UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA

Case No. 25-cv-23184-BLOOM/Elfenbein

WILLIAM MANNING,
individually and on behalf
of all others similarly situated,

Plaintiff,

v.

ZUMPANO PATRICIOS, P.A.,

Defendant.
_____/

ORDER ON MOTION TO DISMISS CLASS ACTION COMPLAINT

THIS CAUSE is before the Court upon Defendant Zumpano Patricios, P.A.'s Motion to Dismiss Plaintiff's Class Action Complaint ("Motion"), ECF No. [12]. Plaintiff William Manning ("Manning") filed a Response in Opposition, ECF No. [17], to which Defendant filed a Reply, ECF No. [18]. For the reasons that follow, Defendant's Motion is granted.

I. BACKGROUND

This putative class action arises from a 2025 cyber-hacking event of Defendant's servers. According to the Complaint, "Defendant acquired, collected and stored [Plaintiff's and the Putative Class Members'] "protected health information and personally identifiable information . . . including, without limitation, [their] name, member ID number, health insurer information, date of birth, and amounts charged by [their] providers, and the payment amount received for the services" (collectively referred to as "Private Information") in a database on its servers. ECF No. [1] at ¶¶ 1,4. Plaintiff and the Putative Class Members were required to provide this Private Information "in order to receive services and/or employment." ECF No. [1] at ¶ 35. Consequently, "Defendant assumed legal and equitable duties over the Private Information" and knew it was

responsible for protecting the data from any unauthorized disclosures. *Id.* at ¶ 40. Therefore, when Plaintiff and the Putative Class Members provided Private Information to Defendant, there was a "mutual understanding," and a reasonable expectation "that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access." *Id.* at ¶ 35. However, on May 6, 2025, "cybercriminals infiltrated Defendant's inadequately protected network and accessed the Private Information which was being kept under-protected (the 'Data Breach.')." *Id.* at ¶ 4.

As a result of Defendant's failure to take reasonably appropriate precautionary measures,[1] Plaintiff's and the Putative Class Member's "Private Information was compromised through disclosure to an unknown and unauthorized third party[.]" *Id.* at ¶ 5. Plaintiff is still unsure about "what particular data was stolen" and is "left to speculate as to where their Private Information ended up, who has used it and for what potentially nefarious purposes." *Id.* at ¶ 36. However, the health records that were disclosed contained "a plethora of sensitive information . . . that is valuable to cybercriminals"[2] who can sell that sensitive information on the "cyber black market." *Id.* at ¶ 57. Therefore, Plaintiff maintains that the cybercriminal's intent was to misuse their "Private Information, including marketing and selling [their] Private Information." *Id.* at ¶ 33. Accordingly, Plaintiff believes his and the Putative Class Members' "Private Information may end up for sale on the dark web, or simply fall into the hands of companies that will use the detailed Private Information for targeted marketing without [their] approval. *Id.* at ¶ 37. According to Plaintiff, "[t]hese criminal activities have and will result in devasting financial and personal losses" and the

[1] Plaintiff asserts that "Defendant could have prevented the Data Breach by properly securing and encrypting and/or more securely encrypting its servers generally, as well as [Plaintiff's] Private Information. ECF No. [1] at ¶ 42.

[2] Plaintiff claims that "[o]ne patient's complete record can be sold for hundreds of dollars on the dark web." ECF No. [1] at ¶ 57.

potential for "fraud will be an omnipresent threat for [Plaintiff and the Punitive Class Members] for the rest of [their life]." *Id.* at ¶ 60. Furthermore, Plaintiff asserts that, as a result of Defendant's negligence, Plaintiff and the Putative Class Members have suffered and will continue to suffer the following injuries:

