UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

In re Morgan Stanley Data Security Litigation	20-cv-5914 (AT)

ORAL ARGUMENT REQUESTED

MEMORANDUM OF LAW IN SUPPORT OF MORGAN STANLEY SMITH BARNEY LLC'S MOTION TO DISMISS

Paul, Weiss, Rifkind, Wharton & Garrison LLP
1285 Avenue of the Americas
New York, NY 10019
(212) 373-3000

2001 K Street NW
Washington, DC 20006
(202) 223-7300

Attorneys for Defendant

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

Other Authorities

Defendant Morgan Stanley Smith Barney LLC ("Morgan Stanley" or "the Company") respectfully submits this memorandum of law in support of its motion to dismiss the Second Consolidated Amended Complaint ("Complaint" or "SAC") (ECF No. 60) pursuant to Fed. R. Civ. P. 12(b)(1) or 12(b)(6).

PRELIMINARY STATEMENT

Plaintiffs drafted the SAC with the benefit of nearly nine months of discovery, during which they received 29,818 documents from Morgan Stanley and productions from 10 third parties, interviewed numerous witnesses, and took two depositions. Although plaintiffs have combed those materials to lard their amended pleading with innuendo, suggestions of impropriety, and blatant mischaracterizations, the SAC remains devoid of basic facts sufficient to support Article III standing or the necessary element of harm for each of plaintiffs' purported claims.

Despite all of plaintiffs' incendiary allegations, this case fundamentally arises out of events that did ***not*** involve the exposure of any personal or financial information in connection with a specific data breach, any malicious actors, a deliberate cyberattack, phishing or malware. Rather, this case arises out of two incidents that occurred in 2016 and 2019, respectively. The first involved computer equipment that Morgan Stanley's vendors were supposed to wipe and/or destroy; Morgan Stanley later discovered that certain devices still contained data when they left the vendor's control. The second relates to branch office computer equipment that was disconnected and replaced; after an inventory, Morgan Stanley was unable to locate a small number of those devices. Following in-depth investigations in consultation with internal and outside technical experts and continual monitoring for potential misuse of any data derived from any Morgan Stanley source, and despite the passage of years, Morgan Stanley has not become aware of a single instance of its customers' personally identifiable information ("PII") being accessed or misused in

connection with either event. On July 10, 2020, Morgan Stanley provided information regarding these two data security events to potentially impacted customers and to the state attorneys general. (*See* O'Brien Decl. Ex. 1, Consumer Notice of Data Breach (ECF 1-1) (hereinafter, "Consumer Notice") and O'Brien Decl. Ex. 2, Notice of Data Breach to State Attorney General (ECF 1-2).)[1]

On the heels of that notice, eight separate lawsuits were filed and later consolidated into the proceeding now before this Court. In their Complaint, named plaintiffs Mark Blythe, Richard and Cheryl Gamen, Howard Katz, Amresh Jaijee, Richard Mausner, John and Midori Nelson, Desiree Shapouri, Sylvia Tillman, and Vivian Yates—individuals residing in California, Florida, Illinois, New York, New Jersey, and Pennsylvania—purport to advance myriad common law and statutory claims arising out of these events on behalf of a putative class. However, their Complaint suffers from several fundamental and dispositive flaws that mandate dismissal.

First, the Complaint is (unsurprisingly) devoid of plausible allegations that any of plaintiffs' or the proposed class members' personal data was ever accessed or misused as a result of the data events, or any other cognizable injury. Thus, plaintiffs lack Article III standing to pursue any of their claims. None of the plaintiffs have alleged suffering any purported injury prior to June 2019, rendering any claims arising out of the 2016 incident purely speculative. Nor do any of the four theories advanced by plaintiffs establish a credible injury-in-fact with respect to either incident: (i) plaintiffs' allegations that they face injury due to the mere *possibility* of their data being misused are too attenuated to establish standing; (ii) plaintiffs fail plausibly to allege that the events diminished the value of their PII; (iii) their claim of standing based on so-called "out-of-pocket expenses" associated with the prevention of misuse of PII is deficient as a matter of law;

---

[1] Citations to "O'Brien Decl." refer to the Declaration of Jane O'Brien in Support of the Memorandum of Law in Support of Defendant's Motion to Dismiss, filed in support of this motion.

and (iv) plaintiffs' allegations that they suffered injuries in the form of annual fees or other similar payments to Morgan Stanley are too vague and conclusory to confer standing.

Second, the Complaint should be dismissed with prejudice for the independent reason that plaintiffs fail to state a claim under Fed. R. Civ. P. 12(b)(6). Each cause of action is deficient: (i) plaintiffs' negligence claims fail because they have not alleged that Morgan Stanley breached any general or specific duty of care, or that plaintiffs suffered any damages; (ii) their claim under New York's General Business Law § 349 fails because it is time-barred and is premised on nonactionable statements and, in any event, plaintiffs have not alleged injury; (iii) plaintiffs fail to plausibly allege a fiduciary duty that has been breached; (iv) the unjust enrichment claim is duplicative of plaintiffs' common law tort claims and fails to plausibly plead that Morgan Stanley was enriched at plaintiffs' expense; and (v) New York law does not recognize a claim for "breach of confidence" claim as pleaded by plaintiffs in the context of a data breach action; this claim also should be dismissed because plaintiffs have failed to adequately plead damages.

For these reasons and as set forth more fully below, the Complaint should be dismissed in its entirety and with prejudice.

STATEMENT OF FACTS

In 2016, Morgan Stanley decommissioned two data centers and contracted with a vendor—Triple Crown—to remove the devices from those centers, wipe any data that the devices may have contained, and recycle the non-data materials. (¶¶ 1, 32.)[2] Morgan Stanley later learned that Triple Crown unilaterally breached its contract by selling the devices to another company, AnythingIT, despite a requirement that Triple Crown only subcontract is obligations with Morgan Stanley's express written consent—which it did not obtain. (¶ 45.) Anything IT provided Triple Crown with

[2] Citations in the form "¶ __" are to paragraphs in the SAC.

certificates of indemnification, which Triple Crown then falsely described as certificates of destruction in transmitting them to Morgan Stanley. (¶ 112.) In reality, and unbeknownst to Morgan Stanley, Anything IT failed to wipe the devices, and sold them to a third party, KruseCom, which in turn either destroyed the devices or sold them online (¶ 51.) Nevertheless, Triple Crown fraudulently billed Morgan Stanley for destruction services.

Over a year later, on October 25, 2017, an Oklahoma-based IT consultant e-mailed Morgan Stanley's IT department, stating that he had found Morgan Stanley data on storage drives he purchased from KruseCom. (¶¶ 7(h), 131.) Morgan Stanley immediately took steps to investigate and recover the devices, and found no evidence that any customers' personal information was accessed or misused (the "2016 Data Center Event" or "2016 Event").

Separately, in 2019, Morgan Stanley removed and replaced approximately 500 Wide Area Application Services ("WAAS") devices from its local branch offices as part of a larger hardware refresh program. (¶¶ 157, 167.) In a subsequent inventory, the Company determined that it was unable to locate a small number of those devices; the manufacturer later informed Morgan Stanley of a software flaw that could have resulted in small amounts of previously deleted information remaining on the disks in unencrypted form (the "2019 WAAS Event" or "2019 Event"). (*Id.*)

Upon learning of each of these events, Morgan Stanley undertook thorough investigations, and worked with internal and outside technical experts to understand whether there was any potential risk to customer data. Morgan Stanley also has continuously monitored internet and "dark web" forums for any evidence of misuse of Morgan Stanley customer data and has not detected *any* unauthorized activity related to these incidents. The Company provided notice to customers and state attorneys' general of the 2016 and 2019 Events beginning on July 10, 2020.

