UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

In re Morgan Stanley Data Security Litigation	1:20-cv-5914 (AT) **ORAL ARGUMENT REQUESTED**

REPLY MEMORANDUM OF LAW IN FURTHER 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 reply memorandum of law in further support of its motion to dismiss plaintiffs' Second Consolidated Amended Complaint ("Complaint" or "SAC") (ECF No. 60) pursuant to Fed. R. Civ. P. 12(b)(1) and 12(b)(6).

I. PLAINTIFFS FAIL TO PLEAD ARTICLE III STANDING

A. Plaintiffs Lack Standing under the *McMorris* Test

Plaintiffs' primary theory of standing is that they face "a substantially increased risk of identity theft." (Opp'n 7–13.)[1] As such, whether plaintiffs have adequately pleaded an injury-in-fact is governed by the three-factor test established earlier this year by the Second Circuit in *McMorris* v. *Carlos Lopez & Assocs., LLC*, 995 F.3d 295 (2d Cir. 2021). As explained in Morgan Stanley's opening brief, a straightforward application of those factors mandates dismissal of the SAC for lack of Article III standing. (*See* Def. Mem. 8–18.)

In response, plaintiffs mischaracterize and misapply *McMorris*. Most notably, plaintiffs entirely miss the point of the "[f]irst, and ***most important***[]" factor in any analysis of an "increased-risk" theory of standing—i.e., "whether the data at issue has been compromised ***as a result of a targeted attack*** intended to obtain the plaintiffs' data." *McMorris*, 995 F.3d at 301 (emphases added). This factor provides a means for courts to assess the likelihood of identity theft or fraud (and thus injury-in-fact), because data stolen as part of a targeted attack by a bad actor is much more likely to result in cognizable harm, for obvious reasons. There is no dispute that Morgan Stanley's customer data was not targeted and stolen by a malicious actor. Plaintiffs therefore cannot satisfy the "most important" *McMorris* factor.

---

[1] Capitalized terms have the definitions provided in Morgan Stanley's Memorandum of Law in Support of the Motion to Dismiss (ECF No. 64) (also cited herein as "Def. Mem."). Plaintiffs' Memorandum in Opposition (ECF No. 68) is cited herein as "Opp'n."

Unable to point to an intentional data breach, cyberattack, phishing, or malware scheme that are the usual hallmarks of data suits in which courts have found standing, plaintiffs focus instead on the purported "egregiousness" of Morgan Stanley's alleged misconduct in connection with the data center device decommissioning and hardware refresh program underlying the 2016 and 2019 Events. (Opp'n 13.) Plaintiffs ague that "[t]his case is not the result of a mistake," but rather is "the result of Morgan Stanley's systemic failure to implement industry-standard practices." (Opp'n 7). In other words, plaintiffs would have the Court treat this as a "bad-actor" case rather than a "lost-data" case because of *Morgan Stanley*'s supposedly "bad" behavior. But for all of plaintiffs' breathless hyperbole, none of their allegations support Article III standing under *McMorris*. In a lost-data case such as this one, the absence of allegations of a malicious actor or other link between the lost data to actual misuse means that there is no basis to presume that the lost data is *actually being misused*. Thus, even assuming that plaintiffs' incendiary allegations are true,[2] they simply have no relevance to the threshold issue of standing. *See McMorris*, 995 F.3d at 300 (citing *Susan B. Anthony List* v. *Driehaus*, 573 U.S. 149, 158 (2014)).[3]

---

[2] When deciding subject matter jurisdiction, although the court must accept as true the facts alleged in the complaint, "argumentative inferences favorable to the party asserting jurisdiction should not be drawn." *Buday* v. *N.Y. Yankees P'ship*, 486 F. App'x 894, 895 (2d Cir. 2012) (citation and quotation marks omitted).