> (i) actual identity theft, (ii) the loss of the opportunity of how their Private Information is used, (iii) the compromise, publication and/or theft of their Private Information, (iv) out-of-pocket expenses associated with the prevention, detection and recovery from identity theft, tax fraud and/or unauthorized use of their Private Information, (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest and recover from embarrassment and identity theft, (vi) lost continuity in relation to their personal records, (vii) the continued risk to their Private Information, which may remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Representative Plaintiff's and Class Members' Private Information in its continued possession, and (viii) future costs in terms of time, effort and money that will be expended to prevent, detect, contest and repair the impact of the Private Information compromised as a result of the Data Breach

Id. at ¶ 95. Furthermore, because of Defendant's negligence, Plaintiff has "suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy . . . the continued risk of exposure of [his] private information," and other economic and noneconomic losses. *Id.* at ¶¶ 96-97.

Due to the Data Breach and his resulting injuries, Plaintiff brought the instant action asserting the following claims: (1) Negligence; (2) Breach of Implied Contract; and (3) Breach of Implied Covenant of Good Faith and Fair Dealing. *See id.* Defendant filed the instant Motion seeking to dismiss the Complaint in its entirety because Plaintiff lacks standing and has failed to state a claim upon which relief may be granted. *See* ECF No. [12]. Plaintiff responds that he has not only adequately alleged each of his claims, but he has also sustained a sufficiently concrete

injury that is imminent, thereby conferring standing to bring the instant action. *See* ECF No. [17]. The matter being fully briefed is now ripe for consideration.

II. LEGAL STANDARD

Under Article III of the Constitution, federal courts are limited to adjudicating only "Cases and Controversies." U.S. Const Art. III § 2; *see Stalley ex rel. U.S. v. Orlando Regional Healthcare System, Inc.*, 524 F.3d 1299, 1232 (11th Cir. 2008). For a case or controversy to exist, the Plaintiff must have standing to bring the action. *See I.L. v. Alabama*, 739 F.3d 1273, 1278 (11th Cir. 2014) ("Standing is one of the Article III case or controversy requirements."). "Because standing is jurisdictional, a dismissal for lack of standing has the same effect as a dismissal for lack of subject matter jurisdiction under Fed. R. Civ. P. 12(b)(1)." *Cone Corp. v. Fla. Dep't of Transp.*, 921 F.2d 1190, 1203 n.42 (11th Cir. 1991). "The party invoking federal jurisdiction bears the burden of proving standing." *Fla. Pub. Int. Research Grp. Citizen Lobby, Inc. v. E.P.A.*, 386 F.3d 1070, 1083 (11th Cir. 2004). However, "[a]t the pleading stage, general factual allegations of injury resulting from the defendant's conduct may suffice, for on a motion to dismiss [courts] 'presum[e] that general allegations embrace those specific facts that are necessary to support the claim.'" *Lujan*, 504 U.S. at 561 (quoting *Lujan v. Nat'l Wildlife Fed'n*, 497 U.S. 871, 889 (1990)). "But this does not mean that *any* allegations of injury can push a plaintiff across the standing threshold. Rather, a plaintiff must set forth general factual allegations that 'plausibly and clearly allege a concrete injury[.]"' *Tsao v. Captiva MVP Rest. Partners, LLC*, 986 F.3d 1332, 1337-38 (11th Cir. 2021) (emphasis in the original) (quoting *Thole v. U.S. Bank N.A.*, 590 U.S. 538, 544 (2020)); *see also Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) ("[M]ere conclusory statements[ ] do not suffice.").