Each of the named plaintiffs alleges that he or she received Morgan Stanley's July 2020 notice (¶¶ 59–67), but provides scant further detail of how each plaintiff purports to have been injured by the data events. Even after months of discovery, plaintiffs have been unable to improve on the conclusory and boilerplate allegations of harm asserted in their prior complaint. including that (i) they have been injured because they face impending data theft sometime in the future (¶¶ 269; 279; 290; 300; 312; 324; 333; 343; 353); (ii) the value of their PII has diminished, although there is no allegation as to what value their PII had to begin with, how either of the security events impacted the value of their PII in any way, or any efforts by plaintiffs to monetize their PII (¶¶ 267; 277; 288; 298; 310; 322; 331; 341; 351); (iii) they have experienced lost time, annoyance, interference, and inconvenience as a result the alleged data breach incidents (¶¶ 268; 278; 289; 299; 311; 323; 332; 342; 352); and (iv) they have made unspecified payments to Morgan Stanley (¶¶ 266; 276; 287; 297; 309; 321; 330; 340; 350).

For just five of the eleven named plaintiffs, the Complaint includes the following additional—still woefully insufficient—allegations:

- Mark Blythe alleges that, in July 2020 (conveniently after he received notice in this matter, but notably *years* after the events at issue), unauthorized third parties opened a checking account with a credit union in Mr. Blythe's name, applied for a Small Business Administration loan in his name, and opened a savings account in Mr. Blythe's name. (*Id.* ¶ 283.) There are *no* allegations tying these incidents to the 2016 or 2019 Events.

- Richard Gamen alleges that, in June 2020 (again, conveniently after he received notice in this matter, and again *years* after the events at issue), he began receiving scam telephone calls, which claim his Social Security number is "locked" and that he may be arrested. He has also alleged that he started receiving emails from fraudsters claiming a foreign person has died and the fraudster is reaching out to share the money. (¶ 305.) There are *no* allegations tying these incidents to the 2016 or 2019 Events.

- Amresh Jaijee alleges that, in June 2020 (a similarly convenient date), she received a telephone call from an individual claiming to represent an insurance company, and that this individual knew her Social Security number and attempted to have her verify it along with her bank routing number. (¶ 316.) She also alleges that since June 2020 she has received an increased number of scam telephone calls. (¶ 317.) Again, there are *no* allegations tying these incidents to the 2016 or 2019 Events.

- Midori Nelson alleges that, in June 2019 and again later in 2019, fraudulent purchases appeared on a credit card account. (*Id.* ¶ 263.) In both instances, the credit card issuer—notably, not Morgan Stanley—confirmed the fraud, reimbursed the account, and replaced the card. (*Id*.) Ms. Nelson does *not* allege that her credit card information had been provided to Morgan Stanley, or that it was implicated in either the 2016 or 2019 Events.

- Desiree Shapouri alleges that, in September 2019, she experienced twelve unauthorized charges on her American Express credit card. (¶ 337.) She does not allege that she had provided her American Express credit card information to Morgan Stanley and, once again, there are *no* allegations tying these incidents to the 2016 or 2019 Events.

None of the named plaintiffs purport to have suffered any injury proximate to the 2016 Event or prior to June 2019.

ARGUMENT

I. PLAINTIFFS LACK ARTICLE III STANDING

Plaintiffs' SAC fails to plausibly allege that they have Article III standing. While the SAC contains new, salacious allegations based on plaintiffs' misrepresentations of materials obtained in discovery, plaintiffs have done nothing to address the core shortcoming that dooms their case to dismissal: the SAC contains no allegations establishing that any malicious actor has *in fact* sought or obtained *any* Morgan Stanley client data as a result of the data security events. Reading the SAC's allegations in the light most favorable to plaintiffs, plaintiffs present—at most—a "lost data" case rather than a cognizable data breach action.[3] Plaintiffs have suffered no actual injury, face no imminent likelihood of future injury, and have experienced no other collateral form of injury giving rise to Article III standing. Under binding Second Circuit authority and persuasive case law from circuit and district courts across the country, plaintiffs in lost data cases such as this face significant, if not insurmountable, obstacles to showing they have Article III standing.

[3] Morgan Stanley adopts the term "lost data" from case law cited below for the purposes of setting forth its legal arguments in this motion. Morgan Stanley does not concede that it acted in any way inappropriately in decommissioning the assets involved in the 2016 or 2019 Events or that any device at issue bore PII belonging to any particular Morgan Stanley customer.

In their attempt to do so here, plaintiffs purport to show that they have suffered an injury-in-fact under four theories. Specifically, they allege that they: (i) face impending injury due to the likelihood of their data being misused (¶¶ 269; 279; 290; 300; 312; 324; 333; 343; 353); (ii) have suffered injury in the form of damages and diminution in the value of their PII (¶¶ 267; 277; 288; 298; 310; 322; 331; 341; 351); (iii) have experienced lost time, annoyance, interference, and inconvenience as a result the incidents (¶¶ 268; 278; 289; 299; 311; 323; 332; 342; 352); and (iv) each paid "annual fees" or "money" to Morgan Stanley for facilitating their accounts which they allegedly would not have paid if Morgan Stanley had "disclosed that it lacked data security practices adequate to safeguard customers' PII" (¶¶ 266; 276; 287; 297; 309; 321; 330; 340; 350).

As explained below, none of these allegations suffice to establish standing; because this defect is not curable—and plaintiffs already have had an opportunity to amend—the Court should dismiss this case in its entirety with prejudice.

A. The Second Circuit and Other Courts Have Held that Plaintiffs in "Lost Data" Cases Generally Cannot Show Article III Standing

Plaintiffs must show that they have Article III standing to bring their claims in federal court; failure to do so deprives the Court of subject matter jurisdiction and necessitates dismissal. *See McMorris* v. *Carlos Lopez & Assocs., LLC*, 995 F.3d 295 (2d Cir. 2021). Article III standing consists of three elements: (i) "the plaintiff must have suffered an 'injury in fact'—an invasion of a legally protected interest"; (ii) "there must be a causal connection between the injury and the conduct complained of"; and (iii) "it must be likely, as opposed to merely speculative, that the injury will be redressed by a favorable decision." *Lujan* v. *Defs. of Wildlife*, 504 U.S. 555, 560 (1992) (citations and internal quotation marks omitted); *accord McMorris*, 995 F.3d at 295. The burden is on the party seeking to establish Article III standing. *McMorris*, 995 F.3d at 295.