[3] Plaintiffs' attempts to distinguish *TransUnion LLC* v. *Ramirez*, 141 S. Ct. 2190 (2021), and *In re Science Applications International Corp. Backup Tape Data Theft Litigation*, 45 F. Supp. 3d 14 (D.D.C. 2014), fall flat. Plaintiffs suggest that the Supreme Court's recent decision has already been abrogated by a South Carolina district court. That court distinguished *TransUnion* in part because it arose at a later stage in litigation. *See In re Blackbaud, Inc., Customer Data Breach Litig.*, No. 3:20-MN-02972-JMC, 2021 WL 2718439, at *6 (D.S.C. July 1, 2021). But that distinction is unavailable here, given the extensive development of the record. Furthermore, the data at issue in *Blackbaud* was implicated in a plot by "cybercriminals" who "orchestrated a two-part ransomware attack on Blackbaud's system." *Id.* at *1. Plaintiffs attempt to distinguish this case from *In re Science Applications* by emphasizing that here, the at-issue devices contain allegedly accessible PII. But there, as here, "until [p]laintiffs can aver that their records have been viewed (or certainly will be viewed), any harm to their privacy remains speculative." 45 F. Supp. 3d at 29.

Plaintiffs also fail to distinguish the facts of *McMorris*, which is on all fours with this case (*see* Def. Mem. 8–10), and otherwise ignore or mischaracterize the growing body of law explaining why plaintiffs in lost-data cases such as this one lack Article III standing (*see id.* 10–11 (collecting cases)). For example, in *Beck* v. *McDonald*, upon which the *McMorris* court relied, a laptop containing "unencrypted personal information of approximately 7,400 patients, including names, birth dates, the last four digits of social security numbers, and physical descriptors" was lost, and an investigation determined that "the laptop was likely stolen." 848 F.3d 262, 267 (4th Cir. 2017). Even though the laptop was stolen and the patient data was highly sensitive, the Fourth Circuit rejected plaintiffs' "substantial risk" theory because "even after extensive discovery, the *Beck* plaintiffs have uncovered no evidence that the information contained on the stolen laptop has been accessed or misused or that they have suffered identity theft, nor, for that matter, that the thief stole the laptop with the intent to steal their private information." *Id.* at 274–75.[4] Likewise here, notwithstanding plaintiffs' extensive investigation and over nine months of discovery, they have uncovered no evidence that any customer data from the devices at issue has been accessed and misused—and have entirely failed to plead any such access and misuse.[5]

Plaintiffs attempt to distinguish *Beck* by pointing to their expert's analysis of a Morgan Stanley device that was recovered through discovery in this litigation (Opp'n 5, 9, 12), but this is a red herring. It is hardly surprising that a forensic expert who was retained and paid to search for

---

[4] One of the named plaintiffs in *Beck* did testify to several unauthorized credit card charges, but she "failed to attribute those charges to the 2013 laptop theft"—much like the scattered instances of identity theft pleaded by plaintiffs in this case. *Id*. at 274 n.6.

[5] Plaintiffs' reliance on *Hutton* v. *National Board of Examiners in Optometry, Inc.*, 892 F.3d 613, 621 (4th Cir. 2018) is misplaced: each named plaintiff pled a nexus between the alleged data misuse to the breach at issue because each plaintiff had provided the particular PII misused (maiden names). *See id.* at 621 (observing that "a mere compromise of personal information, without more, fails to satisfy the injury-in-fact element in the absence of an identity theft.").

data on a device that he was told contained unencrypted PII related to Morgan Stanley customers in fact—after considerable effort requiring highly technical expertise and equipment—was able to find some. That is a far cry from a random individual possessing the necessary expertise and equipment searching eBay, purchasing a piece of used equipment that they had no reason to suspect previously belonged to Morgan Stanley (or, indeed, any other bank or financial institution) or still contained any unencrypted data, and then spending the time and money to access the data on the device with the hope that this randomly identified piece of equipment actually contained PII. This is precisely the sort of "attenuated chain of possibilities" that negates Article III standing. *See Clapper* v. *Amnesty Int'l USA*, 568 U.S. 398, 410 (2013).[6]

Plaintiffs' allegations regarding "Mr. Oklahoma" and his supposed "unfettered access" to Morgan Stanley customer PII are likewise unavailing. (Opp'n 2–3.) Even assuming that Mr. Oklahoma did access PII on the Morgan Stanley drives that he acquired on eBay,[7] plaintiffs do not contend that any of the data was retained or misused by Mr. Oklahoma. Plaintiffs' allegations of accessibility, therefore, do not suffice to establish standing in this case.

Plaintiffs also have failed to satisfy the second *McMorris* factor, which enquires into "whether any portion of the dataset has already been misused . . . ." *McMorris*, 995 F.3d at 303.