"To have standing, the plaintiff[] must demonstrate injury in fact, causation, and redressability." *Id.* All three must exist before a federal court may exercise jurisdiction over the case. *See Havana Docks Corp. v. Norwegian Cruise Line Holdings, Ltd.*, 484 F. Supp. 3d 1215,

1225 (S.D. Fla. 2020). "The 'foremost' standing requirement is injury in fact." *Trichell v. Midland Credit Management, Inc.*, 964 F.3d 990, 996 (11th Cir. 2020) (quoting *Steel Co. v. Citizens for a Better Environment*, 523 U.S. 83, 99 (1998)). "An injury in fact is 'an invasion of a legally protected interest which is (a) concrete and particularized, and (b) actual or imminent, not conjectural or hypothetical.'" *I.L.*, 739 F.3d at 1278; *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560 (1992). "A 'concrete' injury must be 'de facto'—that is, it must be 'real, and not abstract.'" *Trichell*, 964 F.3d at 996 (quoting *Spokeo, Inc. v. Robins*, 578 U.S. 330, 340 (2016)). However, an injury need not yet have occurred to constitute an injury in fact. A harm yet to occur will still satisfy the case and controversy requirement if is "sufficiently substantial and imminent." *DiPierro v. Florida Health Sciences Center, Inc.*, Case No: 8:23-cv-01864-KKM-NHA, 2024 WL 3051320, at *5 (M.D. Fla. June 18, 2024). A harm is imminent if there is "a realistic danger of sustaining a direct injury as a result" of the challenged conduct. *Fla. State Conf. of NAACP v. Browning*, 522 F.3d 1153, 1161 (11th Cir. 2008) (quoting *Babbitt v. United Farm Workers Nat'l Union*, 442 U.S. 289, 298 (1979)).[3] '"How likely is enough is necessarily a qualitative judgment,' but, under our law, 'probabilistic harm is enough injury in fact to confer standing in the undemanding Article III sense[.]"' *Mulhall v. UNITE HERE Local 355*, 618 F.3d 1279, 1288 (11th Cir. 2010) (quoting *Fla. State Conf. of NAACP v. Browning*, 522 F.3d 1153, 1161, 1163 (11th Cir. 2008)).

Ultimately, "[i]mminence" as a doctrinal standard is "somewhat elastic," and applying it is not an exercise in conceptual analysis but an attempt to advance the purposes behind the case-or-controversy requirement of Article III, including the guaranty of actual adversity between the parties, the limitation on the power of federal courts, and the reservation of judicial resources to

[3] "*Merriam–Webster* defines 'imminent' in its online dictionary to mean 'ready to take place; *especially*: hanging threateningly" and provides as an example the "*imminent* danger of being run over[.]" https://www.merriam-webster.com/dictionary/imminent." *See Taylor v. Fred's, Inc.*, 285 F. Supp. 3d 1247, 1259 (N.D. Ala. 2018).

resolve more concrete and pressing disputes[.]" *Browning*, 522 F.3d at 1161 (internal citations omitted)).

III. DISCUSSION

A. Article III Standing—Actual Injury Requirement

a. Whether Increased Risk of Future Misuse Establishes Standing

According to Defendant, to establish Article III standing where the alleged injury is a risk of future harm, the "hypothetical harm alleged [must be] either certainly impending or there [must be] a substantial risk of such harm." ECF No. [12] at 8-9 (quoting *Tsao v. Captiva MVP Rest. Partners, LLC*, 986 F.3d 1332, 1338–39 (11th Cir. 2021) (internal quotations omitted)). Defendant argues that, in this case, "Plaintiff has not alleged any misuse of his personal information or any other actual harm fairly traceable to the cyber-attack on [Defendant]." *Id.* at 9. Rather, Plaintiff merely alleges an "increased risk of future harm" resulting from the potential misuse of his information for activities such as fraud and identify theft. Defendant contends, however, that those future injuries are too uncertain to be certainly impending or to at least have a substantial of risk of occurring. *Id.*

Plaintiff responds that his ongoing risk of future harm is not speculative because "the reason cybercriminals steal this information is to use it to commit identity theft or fraud." ECF No. [17] at 9. Therefore, Plaintiff argues the risk of future injury establishes standing, notwithstanding "that the risk of identity theft and fraud has not yet matured into financial harm." *Id.* at 10. Given the sensitive nature of the information stolen and the likely intentions of the thieves, Plaintiff maintains that there is a substantial and imminent risk of actual harm because the thieves now have the means to commit identity theft and fraud. *See id.* at 10-11.