To this end, plaintiffs must show that they suffered an injury that is (i) "concrete and particularized" and (ii) "actual or imminent, not conjectural or hypothetical." *Lujan*, 504 U.S. at 560 (citation and internal quotation marks omitted). In the absence of any allegations of actual injury, allegations of potential future harm "may suffice 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)). "Allegations of *possible* future injury," however, are "not sufficient." *Clapper*, 568 U.S. at 409 (emphasis in original). Indeed, to establish standing, the Supreme Court has held that future injury must be "certainly impending," and a "theory of standing [] which relies on a highly attenuated chain of possibilities[] does not satisfy the requirement that threatened injury must be certainly impending." *Id*. at 410. In addition to showing that they suffered cognizable injury, plaintiffs must plausibly allege that any injury they purportedly suffered is attributable to Morgan Stanley's conduct in relation to the 2016 or 2019 Events and the relief plaintiffs seek will redress—that is, ameliorate and remedy—the particular injury they suffered and that is attributable to Morgan Stanley's conduct. *See Garelick* v. *Sullivan*, 987 F.2d 913, 919 (2d Cir. 1993).[4]

The Second Circuit recently established an authoritative test for determining whether plaintiffs in a data breach case have presented allegations sufficient to establish Article III standing. *See McMorris*, 995 F.3d at 303. In *McMorris*, an employee of the defendant company, a veteran's services provider, accidentally emailed a spreadsheet containing sensitive PII of approximately 130 current and former employees to 65 employees of the company. *Id.* at 298.

[4] Additionally, in a putative class action such as this one, the "named plaintiffs who represent a class must allege and show that they personally have been injured, not that injury has been suffered by other, unidentified members of the class to which they belong." *Ortiz* v. *CIOX Health LLC*, 386 F. Supp. 3d 308, 312 (S.D.N.Y. 2019) (*quoting Spokeo, Inc*. v. *Robins*, 136 S. Ct. 1540, 1547 n.6 (2016)).

Plaintiffs brought a class action on behalf of the employees whose data was exposed bringing various claims against the company similar to those brought here, alleging that the company's disclosure placed them "at imminent risk of suffering identity theft." *Id.* The parties settled. The district court, however, rejected the settlement and dismissed the case *sua sponte*, holding that it lacked subject matter jurisdiction due to plaintiffs' failure to show that they had Article III standing—particularly in light of their failure to allege that a malicious actor targeted and obtained their data. *See Steven* v. *Carlos Lopez & Assocs., LLC*, 422 F. Supp. 3d 801, 805 (S.D.N.Y. 2019).

After plaintiffs appealed, the Second Circuit affirmed the dismissal and set forth a test consisting of three non-exclusive factors that a court should consider when determining whether plaintiffs have plausibly alleged facts sufficient to establish Article III standing in a data breach case. *First*, the court held that "most importantly" among these factors, circuit courts "have consistently considered whether the data at issue has been compromised as the result of a *targeted attack intended to obtain the plaintiffs' data*." *McMorris*, 995 F.3d at 301 (emphasis added). *Second*, the court held that plaintiffs are more likely to "establish[] a substantial risk of future injury where they can show that at least some part of the compromised dataset has been misused." *Id. Third*, the court noted that a relevant consideration is "the type of data at issue, and whether that type of data is more or less likely to subject plaintiffs to a perpetual risk of identity theft or fraud once it has been exposed." *Id.* at 302.

Applying these factors, the court noted that the first two factors weighed against a finding of standing, as plaintiffs offered no evidence that a malicious actor targeted their data (rather, their data was exposed accidently) and presented no allegations of misuse connected to the incident. *Id.* at 303. The court acknowledged that the third factor weighed in favor of standing because the

defendant had exposed, among other things, employee social security numbers, but it held that the other two factors outweighed the third factor and therefore plaintiffs lacked standing. *Id.* at 304.

The Second Circuit's and district court's decisions in *McMorris* emphasize that plaintiffs—in what many courts call "lost data" cases—face steep, if not insurmountable, obstacles to showing they have Article III standing. This is because, as the district court in *McMorris* held, allegations of misuse—or, at the very least, theft—are crucial for standing purposes because the "intentional act of theft [gives] rise, in turn, to a plausible inference that the stolen data [will] be misused." *Steven*, 422 F. Supp. 3d at 805. Absent such allegations of intentional theft or data misuse, plaintiffs, like the plaintiffs in this case, can show only an "attenuated chain" of inferences "that at some unspecified point in the indefinite future they will be the victims of identity theft," which is insufficient to confer standing. *Id.* at 806 (internal citations and quotation marks omitted). *Id.* The Second Circuit underscored the district court's holding on this point in describing the first *McMorris* factor as the "most important[]." *McMorris*, 995 F.3d at 301.

The Second Circuit's decision in *McMorris* is in line with a wealth of circuit and district court decisions from across the country that have reached the same result in lost data cases, and the Second Circuit cited to a number of them in emphasizing the importance of the first factor in the standing analysis. *See Beck* v. *McDonald*, 848 F.3d 262, 274–76 (4th Cir. 2017) (cited in *McMorris* and holding the "mere theft" of a device containing PII, "without more, cannot confer Article III standing"); *Katz* v. *Pershing, LLC*, 672 F.3d 64, 79 (1st Cir. 2012) (cited in *McMorris* and holding standing is not established where plaintiff "has not alleged that [its] nonpublic personal information actually has been accessed by any unauthorized person,"); *Reilly* v. *Ceridian Corp.*, 664 F.3d 38, 40–44 (3d Cir. 2011) (cited in *McMorris* and holding where there "has been no misuse of the information, [there is] no harm").

Accordingly, district courts across the country have held that plaintiffs in lost data cases cannot show that they have Article III standing. *U.S. Hotel & Resort Mgmt., Inc.* v. *Onity, Inc.*, Civil No. 13-1499 (SRN/FLN), 2014 WL 3748639, at *5 (D. Minn. July 30, 2014) ("In the 'lost data' context, where the courts have split somewhat on the question of standing, it now appears that a majority of the courts to have addressed the 'lost data' issue hold that plaintiffs whose confidential data has been exposed, or possibly exposed, by theft or a breach of an inadequate computer security system, but who have not yet had their identity stolen or their data otherwise actually abused, lack standing to sue the party who failed to protect their data." (citing *Reilly*, 664 F.3d at 43)); *Blahous* v. *Sarrell Reg'l Dental Ctr. for Pub. Health, Inc.*, No. 19-cv-798-RAH-SMD, 2020 WL 4016246, at *5–7 (M.D. Ala. July 16, 2020) (noting "lower federal courts presented with 'lost data' or potential identity theft cases in which there is no proof of *actual* misuse or fraud have held that plaintiffs lack standing to sue the party who failed to protect their data"); *see also, e.g.*, *Randolph* v. *ING Life Ins. & Annuity Co.*, 486 F. Supp. 2d 1, 7–8 (D.D.C. 2007); *Whitaker* v. *Health Net of Cal., Inc.*, No. CIV S-11-0910 KJM-DAD, 2012 WL 174961, at *3 (E.D. Cal. Jan. 20, 2012) (plaintiffs lacked standing because they alleged that their data was lost and "do not explain how the loss here has actually harmed or threatens to harm them, or that third parties have accessed their data."); *Engl* v. *Natural Grocers by Vitamin Cottage, Inc.*, No. 15-cv-02129-MSK-NYW, 2016 WL 8578252, at *5 (D. Colo. Sept. 21, 2016) ("[T]he risk of future injury alone is not sufficient [in] cases where a data breach merely exposes data to those who might use it, but in cases where there is indicia that hackers have actually obtained and used the data, there is a present [*sic*] a risk of future injury sufficient to support standing." (emphases in original)).

In short, there is overwhelming case law establishing that in cases such as this one, absent specific, detailed allegations of harm, plaintiffs are unable to show that they have suffered any cognizable injury giving rise to Article III standing. The same is true here.