---

[6] Plaintiffs argue that certain of Morgan Stanley's arguments should be disregarded as outside the record. (Opp'n 7.) But plaintiffs make repeated allegations that their expert was able to find data on Morgan Stanley's devices by searching a forensic image of the drives. (¶ 41.) Plaintiffs thus "rel[y] heavily upon" the "effect" of this evidence, and as such, the Court may consider Morgan Stanley's arguments as to this evidence. *See Chambers* v. *Time Warner, Inc.*, 282 F.3d 147, 153–54 (2d Cir. 2002).

[7] Plaintiffs have selectively mischaracterized the record as it pertains to Mr. Oklahoma, his access to any Morgan Stanley data, and his dealings with Morgan Stanley. In Mr. Oklahoma's deposition—which plaintiffs quote from in their complaint (¶ 7(l))—he testified that he did not see any Morgan Stanley customer data. ("Q. Mr. [Oklahoma], did you at any time access any of Morgan Stanley's customers' PII on the assets that you acquired from Kruzecom [sic]? A. No, ma'am. I didn't let it be possible to do that.")

In their opposition, plaintiffs simply repeat the boilerplate and scattershot allegations of data misuse from the SAC, but they never address their failure to link (temporally or otherwise) any such alleged misuse that occurred *after* their complaint was filed to the 2016 Event (which is the only Event for which they are alleged to have received notice). (*See* Def. Mem. 12–14; ¶¶ 59–67, 198.) The lengthy passage of time between the loss of the data and the complained-of misuse further undermines plaintiffs' standing arguments. *See Beck*, 848 F.3d at 275 ("[A]s the breaches fade further into the past," plaintiffs' "threatened injuries become more and more speculative." (citation and quotation marks omitted)); *In re Zappos.com*, 108 F. Supp. 3d 949, 958 (D. Nev. 2015) ("[T]he passage of time without a single report from plaintiffs that they in fact suffered the harm they fear must mean something.").[8] Furthermore, if plaintiffs' theory had any merit, they would have pled concrete instances of actual data misuse and identity theft. Indeed, according to plaintiffs, there are *thousands* of devices each bearing the PII of *hundreds of thousands of* individuals that are in the hands of "*[c]ountless* . . . internet purchasers." (*See* ¶¶ 7(o)–(p).)

As for the third *McMorris* factor, plaintiffs do not address Morgan Stanley's argument that even though the data at issue is sensitive, the circumstances of its disclosure still weigh against a

[8] Plaintiffs reliance on *In re Equifax Inc. Customer Data Sec. Breach Litig.*, 999 F.3d 1247 (11th Cir. 2021), is misplaced, because (like all the other cases plaintiffs rely on) it involved an intentional hack. Plaintiffs also fail to distinguish the authority cited in Morgan Stanley's opening brief. (*See* Def. Mem. at 13–14.) Plaintiffs do not even address *Welborn* v. *IRS*, 218 F. Supp. 3d 64, 79–80 (D.D.C. 2016) (traceability element of standing is not satisfied where plaintiff "simply allege[d] that the alleged financial fraud happened *after*" the breach,") or *Kimbriel* v. *ABB, Inc.*, No. 19-CV-215-BO, 2019 WL 4861168, at *2–*3 (E.D.N.C. Oct. 1, 2019) (plaintiffs failed to establish Article III standing for data breach where the only alleged harm was scattered instances of credit inquiries.). Although plaintiffs discuss *Fernandez* v. *Leidos, Inc.*, 127 F. Supp. 3d 1078, 1087 (E.D. Cal. 2015), they do not (and cannot) challenge its primary holding, that the plaintiff had not shown any alleged risk of future identity theft, in part because the passage of time since the incident was so prolonged. The other cases cited by plaintiffs on page 12 of their brief as "uniformly h[olding] that allegations similar to Plaintiffs as to traceability are sufficient to survive a Rule 12 motion" all involved intentional hacks.

finding of standing. (Def. Mem. 15.) Indeed, in *McMorris*, the Second Circuit held "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." 995 F.3d at 304.

