.Y. Feb. 2, 2022), the court found the threatened harm insufficiently imminent where more than a year had passed without identity theft, and *Whalen v. Michaels Stores Inc.*, 153 F. Supp. 3d 577, 583 (E.D.N.Y. 2015) likewise reasoned that the passage of time without the predicted fraud weakens an assertion that

the threatened harm is immediate or substantial.

The third *McMorris* factor—the type of information exposed—ultimately also weighs against finding a substantial risk of future identity theft. The Second Circuit has recognized that “the nature of the data itself” may demonstrate that plaintiffs are not substantially at risk of identity theft. *McMorris*, 995 F.3d at 304 n.6. In the instant action, the compromised Personal Information includes dates of birth and information concerning health insurance, medications, and associated medical conditions. (ACC ¶ 43.) Plaintiffs cite *Fero* and *Webb* for the proposition that the “highly sensitive nature of the Personal Information in the Data Breach” heightens the risk of future misuse.⁵ (Pltfs. Opp. to Dfts. at 11.) However, *Webb* involved Social Security numbers, and *Fero* involved Social Security numbers and financial information. *Webb v. Injured Workers Pharmacy, LLC*, 72 F.4th 365, 376 (1st Cir. 2023); *Fero v. Excellus Health Plan, Inc.*, 304 F.Supp.3d 333, 341 (W.D.N.Y. 2018). As *Bohnak* emphasized, Social Security numbers pose a particular danger because of their utility for fraud and the difficulty of changing them. 79 F.4th at 281.

Here, Social Security numbers and financial account numbers were not contained in the CarePath database. Plaintiffs cite no cases that health-condition and insurance information, without accompanying Social Security numbers or financial information, is sensitive enough to create a substantial risk of future harm. Plaintiffs allege generally that criminals can combine the information exposed in one breach with information obtained elsewhere to create “Fullz” packages (ACC ¶¶ 134–36), and state conclusorily that the “Fullz” package process is “exactly what happened” to Wright and Calhoun. (*Id.* ¶ 140) However, the ACC alleges no facts showing that any actor actually combined CarePath data with information obtained elsewhere to create a “Fullz” package, on Wright, Calhoun or any other Plaintiff. Further, as the Second Circuit stated in

⁵ Plaintiffs’ citation to *In re Meta Pixel Healthcare Litig.*, 647 F. Supp. 3d 778, 792 (N.D. Cal. 2022) is unavailing as that case is unrelated to standing.

McMorris, even if the information disclosed put Plaintiffs “at a substantial risk of identity theft or fraud, in the absence of any other facts suggesting that the PII was intentionally taken by an unauthorized third party or otherwise misused, this factor alone does not establish an injury in fact.” *McMorris*, 995 F.3d at 304. As explained *supra* page 10-12, Plaintiffs have not alleged that the compromised data has been actually misused.

Considering the *McMorris* factors together, the ACC does not plausibly allege an imminent or substantial risk of future identity theft or fraud. Plaintiffs therefore cannot establish injury in fact based on the asserted future risk.

C. Other Harms, including Mitigation Expenses, Lost Time, and Emotional Damages

Plaintiffs also allege harms allegedly incurred in response to the breach, including “mitigation expenses incurred, lost time, and emotional damages.” (Pltfs. Opp. to Dfts. at 13; *see, e.g.*, ACC ¶¶ 171, 183, 195, 207, 219, 231, 243, 255, 267, 279, 291, 302.) Plaintiffs rely on *TransUnion*, *Maddox*, and *In re USAA* to argue that reasonable mitigation expenditures can themselves constitute present concrete harms where the plaintiff is responding to a substantial risk of identity theft. (Pltfs. Opp. to Dfts. at 13.) But as the Supreme Court articulated in *Clapper v. Amnesty International USA*, plaintiffs may not create Article III standing by incurring costs to protect themselves against a future injury that is not itself sufficiently imminent. 568 U.S. 398, 416 (2013); *see also Liau v. Weee!*, 2024 WL 729259, at *4-6 (S.D.N.Y. Feb. 22, 2024) (rejecting standing based on post-breach monitoring costs where the underlying threatened injury was insufficient); *De Medicis v. Ally Bank*, 2022 WL 3043669, at *10 (S.D.N.Y. Aug. 2, 2022) (“[I]n the absence of a substantial risk of future injury, Plaintiff’s allegations about the ‘time spent’ monitoring his accounts, ‘exploring credit monitoring and identity theft protection,’ . . . cannot