B. Plaintiffs' Attempts to Plead Standing Are Unavailing

While the SAC includes numerous additional allegations pertaining to Morgan Stanley's purported failures to protect plaintiffs' PII, it is more remarkable for what it does *not* contain: there is not a single allegation that a malicious actor has accessed or is likely to have the ability to access any of plaintiffs' PII, let alone that plaintiffs have suffered any actual injury as a result of the 2016 or 2019 Events. As a result, all of plaintiffs' standing theories fail.

1. An Application of the *McMorris* Factors Shows Plaintiffs Lack Article III Standing Based on the Lack of Risk of Imminent Future Harm

Applying the *McMorris* test to this case, and against the backdrop of extensive lost data case law, the Court should find that plaintiffs have failed to show that they have experienced actual injury or face a sufficient likelihood of imminent future injury to establish injury-in-fact for the purposes of Article III standing. As explained below, all three factors—and in particular the first and second factors—weigh strongly against any finding of standing.

a. No Malicious Actor Targeted or Acquired Morgan Stanley Data. The first and most important factor in the standing analysis is whether plaintiffs have alleged that their PII was exposed as a result of a malicious actor targeting and acquiring that data. Plaintiffs have not—and cannot—make any such allegation.

b. Plaintiffs Have Not Plausibly Alleged that the PII of Any Putative Class Member Has Been Misused as a Result of the Incidents. The second *McMorris* factor requires that plaintiffs plausibly allege that at least some members of the class have suffered misuse of or improper access of their PII as a result of Morgan Stanley's conduct. The SAC is devoid of any such allegations.

Rather, plaintiffs recycle the same boilerplate assertions of "substantially increased risk of fraud, identity theft, and misuse" (¶¶ 269; 279; 290; 300; 312; 324; 333; 343; 353).

It is particularly striking that plaintiffs are unable to make any plausible allegations of identity theft related to the 2016 or 2019 Events in a class of approximately 14.5 million people and with the benefit of nine months of wide-ranging discovery. The handful of instances of identity theft or data misuse that are actually alleged are entirely untethered to either the 2016 or 2019 Events; rather, they are the sorts of unfortunately commonplace inconveniences of modern life that many of us have experienced. For instance, plaintiffs point to complaints that Morgan Stanley received from customers after receiving the notices at issue in this case. (¶¶ 23–24.) But even among the handful of complaints that actually involve allegations of data misuse, none of them provides any plausible basis to connect those allegations to the data security events at issue here.[5]

Elsewhere, five of the eleven named plaintiffs allege scattered instances of recent attempts at credit card theft, phishing, or spamming—all occurring *after* June 2019. As an initial matter, it strains credulity to claim that these events were caused by the 2016 Data Center Event, given the passage of time and the lack of any allegations connecting them to Morgan Stanley. *See, e.g., Fernandez* v. *Leidos, Inc.*, 127 F. Supp. 3d 1078, 1087 (E.D. Cal. 2015) ("Further, in light of the fact that Plaintiff waited thirty-six months after the Data Breach to file his Complaint, and that now almost four years has elapsed since the Data Breach, Plaintiff has not shown that any alleged risk of future identity theft, identity fraud, and/or medical fraud is imminent."). At a minimum,

[5] Plaintiffs' allegation is drawn from an internal Morgan Stanley spreadsheet, which was produced by defendant under a highly confidential designation and is incorporated by reference into plaintiffs' complaint. (¶ 23.) Of approximately 400 client complaints that Morgan Stanley received—itself a tiny fraction of the total number of notice recipients—roughly 350 of the complaints were either administrative or logistical in nature (*i.e.*, questions about accessing the free credit monitoring services Morgan Stanley offered) or merely an expression of annoyance. Morgan Stanley will provide a copy of the spreadsheet under seal at the Court's request.

claims arising out of the 2016 Data Center Event should be dismissed from this case. Plaintiffs cannot plausibly link them to Morgan Stanley, and, unsurprisingly, have made no more than conclusory allegations to overcome that disability. (¶¶ 263, 283, 305, 316-317, 337.) Two of these five plaintiffs—Midori Nelson and Desiree Shapouri—allege that their credit card information was misused, but credit card numbers were not exposed in either of the alleged data breach incidents. (¶¶ 263, 337.)[6] The other three plaintiffs— Mark Blythe, Richard Gamen, and Amresh Jaijee—allege that they experienced various instances of spamming and potential identity fraud in either June or July 2020. While that timing coincides with plaintiffs' receipt of the Consumer Notice, it is not sufficiently linked in any plausible way to either the 2016 or 2019 Events to allege causation. (¶¶ 283, 305, 316–317.)

In any event, plaintiffs offer no plausible allegations giving rise to the inference that any of these scattered incidents are in any way connected to the 2016 or 2019 Events. *See, e.g.*, *Welborn* v. *IRS*, 218 F. Supp. 3d 64, 79–80 (D.D.C. 2016) (holding traceability element of standing not satisfied where plaintiff "simply allege[d] that the alleged financial fraud happened *after*" the breach without showing that "the type of data obtained from the theft" was misused); *Kimbriel* v. *ABB, Inc.*, No. 19-CV-215-BO, 2019 WL 4861168, at *2–*3 (E.D.N.C. Oct. 1, 2019) (holding plaintiffs failed to establish Article III standing for claims arising from data breach where the only alleged harm was scattered instances of credit inquiries). Indeed, courts are "usual[ly] reluctan[t] to endorse standing theories that rest on speculation about the decisions of independent actors," *Clapper*, 568 U.S. at 414, especially where it rests on "speculation" about a future unlawful injury.

[6] Additionally, Morgan Stanley did not assert in its Consumer Notice that the relevant devices had credit card data—a fact plaintiffs do not dispute. (Ex. 1.)

c. The Circumstances of the 2016 and 2019 Events Further Decrease the Plausibility of Any Injury to Plaintiffs. The third *McMorris* factor also weighs against standing. While the devices at issue contained sensitive forms of PII, including social security numbers, the court in *McMorris* stressed that this factor, at bottom, is concerned with whether the PII is exposed in such a way that makes it "more or less likely to subject plaintiffs to a perpetual risk of identity theft or fraud once it has been exposed." *McMorris*, 995 F.3d at 302. To this end, while the court in *McMorris* noted that the case involved highly sensitive PII, the court also emphasized that the circumstances of disclosure matter: "[T]here 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." *See id.* 304 n.6; *see also id.* at 304 ("[W]e conclude that the sensitive nature of McMorris's internally disclosed PII, by itself, does not demonstrate that she is at a substantial risk of future identity theft or fraud.").

The allegations in the SAC and documents incorporated by reference show that the circumstances of potential exposure here diminish—rather than increase—the likelihood of injury. Plaintiffs offer no basis for inferring that the type of data that was allegedly exposed in this case—and crucially, the manner in which it was stored—create any meaningful likelihood of future theft or misuse. Indeed, the investigative materials from PwC and Stroz, and Morgan Stanley's representations to regulators that plaintiffs rely on extensively demonstrate otherwise.[7] They show that Morgan Stanley concluded that the data bearing elements of the non-NetApp devices were likely destroyed or wiped or otherwise contained data of minimal sensitivity. With respect to the NetApp devices, these documents show the difficulties a malicious actor would experience in

[7] These materials were all produced by defendant under a highly confidential designation and are incorporated by reference into plaintiffs' complaint. (¶¶ 167; 169-174; 194). Morgan Stanley will provide a copy of these materials under seal at the Court's request.

seeking to access data on the devices, including the need for proper equipment, extensive technological abilities and comprehensive forensic analysis.