B. Alleged Subsequent Out-of-Pocket Expenses Do Not Establish Standing

As explained in Morgan Stanley's opening brief, *McMorris* squarely held that out-of-pocket expenses alone cannot independently establish standing. (*See* Def. Mem. at 18–19.) Those expenditures must be coupled with plausible allegations of "a substantial risk of future identity theft," which are analyzed using the Second Circuit's three-factor test discussed above. *McMorris*, 995 F.3d at 303. Plaintiffs have not cited a single post-*McMorris* case to the contrary. (Opp'n at 14–15.)

C. Plaintiffs' Benefit-of-the-Bargain Theory Does Not Confer Standing

Plaintiffs' opposition confirms that they have not pleaded any connection between payments made to Morgan Stanley and the storage or alleged loss of their data. They merely plead, in a conclusory fashion, that they made payments to Morgan Stanley that would not have been made "had [Morgan Stanley] disclosed that it lacked data security practices adequate to safeguard customers' PII." (¶¶ 266; 276; 287; 297; 309; 321; 330; 340; 350.) These threadbare allegations are too attenuated to confer standing. *See 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." (citing *In re Zappos.com, Inc.*, 108 F. Supp. 3d at 962 n.5)).

Plaintiffs' reliance on *Wallace* v. *Health Quest Systems, Inc*., 20 CV 545 (VB), 2021 WL 1109727, at *8 (S.D.N.Y. March 23, 2021), as holding that similar allegations satisfy benefit of

the bargain damages is unavailing. *Wallace*, yet again, involved an intentional hack, and the court in *Wallace* found standing primarily on the basis that the plaintiffs there "allege[d] their sensitive Private Information was accessed by unknown third parties and they are thereby exposed to a high degree of risk of identity fraud and future economic harm." *Id.* at *5.

Other courts have squarely rejected benefit-of-the-bargain theories of standing in data breach cases, where plaintiffs do not allege that they actually read and relied on a privacy policy. *See In re LinkedIn User Privacy Litigation*, 932 F. Supp. 2d 1089, 1094 (N.D. Cal. 2013) ("Because a causal connection between a defendant's actions and plaintiff's alleged harm is required for standing, plaintiffs have not established standing based on an alleged misrepresentation."); *see also In re Sci. Applications*, 45 F. Supp. 3d at 30 ("To the extent that [p]laintiffs claim that some indeterminate part of their premiums went toward paying for security measures, such a claim is too flimsy to support standing.").

With respect to their Section 349 claim, plaintiffs do not meaningfully address *Transunion*, which made clear that a mere violation of a statutory provision alone does not necessarily constitute an injury-in-fact for Article III standing. *See TransUnion*, 141 S. Ct. at 2205. Plaintiffs' reliance on *Dubuisson* v. *Stonebridge Life Ins. Co*., 887 F.3d 567 (2d Cir. 2018), for the proposition that a violation of Section 349 suffices for articulating an injury-in-fact is unavailing, as plaintiffs there suffered harm by paying premiums for a facially illegal policy and it was indisputable that the prices were inflated because the policy itself was illegal. Here, plaintiffs have not plausibly alleged that the price they paid for investment management services was impacted by data security practices. Plaintiffs cannot manufacture a cognizable injury simply by arguing that there has been a statutory violation.

D. Standing Cannot Be Premised on Alleged Diminution of Value of PII

Finally, plaintiffs have not stated a theory of standing based on diminution of the value of

their PII. Plaintiffs argue that this is a valid theory of harm because plaintiffs' PII is "the type of PII commonly sold on the dark web." (Opp'n 16.) This argument is insufficient, and the case that plaintiffs rely on, *Wallace*, actually considered a diminution-of-value theory of damages (not standing) and nonetheless rejected it, because the plaintiffs there only speculated about the value of their PII on that market, did not allege how they could have monetized their private information, and did not allege that their PII was actually monetized. 2021 WL 1109727, at *8.[9] So too here.

II. EACH OF PLAINTIFFS' CLAIMS FAIL AS A MATTER OF LAW

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

As explained in Morgan Stanley's opening brief, plaintiffs have failed to plead causation or damages with respect to their negligence claim. Plaintiffs do not address these arguments—except to say that "to the extent Morgan Stanley rehashes its standing-related argument. . . those arguments fail on the same basis as its standing arguments"—and they disregard the many cases cited in support of Morgan Stanley's position. (*See* Def. Mem. 22–23; *see also 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."). Plaintiffs have thus waived any further arguments with respect to these elements.