constitute a present injury in fact.”). The same is true of alleged emotional injuries in data breach cases. *See Maddox v. Bank of N.Y. Mellon Tr. Co. N.A.*, 19 F.4th 58, 66 (2d Cir. 2021) (noting that emotional distress or actions taken to prevent a risk that were “wholly incommensurate with the stimulant” are not enough to establish standing); *In re Practicefirst*, 2022 WL 354544, at *4 (finding that allegations of “great stress, mental anguish, and anxiety” were not sufficient to confer standing where the plaintiff did not allege an imminent or certainly impending risk of future harm).

For the reasons set forth *supra* section I.B., Plaintiffs have not plausibly alleged that they face an imminent or substantial risk of identity theft or fraud attributable to the Data Breach, and their efforts to guard against that speculative harm and any alleged emotional damages cannot independently supply Article III standing.

Plaintiffs’ remaining generalized economic injuries are similarly insufficient to confer standing. A diminution in the value of Personal Information is cognizable where the plaintiff plausibly alleges a market for that information and some actual diminution in his or her ability to use or sell it. *In re Practicefirst*, 2022 WL 354544, at *7 (finding no standing where “plaintiffs do not allege that they attempted to sell their personal information and were forced to accept a decreased price nor do they allege any details as to how their specific, personal information has been devalued because of the breach”); *Fero*, 236 F. Supp. 3d at 735 (holding that the mere allegation that data “commands a high price on the black market” is not sufficient to establish injury). While the ACC alleges that there is a market for personal information sold on the dark web, (ACC ¶¶ 147-52) Plaintiffs do not allege that they ever sought to sell or monetize their Personal Information, that the Data Breach impaired their ability to do so, or that they could now obtain less for their information than they could have before the Data Breach. Plaintiffs’ benefit-of-the-bargain theory is similarly deficient because use of CarePath was free and the ACC does

not allege that Plaintiffs exchanged consideration for a particular level of data security. *See In re Practicefirst*, 2022 WL 354544, at *8 n.11 (“The Court also rejects any attempt by plaintiffs to establish standing by alleging that they failed to receive the ‘benefit of their bargain’ by providing their private information to their medical providers, who then entrusted the data to defendants.”); *see also Aponte v. Northeast Radiology, P.C.*, 2022 WL 1556043, at *3 (S.D.N.Y. May 16, 2022) (“Plaintiffs do not allege any misuse or attempted misuse of their data resulting from the breach. Even if plaintiffs ‘lost some measure of privacy and that privacy was part of the bargain for medical services, [they] ha[ven’t] alleged any concrete harm from the alleged data breach.’”).

Accordingly, Plaintiffs’ mitigation expenses, lost time, opportunity costs, emotional distress, diminution-in-value theory, and related economic harms do not provide an independent basis for Article III standing.

CONCLUSION

For the foregoing reasons, Defendants’ motion to dismiss is GRANTED. Because Plaintiffs have already been afforded an opportunity to amend their standing allegations, and Plaintiffs neither request further leave to amend nor identify additional facts that could cure those deficiencies, the Court declines to grant further leave to amend. Accordingly, Plaintiffs’ Amended Consolidated Complaint is dismissed. The Clerk of Court is directed to terminate the motion at ECF No. 70 and to terminate this action.

Dated: September 17, 2026
White Plains, New York

SO ORDERED:



NELSON S. ROMÁN
United States District Judge