Plaintiffs' allegations that third parties have "unfettered" access to customer PII and that plaintiffs' expert has identified the unencrypted PII of one of the named plaintiffs are false and misleading. The data stored on the devices at issue can only be accessed two ways: by having the right hard drives in the right order or by using forensic techniques. Plaintiffs do not allege that anyone has the right set of hard drives to recreate the data. Instead, they claim a malicious actor could have "unfettered access" to the data because their expert was able to find some by searching a forensic image of some of the drives. (¶ 41.) But they conveniently omit that their expert only did so after Morgan Stanley's expert, Stroz Friedberg, undertook a complicated technical analysis to produce the image for Plaintiffs' expert to search. They also fail to note that Stroz was only able to conduct that analysis with specialized hardware that, despite being a major forensics firm that routinely conducts this type of analysis, Stroz did not own, because the devices at issue are intended for a data center, not a retail or consumer user. Absent Stroz's procurement of special hardware, use of forensics tools, and their technical analysis—all of which plaintiffs misleadingly fail to acknowledge—plaintiffs would have had no access to any information on the devices, let alone client PII. Most importantly, plaintiffs do not—and cannot—allege that anyone other than the parties in this case have accessed any data.

In this respect, the case at hand presents a strikingly similar factual circumstances to that at issue in *In re Science Applications International Corp. (SAIC) Backup Tape Data Theft Litigation*, where the court held plaintiffs lacked standing in a data breach case. 45 F. Supp. 3d 14, 19–20 (D.D.C. 2014). In that case, the court held the plaintiffs failed to plausibly plead any Article III injury on the grounds that "disclosure and access of Plaintiffs' personal information is anything

but certain," because "the information is itself locked inside tapes that require some expertise to open and decipher" and pointed out that it was "highly unlikely that the crook even understood what the tapes were, let alone had the wherewithal to access them or navigate her way to any one of the 4.7 million records contained therein." *Id.* at 29. As a result, the court concluded that "until Plaintiffs can aver that their records have been viewed (or certainly will be viewed), any harm to their privacy remains speculative" and unable to support Article III standing. *Id.*

A recent Supreme Court decision offers additional support. In *TransUnion LLC* v. *Ramirez*, where plaintiffs brought claims under the TPCA based on defendant accidently including incorrect and damaging facts about plaintiffs in the plaintiffs' credit reports, the Court held that in "cases such as these where allegedly inaccurate or misleading information sits in a company database, the plaintiffs' harm is roughly the same, legally speaking, as if someone wrote a defamatory letter and then stored it in her desk drawer. A letter that is not sent does not harm anyone, no matter how insulting the letter is. So too here." 141 S. Ct. 2190, 2210 (2021).

This case is similar to *In re Science* and *TransUnion* in that the well-pleaded allegations in the Complaint show that the circumstances of the alleged exposure of plaintiffs' data make it unlikely that plaintiffs will, in fact, suffer imminent harm as a result of that exposure. For the reasons provided above, plaintiffs offer no basis for finding that the manner in which their data was allegedly exposed presents a meaningful likelihood of future injury through identity theft or misuse of the data. As a result, the third *McMorris* factor, too, weighs against standing.

In any event, even if the Court holds that the third factor weighs in favor of standing, the first two factors (particularly the first factor) strongly weigh against standing and should prove dispositive, as in *McMorris*. *See McMorris*, 995 F.3d at 304 ("Finally, while the information that was inadvertently disclosed by CLA included the sort of PIII that might put Plaintiffs at a

substantial risk of identity theft or fraud, in the absence of any other facts suggesting that the PIII was intentionally taken by an unauthorized third party or otherwise misused, this factor alone does not establish an injury in fact.") Setting aside whatever dispute the parties may have about the accessibility of data on the devices, plaintiffs cannot establish standing because they do not allege a single instance where any Morgan Stanley customer's data was actually accessed and misused as a result of either the 2016 or 2019 Events. This is all the more striking given that nearly nine months of discovery have elapsed, that plaintiffs have had access to a purported class of more than 14 million members, and that five years have passed since the 2016 equipment was decommissioned. As clearly held in *McMorris*, where a plaintiff "[does] not allege that her PII was subject to a targeted data breach or allege any facts suggesting that her PII (or that of any others) was misused," that plaintiff has failed to establish an Article III injury in fact. *Id.* at 305.

2. Plaintiffs Cannot Establish Standing Based on Alleged Subsequent Out-of-Pocket Expense

Plaintiffs also allege standing based on so-called "out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud and/or unauthorized use of their PII" and "lost opportunity costs associated with attempting to mitigate the actual consequences of" the 2016 and 2019 Events. (¶¶ 268; 278; 289; 299; 311; 323; 332; 342; 352; 412.) The Second Circuit's decision in *McMorris*, however, forecloses this theory of standing. In *McMorris*, the court held that "where plaintiffs have not alleged a substantial risk of future identity theft, the time they spent protecting themselves against this speculative threat cannot create an injury"—in other words, "plaintiffs cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending." 995 F.3d at 303 (citations and quotation marks omitted). The same is true in this case. Because plaintiffs here cannot establish that they expended time and money to mitigate actual or imminent

injury, those out-of-pocket expenses cannot serve as an alternative basis for establishing Article III standing. In any event, plaintiffs' own allegations reflect that Morgan Stanley rendered these expenditures unnecessary by providing two years of credit monitoring service. (¶ 242.)

3. Plaintiffs Cannot Establish Standing Based on Morgan Stanley's Purported Failure to Disclose Inadequate Data Security Measures

Plaintiffs offer only conclusory allegations that they suffered injury through payments of fees or money to Morgan Stanley for "facilitating" their accounts and that they would not have made these payments "had [Morgan Stanley] disclosed that it lacked data security practices adequate to safeguard customers' PII." (¶¶ 266; 276; 287; 297; 309; 321; 330; 340; 350.) But nowhere do plaintiffs plead what these payments were for, or that they were at all connected to storage of plaintiffs' PII (as opposed to the numerous financial services Morgan Stanley provided that were the core purposes of plaintiffs' relationship with Morgan Stanley), that data security practices at Morgan Stanley impacted plaintiffs' decision to use Morgan Stanley over another financial institution, or otherwise connecting the payments to either data event. These threadbare allegations of payments made to Morgan Stanley are too attenuated to confer standing. *Lujan*, 504 U.S. at 564 n.2; *see also Jackson* v. *Loews Hotels, Inc.*, No. ED CV 18-827-DMG (JCx), 2019 WL 6721637, at *2 (C.D. Cal. July 24, 2019) ("Plaintiffs have identified no authority approving of a 'benefit of the bargain' theory in a data breach case based on such conclusory allegations of an *implied* promise to earmark a portion of the purchase price for ensuring data safety. Indeed, case law appears to require more precise allegations and more explicit promises." (emphasis in original) (citing *In re Zappos.com, Inc.*, 108 F. Supp. 3d 949, 962 n.5 (D. Nev. 2015)). In any event, plaintiffs have not and cannot show that they suffered any actual injury as a result of the purported disclosure of their data. Therefore, they cannot show that they were, in fact, injured by Morgan Stanley's alleged failure to disclose the alleged issues with its data security practices.