As the Supreme Court and the Eleventh Circuit have made clear, "a plaintiff alleging a threat of harm does not have Article III standing unless the hypothetical harm is either 'clearly

impending' or there is a 'substantial risk' of such harm." *Tsao v. Captiva MVP Rest. Partners, LLC*, 986 F.3d 1332, 1339 (11th Cir. 2021) (*Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 409 (2013)). Moreover, "[e]vidence of a mere data breach does not, standing alone, satisfy the requirements of Article III standing" and "without specific evidence of some misuse of class members' data, a named plaintiff's burden to plausibly plead factual allegations sufficient to show that the threatened harm or future identity theft was 'certainly impending'—or that there was a 'substantial risk' of such harm—will be difficult to meet." *Tsao*, 986 F.3d at 1344 (citing *Resnick v. AvMed, Inc.*, 693 F.3d 137, 1323 n.1 (11th Cir. 2012) (finding that while plaintiffs who suffer "actual" identify theft typically will have standing, "speculative" identity theft may not be sufficient to confer standing)); *see also In re Fortra File Transfer Software Data Sec. Breach Litig.*, 749 F. Supp. 3d 1240, 1258 (S.D. Fla. 2024) ("Courts 'typically require misuse of the data cybercriminals acquire from a data breach because such misuse constitutes both a present injury and a substantial risk of harm in the future.'") (quoting *Green-Cooper*, 73 F.4th at 888–89) (additional level of citation and quotation omitted)).

While Plaintiff's allegations may establish that he is facing an increased risk of identity theft or fraud, "an increased risk of identity theft [or fraud] has been found to be too speculative to constitute an injury" without further supporting allegations. *In re 21st Century Oncology Customer Data Sec. Breach Litig.*, 380 F. Supp. 3d 1243, 1254 (M.D. Fla. 2019). Here, Plaintiff has failed to assert anything further other than conclusory allegations regarding the misuse of Private Information stolen in the Data Breach.[4] Indeed, Plaintiff readily admits he is merely speculating as to what data was stolen in the Data Breach or where the data is now.[5] *See* ECF No. [1] at ¶ 36

[4] Although Plaintiff claims he and the Class Members have suffered "actual identity theft," Plaintiff offers not facts or details to support this wholly conclusory assertion. ECF No. [1] at ¶ 95.

[5] While Plaintiff alleges that he, along with members of the putative class, provided Defendant their "name,

("representative Plaintiff and the Class Members remain, even today, in the dark regarding what particular data was stolen . . . [and are] thus left to speculate as to where their Private Information ended up, who has used it and for what nefarious purposes.").[6] The Complaint offers no specific details that would suggest any of Plaintiff or the Class Members' Private Information that was stolen has yet to be misused and, as such, Plaintiff has not plausibly established a substantial risk of future harm, let alone that any injury is imminent. *See DiPierro v. Fla. Health Scis. Ctr., Inc.*, 737 F. Supp. 3d 1314, 1323 (M.D. Fla. 2024) ("[P]laintiffs must identify 'specific evidence of some misuse of class members' data' to plead a substantial risk of future harm. [ ] '[V]ague, conclusory allegations that members of the class have suffered' misuse do not suffice, even under a plausibility standard.").

Plaintiff's mere belief that sensitive data will be misused or sold on the dark web is not enough without specific allegations establishing the risk is more than speculative. *See id.* ("The [ ] allegation that Plaintiffs 'believe' the class's private information has been sold on the dark web is not enough either. . .. Plaintiffs' conclusory allegation that they believe their information has been or will be sold because[,]that is the nature of things[,] is speculative.") (citing *Clapper*, 568 U.S. at 414 n.5) (explaining that an "attenuated chain of inferences" and "speculation about the unfettered choices made by independent actors not before the court" is insufficient to satisfy the

member ID number, health insurer information, date of birth, [ ] amounts charged by [their] providers, and the payment amount received for the services" as well as a "plethora of [other] sensitive information (e.g., patient data, patient diagnosis, lab results, medical prescriptions, treatment plans, etc.)," Plaintiff never specifies what data is believed to have been stolen. ECF No. [1] at ¶¶ 1, 57.