Plaintiffs also have failed to adequately allege the other elements of their negligence claim. As explained in Morgan Stanley's opening brief, plaintiffs' allegations that Morgan Stanley's data policies or practices deviated from an acceptable industry baseline or standard are too perfunctory to plead a breach of any duty. *See MLSMK Inv. Co.* v. *JP Morgan Chase & Co*., 431 F. App'x 17, 20 (2d Cir. 2011) (summary order) (affirming dismissal where allegations of breach of duty were

[9] *In re Anthem, Inc. Data Breach Litigation*, No. 15-MD-02617-LHK, 2016 WL 3029783, at *15 (N.D. Cal. May 27, 2016), which plaintiffs also cite, considered diminution of value for purposes of damages, not for standing.

conclusory). In response, plaintiffs cite only inapposite, out-of-circuit cases applying non-New York law. (Opp'n 17–18 (citing *In re Equifax, Inc., Customer Data Sec. Breach Litig.*, 362 F. Supp. 3d 1295, 1325–26 (N.D. Ga. 2019) (construing duty under Georgia law, which recognizes a broad, general duty "to all the world not to subject them to an unreasonable risk of harm"); *In re Arby's Rest. Grp., Inc., Litig.*, No. 17-cv-0514-AT, 2018 WL 2128441, at *3–*5 (N.D. Ga. Mar. 5, 2018) (same); *In re Target Corp. Customer Data Sec. Breach. Litig.*, 64 F. Supp. 3d 1304, 1309–10 (D. Minn. 2014) (under Minnesota law, "a defendant owes a duty to protect a plaintiff when action by someone other than the defendant creates a foreseeable risk of harm to the plaintiff and the defendant and plaintiff stand in a special relationship"); *Brush* v. *Miami Beach Healthcare Grp., Ltd.*, 238 F. Supp. 3d 1359, 1365 (S.D. Fla. 2017) (referencing Florida law, which states that there is a generalized duty to safeguard private information); *In re Marriott Int'l, Inc., Customer Data Sec. Breach Litig.*, 440 F. Supp. 3d 447, 479–81 (D. Md. 2020) (applying Georgia law).)[10]

Plaintiffs are also incorrect that courts have "repeatedly held" that statutes like the FTC Act can be used to "establish evidence of the standards or care." The cases they cite held no such thing. *Cf. Marshall* v. *Conway Reg'l Med. Ctr.*, No. 20-CV-00933 JM, 2020 WL 5746839, at *2 (E.D. Ark. Sept. 25, 2020) (no federal jurisdiction for a negligence claim relying on a standard of care derived from the FTC Act); *C.J. by & through Brady* v. *Truman Med. Ctr., Inc.*, No. 20-CV-00261-DGK, 2020 WL 3473651, at *3 (W.D. Mo. June 25, 2020) (same).

Plaintiffs raise the unremarkable point that their allegations at the pleading stage are subject to a lower threshold than at summary judgment, and that this is especially true where specific

[10] *Morgan Stanley & Co. Inc.* v. *JP Morgan Chase Bank, N.A.*, 645 F. Supp. 2d 248, 252 (S.D.N.Y. 2009), involved claims that a rent check was intercepted, fraudulently endorsed, and deposited in an account at Morgan Stanley and is not a data breach case. *In re Michaels Stores Pin Pad Litig.*, 830 F. Supp. 2d 518, 521–22 (N.D. Ill. 2011), involved actual theft of credit card information from pin pads at Michaels' stores, and is therefore inapplicable.

details regarding the injury suffered may not be accessible until after discovery.[11] Plaintiffs fail to acknowledge that, here, they have the benefit of over nine months of discovery, including 31,000 documents produced by Morgan Stanley spanning 163,715 pages, productions from 10 third parties, numerous witness interviews, and two depositions. Furthermore, allegations about their own injuries clearly are within the control of plaintiffs themselves.