Relatedly, plaintiffs cannot claim to have suffered actual injury as a result of Morgan Stanley's purported failure to adequately disclose alleged problems with its data security policies and practices under Section 349. Even if plaintiffs are able to satisfy the misrepresentation element of their Section 349 claim—which as explained below, they cannot—their ability to do so for the purposes of substantively proving their statutory claim does not mean they have Article III standing to bring the claim in the first place. As the Supreme Court in *Transunion* made clear, a violation of a statutory provision alone does not necessarily constitute an injury-in-fact for the purposes of showing Article III standing. *See Transunion*, 141 S. Ct. at 2205 ("But even though Congress may elevate harms that exist in the real world before Congress recognized them to actionable legal status, it may not simply enact an injury into existence, using its lawmaking power to transform something that is not remotely harmful into something that is." (citation and quotation marks omitted)). Plaintiffs here cannot manufacture a cognizable injury simply by arguing that they can satisfy a false statement element of a state unfair and deceptive practices statute.

4. Plaintiffs Cannot Establish Standing Based on an Alleged Diminution of Value of their PII

Finally, plaintiffs' weak attempt to allege that the data events diminished the value of their PII fails, because they have not alleged any particular value of which they have been deprived. *See, e.g.*, *Welborn,* F. Supp. 3d at 78 ("Courts have routinely rejected the proposition that an individual's personal identifying information has an independent monetary value."). Rather, they repeatedly allege in a simplistic and conclusory fashion that each plaintiff "suffered actual injury in the form of damages to and diminution in the value of their PII—a form of intangible property." (¶¶ 267; 277; 288; 298; 310; 322; 331; 341; 351.) "General, conclusory allegations need not be credited . . . when they are belied by more specific allegations of the complaint." *Hirsch* v. *Arthur Andersen & Co.*, 72 F.3d 1085, 1092 (2d Cir. 1995).

For these reasons, plaintiffs fail to establish standing; their Complaint should be dismissed.

II. PLAINTIFFS' CLAIMS FAIL AS A MATTER OF LAW

Even if plaintiffs had established Article III standing, which they have not, the Complaint should be dismissed with prejudice for failure to state a claim under Fed. R. Civ. P. 12(b)(6). Although the material facts alleged in the complaint are to be treated as true at the pleading stage, "a plaintiff's obligation to provide the grounds of his entitlement to relief requires more than labels and conclusions, and a formulaic recitation of the elements of a cause of action will not do." *Bell Atl. Corp.* v. *Twombly*, 550 U.S. 544, 555 (2007) (citation and internal quotation marks omitted). To survive a motion to dismiss, a complaint's "[f]actual allegations must be enough to raise a right to relief above the speculative level." *Id.* As discussed below, plaintiffs fail to meet this standard.

A. Plaintiffs Fail to State a Claim for Negligence or Gross Negligence.

"Under New York law, in order to recover on a claim for negligence, a plaintiff must show (1) the existence of a duty on defendant's part as to plaintiff; (2) a breach of this duty; and (3) injury to the plaintiff as a result thereof." *Caronia* v. *Philip Morris USA, Inc.*, 715 F.3d 417, 428 (2d Cir. 2013) (citation and internal quotation marks omitted). Plaintiffs' negligence claim fails because they have not alleged that Morgan Stanley breached any general or specific duty of care, or that they have suffered any injury.

Beyond entirely boilerplate, conclusory allegations, plaintiffs fail to plausibly allege how Morgan Stanley's data security practices deviated from acceptable industry custom or practices to plead either the existence of a duty or a breach thereof. (¶¶ 209–230; 400.) For example, plaintiffs assert that Morgan Stanley "had a duty to exercise reasonable care in safeguarding, securing, and protecting . . . information" (without alleging what the source of that duty was) (*id.* ¶ 386); that it "had a duty to exercise appropriate clearinghouse practices" (without identifying what those clearinghouse practices were or should have been) (*id.* ¶ 387); and that it "had a duty to have

procedures in place to detect and prevent the improper access and misuse" of PII (without alleging that Morgan Stanley failed to protect against the misuse of plaintiffs' PII) (*id.* ¶ 388).[8] These conclusory and formulaic pleadings fail plausibly to allege that specific data security practices at Morgan Stanley were deficient or deviated from an acceptable industry baseline or standard sufficient to state a claim for negligence. *See, e.g.*, *MLSMK Inv. Co.* v. *JP Morgan Chase & Co.*, 431 F. App'x 17, 20 (2d Cir. 2011) (summary order) (affirming dismissal of negligence claim because the allegations of breach of duty were conclusory and insufficient to state a claim).[9]

Even if these allegations demonstrated a breach of a duty, plaintiffs do not adequately plead the elements of causation or damages. First, as mentioned *supra* at Part I, plaintiffs have not alleged any cognizable harm or injury. *See, e.g.*, *Willey* v. *J.P. Morgan Chase, N.A.*, No. 09 Civ. 1397 (CM), 2009 WL 1938987, at *9 (S.D.N.Y. July 7, 2009) ("Because [plaintiff] does not allege that any of his personal data (or anyone else's for that matter) was actually misused, he has not alleged

---

[8] While plaintiffs purport to allege that they were in a "special relationship" with Morgan Stanley, they do not identify the source of that special relationship beyond an ambiguous, "'independent duty,' untethered to any contract between" Morgan Stanley and any named plaintiff. (¶¶ 388–389.) Such allegations are insufficient to establish any cognizable duty. A "special relationship" can only give rise to a duty to protect an individual from the conduct of others in limited circumstances, none of which are present here. *See Fay* v. *Assignment Am.*, 666 N.Y.S.2d 304, 306 (3d Dep't 1997) ("Examples of . . . special relationships include the relationship between employers and employees, parents and children, common carriers and their patrons, and school districts and their students, among others.").

[9] Plaintiffs allege that Section 5 of the FTC Act "form[s] part of the basis of Morgan Stanley's duty." (¶ 407). But under New York state law, Section 5 of the FTC Act cannot support a claim for negligence. *See Smahaj* v. *Retrieval-Masters Creditors Bureau, Inc.*, 69 Misc. 3d 597, 608 (N.Y. Sup. Ct. Westchester Cty. 2020) (in a putative class action founded on an alleged data breach, the court held that "Plaintiff's negligence per se claim based on an alleged violation of the FTC Act must also be dismissed" because a negligence per se claim is one that the statute "does not recognize") (quoting *Lugo* v. *St. Nicholas Assoc.*, 2 Misc. 3d 212, 218 (N.Y. Sup. Ct. N.Y. Cty. 2003), *aff'd* 18 A.D.3d 341, 342 (1st Dep't 2005); *cf. In re SuperValu, Inc.*, 925 F.3d 955, 963–64 (8th Cir. 2019) (applying Illinois law).

damages sufficient to support his state law claims [including negligence]."); *Caudle* v. *Towers, Perrin, Forster & Crosby, Inc.*, 580 F. Supp. 2d 273, 281 (S.D.N.Y. 2008) (observing that, where plaintiff had not alleged that anyone had attempted to access or use the laptop containing PII, damages must be "reasonably certain to be incurred" to be recoverable) (citation and internal quotation marks omitted). Even if plaintiffs could show that they were harmed, they have alleged no facts plausibly linking that purported harm to anything Morgan Stanley did (or failed to do). *See, e.g.*, *Mortensen* v. *Mem'l Hosp.*, 483 N.Y.S.2d 264, 270 (1st Dep't 1984) (to demonstrate causation, a defendant's negligent act must have been a "substantial factor in bringing about the plaintiff's injury."). Causation is all-the-more implausible here, considering that more than five years has passed since the 2016 Event and the alleged injury depends on the superseding criminal acts of third parties. *Cf. Deskovic* v. *City of Peekskill*, 673 F. Supp. 2d 154, 161 (S.D.N.Y. 2009) ("Generally, an intervening intentional or criminal act is a type of superseding cause that severs the liability of the original tort-feasor.") (citation and internal quotation marks omitted).