[6] Plaintiff further admits that the Private Information "may end up for sale on the dark web, or simply fall into the hands of companies that will use the detailed Private Information for targeted marketing without Representative Plaintiff's and/or Class Members' approval." ECF No. [1] at ¶ 37. Critically, however, Plaintiff has not alleged this type of misuse has occurred.

"substantial risk standard"). Accordingly, the Court finds that Plaintiff's allegations regarding the risk of future injury is too speculative to satisfy the injury-in-fact standard necessary for standing.

b. Plaintiff's Efforts to Mitigate the Risk of Future Misuse of Personal Information Does Not Confer Standing

Defendant contends that Plaintiff's efforts to mitigate his risk of future harm also does not confer standing, given that "plaintiffs 'cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending.'" ECF No. [12] at 13 (quoting *Clapper*, 568 U.S. at 416). Therefore, Defendant maintains that since Plaintiff has failed to adequately allege that he faces a sufficiently imminent future risk of identity theft or fraud, any time, money, or resources Plaintiff has expended to mitigate or avoid the hypothetical harm that may result from the Data Breach does not confer Article III standing. *See id.* at 14-15.

Plaintiff responds that it is "well-established that lost time is a cognizable injury for standing purposes," and when "a plaintiff faces a sufficient risk of harm, the time, money, and effort spent mitigating that risk are also concrete injuries." ECF No. [17] at 11 (quoting *Shiyang Huang v. Equifax Inc. In re Equifax Customer Data Sec. Breach Litig.*), 999 F.3d 1247, 1262 (11th Cir. 2021)). Plaintiff argues that the "exposure of [his] PII/PHI to unknown criminal actors created a [sufficiently] imminent risk of harm" that justified his mitigation efforts. *See id.*

While Plaintiff is correct that under certain circumstances, mitigation efforts may help support a finding of a concrete injury, the Eleventh Circuit has concluded in the data breach context, that "plaintiffs 'cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending.'" *Tsao*, 986 F.3d at 1344 (quoting *Clapper*, 568 U.S. at 416). Accordingly, where there is no substantial or imminent threat of injury, a plaintiff's efforts to avoid or otherwise mitigate the anticipated injury is

insufficient to confer standing. *See In re 21st Century Oncology Customer Data Sec. Breach Litig.*, 380 F. Supp. 3d 1243, 1256 (M.D. Fla. 2019) ("Courts have found that the harm resulting from mitigation of a risk of future harm is largely dependent on whether the risk itself is substantial enough to be a standalone injury. . .. [W]here the risk of identity theft is too speculative to constitute an injury in fact, the alleged injury of mitigation efforts to minimize that risk is likewise typically found to be non-cognizable."); *In re Mednax Servs., Inc., Customer Data Sec. Breach Litig.*, 603 F. Supp. 3d 1183, 1204 (S.D. Fla. 2022) (citing *In re Practicefirst Data Breach Litig.*, No. 21-00790, 2022 WL 354544, at *6 (W.D.N.Y. Feb. 2, 2022) ("Where plaintiffs have shown substantial risk of future identity theft or fraud, any expenses they have reasonably incurred to mitigate that risk likewise qualify as injury in fact. Conversely, 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.") (internal citation and quotations omitted)).