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

1. Plaintiffs' Section 349 Claim Is Time-Barred

Plaintiffs argue that the issue of whether their Section 349 claim is time-barred cannot be decided at the pleading stage, because "it is an affirmative defense." (Opp'n 20.) But it is perfectly appropriate to raise a statute-of-limitations argument on a motion to dismiss where, as here, the complaint "clearly shows that the claim is out of time." *Zorrilla* v. *Carlson Rests. Inc.*, 255 F. Supp. 3d 465, 479 (S.D.N.Y. 2017); *see also Healthcare Strategies, Inc.* v. *ING Life Ins. & Annuity Co.*, No. 11-CV-282, 2021 WL 162361, at *3 (D. Conn. Jan. 19, 2012). The dates during which plaintiffs' accounts were open are set forth in the SAC—and these are the dates on which plaintiffs' Section 349 claims accrued. (¶¶ 59–67; *see also* Opp'n 13.) As discussed in Morgan Stanley's opening brief, plaintiffs' alleged "injury accrued as soon as [defendant] placed their personal information into its . . . network." (Def. Mem. at 24 (citing *Fero* v. *Excellus Health Plan, Inc.* 502 F. Supp. 3d 724, 736 (W.D.N.Y. 2020)).)[12]

---

[11] *Hinds Cty., Miss.* v. *Wachovia Bank N.A.*, 700 F. Supp. 2d 378, 385–86 (S.D.N.Y. 2010), is not a data breach case. *Mackey* v. *Belden, Inc.*, No. 21-CV-00149-JAR, 2021 WL 3363174, at *1, *6 (E.D. Mo. Aug. 3, 2021), is an out-of-circuit data breach case involving an intentional hack, and is also distinguishable.

[12] To the extent plaintiffs argue that Section 899-aa precludes Morgan Stanley from raising a statute of limitations defense, they are incorrect. Section 899-aa requires disclosure only where PII was, or is reasonably believed to have been, accessed or acquired by a person without valid authorization. NYGBL § 899-aa(2). Following a reasonable investigation and consultation with experts, Morgan Stanley found no evidence that any client data was "acquired by a person

Plaintiffs attempt to distinguish *Fero* by arguing that it involved a one-time misrepresentation, whereas this case involves "annual misrepresentations." But *Fero* makes clear that Section 349 claims accrue not whenever privacy notices are provided, but rather "when [the defendant] allegedly failed to provide the cybersecurity measures it had promised" and the case was dismissed for the "numerous putative class members whose claims are time-barred on their face." 502 F. Supp. 3d at 737–38. The same outcome is warranted here.

Plaintiffs' argument that Morgan Stanley is equitably estopped from raising a statute of limitations defense is similarly unavailing. Plaintiffs do not allege that Morgan Stanley took "subsequent . . . specific actions . . . separate from those that provide the factual basis" of plaintiffs' suit, and that "those subsequent actions somehow kept the plaintiff from timely bringing suit." *Shoreham Hills, LLC* v. *Sagaponack Dream House, LLC*, No. 613802-19, 2020 WL 1127071, at *2 (N.Y. Sup. Ct. Mar. 4, 2020). Defendants must make a new material misrepresentation or deceptive act beyond the complained-of conduct in order to induce a plaintiff to fail to make a timely claim. *Abbas* v. *Dixon*, 480 F.3d 636, 642 (2d Cir. 2007). Equitable estoppel is limited to "extraordinary circumstances" not present here. *Marshall* v. *Hyundai Motor Am.*, 51 F. Supp. 3d 451, 462–63 (S.D.N.Y. 2014).[13]

Finally, plaintiffs argue that the element of "deceptive conduct" or "a fiduciary relationship" for a Section 349 claim is satisfied because Morgan Stanley allegedly "publicly

without valid authorization." Nonetheless, Morgan Stanley promptly disclosed when directed to by the OCC.

[13] Plaintiffs' argument that equitable estoppel is a question of fact that should not be decided at the motion to dismiss phase is incorrect. In fact, the New York Court of Appeals case cited by plaintiffs, *Zumpano* v. *Quinn*, 849 N.E.2d 926, 929–30 (N.Y. 2006), actually decided, at the motion to dismiss phase, whether a statute of limitations was equitably estopped. *Kosakow* v. *New Rochelle Radiology Assocs., P.C.*, 274 F.3d 706, 725 (2d Cir. 2001), did not involve equitable estoppel in the context of a statute of limitations defense, and thus is inapposite.