B. Plaintiffs Do Not Have a Viable Claim Under New York Gen. Bus. Law § 349

New York's UDAP provision, New York Gen. Bus. Law § 349, requires that the plaintiff plausibly allege that the defendant "engaged in (1) consumer-oriented conduct that is (2) materially misleading and that (3) plaintiff suffered injury as a result of the allegedly deceptive act or practice." *City of New York* v. *Smokes-Spirits.Com, Inc.*, 12 N.Y.3d 616, 621 (2009). Here, plaintiffs claim is time-barred, entirely premised on non-actionable statements, and plaintiffs have failed to plead a misleading act that caused injury.

1. Plaintiffs' Section 349 Claim Is Time-Barred

A claim for damages under Section 349 accrues at the time that the plaintiff is induced into an allegedly deceptive transaction. *Fero* v. *Excellus Health Plan, Inc.*, 502 F. Supp. 3d 724, 736 (W.D.N.Y. 2020) (quoting *Gristede's Foods, Inc.* v. *Unkechauge Nation*, 532 F. Supp. 2d 439,

453 (E.D.N.Y. 2007)); *Schandler* v. *New York Life Ins. Co.*, No. 09 Civ. 10463 (LMM), 2011 WL 1642574, at *4–*5 (S.D.N.Y. Apr. 26, 2011) (determining that plaintiff's claim accrued when insurance policy was delivered, not when plaintiff's insurance claims were rejected). Under the statute, any claim for relief must be filed within three years of the accrual date. N.Y. GEN. BUS. LAW § 214(2); *see also*, *Fero*, 502 F. Supp. at 736; *Schandler*, 2011 WL 1642574, at *4. But according to plaintiffs' own complaint, *none* of the named plaintiffs opened their accounts with Morgan Stanley within three years of the filing of their complaints. Indeed, most of them not only opened but closed their accounts with Morgan Stanley decades ago. (*See, e.g.*, ¶¶ 302–303.) Any claims arising from these transactions are time-barred.

Fero v. *Excellus Health Plan, Inc.* is instructive. 502 F. Supp. at 736. There, as here, the plaintiffs claimed that the defendant made "material misrepresentations regarding their data privacy and security practices" and "fail[ed] to reveal that 'its cybersecurity systems were insufficiently equipped to safeguard the PII and PHI Excellus collected from its members.'" *Id.* at 736 (internal citations omitted). The court held that the plaintiffs' "injury accrued as soon as [defendant] placed their personal information into its inadequately protected network," not when the hack was discovered, and concluded that many of the putative class members' claims would be time-barred as they would have given their data and personal health information to the defendant more than three years prior to the initiation of the suit. *Id.* at 736–37.

Plaintiffs' claims here are, in relevant respects, identical to those in *Fero* and should be dismissed for the same reason: Their claims accrued when they entrusted their personal data to Morgan Stanley, many years before the latest date on which they could have filed a timely lawsuit.

2. Plaintiffs' Section 349 Claim Also Fails on the Merits

Plaintiffs' Section 349 claim fails because it is premised on non-actionable statements. A statement is non-actionable "when it makes a generalized or exaggerated statement such that a

reasonable consumer would not interpret the statement as a factual claim upon which he or she could rely." *Kommer* v. *Ford Motor Co.*, No. 17-CV-296(LEK/DJS), 2017 WL 3251598, at *3 (N.D.N.Y. July 28, 2017) (brackets, quotation marks, and citation omitted). The statements on which plaintiffs rely are classic examples of non-actionable statements:

- Morgan Stanley's long standing commitment to safeguard the privacy of information our clients entrust to us is essential to our goal to be the world's first choice for financial services.
- Protecting the confidentiality and security of client information has always been an integral part of how we conduct our business worldwide.
- We pledge to continue to ensure that our global business practices protect your privacy.

(¶ 4.) None of these statements are untrue. Rather, they accurately reflect Morgan Stanley's general commitment to "safeguard" the "privacy" and "confidentiality" of its clients' data, and its "pledge" to "continue" business practices reflecting that commitment in the future. Courts routinely hold that such "general statements" about a company's "integrity" and "compliance with ethical norms" are too vague and aspirational to constitute actionable misstatements. *Cf. Singh* v. *Cigna Corp.*, 918 F.3d 57, 63 (2d Cir. 2019) ("general statements" expressing commitment to "compliance" with applicable regulations were non-actionable puffery under Rule 10(b)(5)); *City of Pontiac Policemen's & Firemen's Ret. Sys.* v. *UBS AG*, 752 F.3d 173, 183 (2d Cir. 2014) (same).

Even if the statements were actionable (which they are not), plaintiffs also have failed to plead, beyond mere boilerplate, that Morgan Stanley had a duty to disclose material information, or that it failed to meet any such duty. (¶ 436; ¶ 438.) Plaintiffs' claim fails for the additional reason that they have not pleaded any injury as a result of deception by Morgan Stanley. They have not alleged that their damages, if any, (i) occurred as a result of any materially misleading representations Morgan Stanley made about its data security practices; or (ii) were caused by the 2016 or 2019 Events. *See Jensen* v. *Cablevision Sys. Corp.*, 372 F. Supp. 3d 95, 127–28 (E.D.N.Y.

2019) ("The potential for the release of private information, without any evidence of the actual release of private information, by itself, does not constitute an injury sufficient to state a claim" in the GBL § 349 context); *Shostack* v. *Diller*, No. 15 Civ. 2255(GBD)(JLC), 2015 WL 5535808, at *8 (S.D.N.Y. Sept. 16, 2015) ("Although the actions of the unknown third party who misappropriated [plaintiff's] identity were undoubtedly fraudulent, there was nothing deceptive about Lending Tree running [plaintiff's] credit report"), *report and recommendation adopted*, No. 15 Civ. 2255(GBD)(JLC), 2016 WL 958687 (S.D.N.Y. Mar. 8, 2016). At best, plaintiffs can only argue that they were harmed because they were allegedly deceived as to the type of data protection Morgan Stanley would provide. But New York law is clear that plaintiffs cannot state a claim under Section 349 where their "only alleged injury" is the "alleged deceptive conduct itself." *See In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, 996 F. Supp. 2d 942, 1005 (S.D. Cal. 2014) ("Plaintiffs only alleged injury is the alleged deceptive conduct itself, which New York courts have consistently rejected as insufficient under the NYDPA.") (citing *Baron* v. *Pfizer, Inc.*, 840 N.Y.S.2d 445, 448 (3rd Dep't 2007)); *Dimond* v. *Darden Rests., Inc.*, No. 13 Civ. 5244(KPF), 2014 WL 3377105, at *9 (S.D.N.Y. July 9, 2014) ("[D]eception and injury must be separately pled."). Thus, their claim under New York's UDAP statute fails to state a claim.