acknowledges its fiduciary relationship with its clients." (Opp'n 22.) But nowhere have plaintiffs pled that the accounts at issue had the features necessary to give rise to a fiduciary duty. *Banco de La Republica de Colombia* v. *Bank of New York Mellon*, No. 10 Civ. 536(AKH), 2013 WL 3871419, at *11 (S.D.N.Y. July 26, 2013) (investment advisors with "substantial discretion over the investment of their clients' funds owe their clients a fiduciary duty," and investment banks with a more limited role— including a lack of control of their clients' investments—do not have a fiduciary duty). Here, plaintiffs have not alleged that Morgan Stanley exercised discretion over their accounts. *Cf.*, e.g., ¶ 261 (the Nelsons had an IRA account); ¶ 271 (Tillman had a California Uniform Transfers to Minors Act account); ¶ 281 (Blythe had a "stock" account and an annuity account); 292 (Yates had a 529 college savings plan account); ¶ 302 (the Gamens had a brokerage account); ¶ 341 (Jaijee had an IRA account); ¶ 345 (Katz had a "trading" account). Even if there were a fiduciary duty as it pertained to the management of plaintiffs' accounts, courts have been clear that there is no general privacy right in New York. (*See* Def. Mem. 26–27.)

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

First, plaintiffs' Section 349 claim is premised on non-actionable statements. The court in *In re Signet Jewelers Ltd. Sec. Litig.*, 389 F. Supp. 3d 221 (S.D.N.Y. 2019), on which plaintiffs rely, affirmed that the statements in *Singh* v. *Cigna Corp.*, 918 F.3d 57, 63 (2d Cir. 2019), were "general declarations about the importance of acting lawfully and with integrity[.]" 389 F. Supp. 3d at 230–31. These statements were remarkably similar to those at issue here, including that "it's so important for every employee. . .to handle, maintain, and report on [Cigna's financial] information in compliance with all laws and regulations" and that "we have a reasonability to act with integrity in all we do." *Id.* at 231.[14]

[14] To the extent plaintiffs rely on a theory that Morgan Stanley's alleged omissions serve as the basis for a Section 349 claim, they have not pled that plaintiffs were misled to their detriment

Plaintiffs also argue that Morgan Stanley retained customer data beyond the time period permitted by regulations, citing *Nick* v. *Target Corp*., No. CV 15-4423 (GRB), 2017 WL 10442061 (E.D.N.Y. Sept. 13, 2017). *Nick* is inapplicable. In *Nick*, Target stated in their privacy policy that they would not use their customer's PII without their consent; but the plaintiffs there alleged that Target was capturing, collecting, and using customers' data for other purposes, such as targeted marketing. 2017 WL 10442061, at *4. There is no allegation that Morgan Stanley used its customers' PII for unconsented purposes.[15]

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

Plaintiffs have not adequately pleaded that Morgan Stanley was subject to a fiduciary duty in New York. There is no generalized fiduciary duty to secure customer data in New York. *U.S. Bank Nat'l Ass'n* v. *Ables & Hall Builders*, 696 F. Supp. 2d 428, 442 (S.D.N.Y. 2010).[16] In response, plaintiffs cite dicta from a 2004 case hypothesizing that "perhaps," in the event that legislation is not passed, courts "should" apply the fiduciary duty concept from the physician-patient context to commercial transactions, while conceding that "this concept has never before been applied to issues surrounding the protection of confidential information." *Daly* v. *Metro. Life*

by Morgan Stanley's alleged omissions. *Cf. Oswego Laborers' Local 214 Pension Fund* v. *Marine Midland Bank*, 647 N.E.2d 741, 745 (N.Y. 1995).

[15] Plaintiffs cannot state a Section 349 claim where the "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 do not respond to this argument. Their citation to *Wilner* v. *Allstate Ins. Co*., 893 N.Y.S.2d 208, 214–15 (N.Y. App. Div. 2010), adds nothing, as that case is not a data breach case, did not impact the line of New York case law cited in Morgan Stanley' memorandum, and is inapposite.

[16] Plaintiffs' attempt to distinguish *Daly* because it was a summary judgment ruling, but whether there is a general fiduciary duty to secure customer data in New York is a pure question of law.