C. Plaintiffs Fail to State a Claim for Breach of Fiduciary Duty

Plaintiffs also have failed to state a claim for breach of fiduciary duty, because no such duty exists between Morgan Stanley and plaintiffs. There is no general fiduciary duty to secure customer data in New York. Further, providing financial accounts, as Morgan Stanley did for plaintiffs, does not create a fiduciary duty. *U.S. Bank Nat'l Ass'n* v. *Ables & Hall Builders*, 696 F. Supp. 2d 428, 442 (S.D.N.Y. 2010) ("[A] bank's generalized desire for its customers to 'trust' it, place 'confidence' in it, and 'continue doing business' with it, is not sufficient, standing alone, to

create a fiduciary relationship with its borrower."); *DDR Const. Servs., Inc.* v. *Siemens Indus., Inc.*, 770 F. Supp. 2d 627, 656–57 (S.D.N.Y. 2011) (collecting cases).

Even if Morgan Stanley had a fiduciary duty toward its brokerage customers, that duty is very limited in scope: It only requires that when recommending securities or investment strategies involving securities that Morgan Stanley act in its clients' best interest. This duty does not impose any special obligations on Morgan Stanley in other, totally unrelated areas such as data security.

To the extent plaintiffs are asking the court to recognize a totally new, common-law fiduciary duty with respect to data security, that effort should be rejected. New York law—which plaintiffs agree applies here—is clear that new and novel common-law privacy rights are heavily disfavored. As the Second Circuit explained in *Young* v. *U.S. Dep't of Justice*, there is no general, "common-law right to privacy in New York." 882 F.2d 63, 640–45 (2d Cir. 1989). And New York courts have generally been "conservative in recognizing causes of action for damages in the privacy field." *Id.* There is a good reason for that—privacy is a complex field, and creating novel rights can have any number of downstream effects on business, civil liberties, or other fields. New York courts rightly leave the resolution of these complex issues to the legislature.

D. Plaintiffs Fail to State a Claim for Unjust Enrichment

To state a claim for unjust enrichment, a plaintiff must allege that "(1) defendant was enriched, (2) at plaintiff's expense, and (3) equity and good conscience militate against permitting defendant to retain what plaintiff is seeking to recover." *Briarpatch Ltd., L.P.* v. *Phoenix Pictures, Inc.*, 373 F.3d 296, 306 (2d Cir. 2004) (citation omitted.)

Plaintiffs' allegations for unjust enrichment are deficient. (¶¶ 272–285.) First, plaintiffs have failed to allege that Morgan Stanley engaged in any inequitable conduct accruing to its benefit. Second, plaintiffs have not plausibly alleged that their PII has any value to Morgan Stanley. *See In re Jetblue Airways Corp. Priv. Litig.*, 379 F. Supp. 2d 299, 330 (E.D.N.Y. 2005).

Plaintiffs offer allegations about the value of PII to cybercriminals (¶¶ 231–237), but not to Morgan Stanley, which is necessary to allege an unjust enrichment claim.[10]

Furthermore, unjust enrichment "is not available where it simply duplicates, or replaces, a conventional contract or tort claim." *Corsello* v. *Verizon N.Y., Inc.*, 18 N.Y.3d 777, 790-91 (2012) (citations omitted); *see also Mahoney* v. *Endo Health Sols., Inc.*, No. 15-cv-9841 (DLC), 2016 WL 3951185, at *11 (S.D.N.Y. July 20, 2016). Here, the unjust enrichment claim fails for because it is duplicative of plaintiffs' tort claims, rendering it "not available." *Hitachi Data Sys. Credit Corp.* v. *Precision Discovery, Inc.*, 331 F. Supp. 3d 130, 152 (S.D.N.Y. 2018).

E. Plaintiffs Fail to State a Claim for Breach of Confidence

Plaintiffs fail to state a claim for breach of confidence because (i) New York does not recognize such a cause of action and (ii) plaintiffs have failed adequately to plead the element of damages. New York courts have not recognized a nebulous "breach of confidence" claim of the sort asserted by plaintiffs—*i.e.*, arising independently from either a fiduciary or contractual relationship (¶ 206)—in the context of a data breach action. *In re Capital One Consumer Data Sec. Breach Litig.*, No. 19-md-2915(AJT/JFA), 2020 WL 5629790, at *18 n.21 (E.D. Va. Sept. 18, 2020) ("The Court is not aware of any decision under [New York] law that has recognized a tort for the breach of confidence within the context of a bank/customer relationship. And in fact, New York courts have expressed reluctance to recognize such a tort." (citing *Young*, 882 F.2d at 637); *Graney Dev. Corp*. v. *Taksen*, 92 Misc. 2d 764 (N.Y. Sup. 1978), *aff'd*, 66 A.D.2d 1008 (4th Dep't 1978)). *See also, Young*, 882 F.2d at 640–41 (noting that "[a]t this point, New York courts have recognized [a breach-of-confidence theory] only in the context of physician-patient

[10] While plaintiffs allude to Morgan Stanley's AI Center of Excellence (¶ 458), they do not allege that the PII at issue in this case was used by the Center of Excellence, or that Morgan Stanley otherwise benefited or profited from retaining plaintiffs' PII.

relationships," and that "New York's courts have been rather conservative in recognizing causes of action for damages in the privacy field"); *Madden* v. *Creative Servs., Inc.*, 84 N.Y.2d 738, 744–47 (1995) (breach of confidence claims recognized in narrow circumstances "premised on [a] violation of a fiduciary or contractual relationship").

Finally, in any event, the breach of confidence claim fails because, for all the same reasons plaintiffs lack standing, they have failed to allege any cognizable damages resulting from either incident. *See, e.g.*, *Attias* v. *CareFirst, Inc*., 365 F. Supp. 3d 1, 9 (D.D.C. 2019) ("Plaintiffs may satisfy the Article III injury-in-fact requirement and yet fail to adequately plead damages for a particular cause of action."). Where, as here, plaintiffs' claim is merely that "they have a heightened fear of having their identities stolen in the future and have, as a result, taken steps to monitor their credit more vigilantly," these allegations lack a "high degree of probability that a future injury will occur" for purposes of pleading damages for negligence. *Hammond* v. *Bank of N.Y. Mellon Corp.*, No. 08 Civ. 6060 (RMB)(RLE), 2010 WL 2643307, at *10 (S.D.N.Y. June 25, 2010) (citation and internal quotation marks omitted); *see also Caudle*, 580 F. Supp. 2d at 282 ("New York would not allow a negligence [claim] to proceed" where no factors demonstrating a serious concern over misuse of stolen data were present).

* * *

Morgan Stanley respectfully submits that the SAC should be dismissed, with prejudice. This court "is not required to grant leave to amend where an amendment would be futile because it could not cure the deficiencies in the original complaint." *Wallace* v. *Conroy*, 945 F. Supp. 628, 639 (S.D.N.Y. 1996) (citations omitted). Here, plaintiffs have had the benefit of nearly nine months of discovery and of numerous amendments; dismissal with prejudice is proper.

CONCLUSION

For the foregoing reasons, Defendant Morgan Stanley respectfully requests that plaintiffs' Complaint be dismissed with prejudice.

Dated: Washington, D.C.
August 9, 2021

PAUL, WEISS, RIFKIND, WHARTON & GARRISON LLP

By: */s/ Jane B. O'Brien*

Brad S. Karp
Susanna M. Buergel
1285 Avenue of the Americas
New York, New York 10019
Telephone: (212) 373-3000
Facsimile: (212) 757-3990
bkarp@paulweiss.com
sbuergel@paulweiss.com

Jane B. O'Brien
2001 K Street NW
Washington, DC 20006
Telephone: (202) 223-7300
Facsimile: (202) 223-7420
jobrien@paulweiss.com

Attorneys for Defendant
Morgan Stanley Smith Barney LLC