Ins. Co., 782 N.Y.S.2d 530, 535–36 (Sup. Ct. 2004). This is mere speculation.[17]

D. Plaintiffs Fail to State a Claim for Unjust Enrichment

Plaintiffs hardly address Morgan Stanley's argument that their unjust enrichment claim should be dismissed as duplicative. They simply reiterate that the claim is pleaded in the alternative by citing to the paragraph in their Amended Complaint that labels the claim "alternative," as well as the Federal Rules of Civil Procedure. (*See* Opp'n 28.) But labelling a claim "alternative" does not make it so, as "even pleaded in the alternative, claims for unjust enrichment will not survive a motion to dismiss where plaintiffs fail to explain how their unjust enrichment claim is not merely duplicative of their other causes of action." *Nelson* v. *MillerCoors, LLC*, 246 F. Supp. 3d 666, 679 (E.D.N.Y. 2017). "A claim is alternative and not duplicative if a plaintiff may fail on one but still prevail on the other." *Doe* v. *Indyke*, 465 F. Supp. 3d 452, 459 (S.D.N.Y. 2020) (citation omitted). Plaintiffs' unjust enrichment claim is premised on the same theory, and will rise and fall, on the same proof as their other claims—i.e., that Morgan Stanley's conduct allegedly led to misuse of plaintiffs' data. (*See* Opp'n 28–29.) Plaintiffs do nothing to explain how their claim is not merely duplicative, nor do they explain how they would prevail on their claim for unjust enrichment but not prevail on their claim for negligence.

Plaintiffs have furthermore failed to allege that Morgan Stanley was enriched through any bad act. Each of the cases relied on by plaintiffs are inapposite. (Opp'n 28–29.) For example, *Rudolph* v. *Hudson's Bay Co.*, No. 18-cv-8472 (PKC), 2019 WL 2023713 (S.D.N.Y. May 7, 2019), dealt with a far more straightforward example of enrichment, in which (i) a plaintiff made a purchase at Saks, (ii) she allegedly would not have purchased the merchandise if Saks had not

[17] Plaintiffs' reliance on *Jones* v. *Com. Bancorp, Inc.*, No. 06 Civ. 835(HB), 2006 WL 1409492, at *3 (S.D.N.Y. May 23, 2006), is similarly misplaced, as that case involved a Bank's authorization of fraudulent withdrawals from a customer's account, not a loss of data.

accepted her debit card, and (iii) the purchase of merchandise conferred a direct benefit on Saks. *Id*. at *12.[18] Here, by contrast, plaintiffs' allegations of enrichment are pure speculation. Plaintiffs argue that Morgan Stanley must have been enriched based on their unsubstantiated allegation that Morgan Stanley retained former clients' data for too long. (Opp'n 28.) Plaintiffs cannot plead a claim for unjust enrichment relying on pure conjecture.

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

Plaintiffs claim that they have stated a cause of action for breach of confidence under New York law, yet the primary case they rely on, *Chanko* v. *Am. Broad. Cos.*, 27 N.Y.3d 46, 53–54 (2016), involved breach of patient confidentiality in the context of a physician-patient relationship. *Cf. Daly*, 782 N.Y.S.2d at 535 (noting that breach of confidence is "derived" from the physician-patient relationship"); *Wallace*, 2021 WL 1109727, at *13 (PII was medical in nature).[19]

CONCLUSION

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

---

[18] *In re JetBlue Airways Corp. Priv. Litig.*, 379 F. Supp. 2d 299, 330 (E.D.N.Y. 2005), cited by plaintiffs, does not demonstrate that client data has extrinsic value, and in fact is irrelevant. The court in JetBlue dismissed an unjust enrichment claim and did not even consider the length of time that data was kept, let alone a length of time that was required by law.

[19] The other cases relied on by plaintiffs fare no better. *Kamal* v. *J. Crew Grp., Inc.*, 918 F.3d 102, 114 (3d Cir. 2019) held that the plaintiff did not allege a sufficiently concrete injury because no third party had gained unauthorized access to his data. So too, here. The other cases apply non-New York law. *See In re Cap. One Consumer Data Sec. Breach Litig.*, 488 F. Supp. 3d 374, 408–11 (E.D. Va. 2020) (Virginia, Florida, and California law); *McGuire* v. *Shubert*, 722 A.2d 1087, 1091 (Pa. Super. Ct. 1998) (Pennsylvania law).

Dated: Washington, DC
September 29, 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, NY 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