Here, the Court has already determined that Plaintiff has failed to establish a substantial risk of future harm because of the Data Breach. Therefore, the time, energy, and money Plaintiff has put in to trying to avoid or otherwise mitigate any potential future injury may not serve as a basis for establishing an injury in fact.

c. Plaintiff's Other Damages Allegations Do Not Establish an Injury Sufficient to Confer Standing

Defendant's final standing arguments address Plaintiff's other purported harms, including: (1) "actual injury in the form of damages to and diminution in the value of his private information;" and (2) the "anxiety and increased concerns for the loss of privacy, as well as anxiety over the impact of cybercriminals accessing, using and selling his private information." ECF No. [12] at 15-16 (quoting ECF No. [1] at ¶ 16).

Regarding the first allegation, Defendant points out that "courts within this circuit have repeatedly held that plaintiffs did not adequately allege a devaluation of their private information because they did 'not plausibly explain how the data breach could have harmed [the plaintiffs'] abilities to sell their information."' *Id.* (quoting *DiPierro v. Fla. Health Scis. Ctr., Inc.*, 737 F. Supp. 3d 1314, 1325 (M.D. Fla. 2024)). Accordingly, because Plaintiff's Complaint fails to allege that "he has (or ever had) the intention of selling his personal information to anyone" Defendant argues that Plaintiff has failed to show that he has actually been harmed by the potential loss in value of his private information.

As for the alleged anxiety Plaintiff suffered from his loss of privacy and the potential impact of "cybercriminals accessing, using and selling his private information," Defendant argues that such injuries are, once again, not "sufficiently concrete." *Id.* at 16. According to Defendant, in the data breach context, emotional damages only constitute a concrete injury where "allegations of emotional distress are coupled with the substantial risk of future harm." *Id.* Accordingly, because Plaintiff has failed to adequately allege a substantial risk of injury or an injury that is actually imminent, Plaintiff's allegations of anxiety and emotional distress necessarily fail to confer standing as well. *See id.*

Plaintiff responds that the growing trend across courts is not to value a consumer's personal information based on its realistic value in some imagined marketplace, but rather to assume that data breaches devalue a plaintiff's personal information "by interfering with their fiscal autonomy." ECF No. [17] at 14 (quoting *Plaintiffs v. MGM Resorts Int'l*, 638 F. Supp. 3d 1175, 1191 (D. Nev. 2022)). Accordingly, Plaintiff insists that "the Court should follow the modern trend and recognize that the inherent value of [Plaintiff's] PHI/PII is diminished by the loss of its confidential and exclusive nature." *Id.* at 14. Plaintiff further argues that anxiety and emotional

distress from a data breach are concrete harms sufficient to establish standing because an individual may be "independently harmed by their exposure to the risk itself." *Id.* (quoting *TransUnion LLC v. Ramirez*, 594 U.S. 413, 436 437 n. 7 (2021)).

Plaintiff also contends that "[i]nvaision of privacy is 'a harm that has traditionally been regarded as providing a basis for a lawsuit in English or American courts.'" *Id.* at 15. (quoting *Perry v. Cable News Network, Inc.*, 854 F.3d 1336, 1340-41 (11th Cir. 2017)). Therefore, because the Data Breach resulted in the release of Plaintiff's personal information, his privacy was invaded and, as such, he has standing to bring the instant claims.

The Court addresses each of these alleged injuries in turn. First, Plaintiff's conclusory allegation that he was injured by the diminution in value of his Private Information simply because the information was stolen does not establish a concrete injury. As an initial matter, the assumption that Plaintiff has "a property interest in [his Private Information] is a legal conclusion, and an unsupported one at that." *Fraga v. UKG, Inc.*, Case No. 22-20105-CIV, 2022 WL 19486310, at *11 (S.D. Fla. May 10, 2022). Accordingly, Plaintiff's initial premise is "entitled to no assumption of truth." *Id.* (citing *Mamani v. Berzain*, 654 F.3d 1148, 1153 (11th Cir. 2011)). Likewise, Plaintiff's allegation that he "suffered actual injury in the form of damages to and diminution in the value of [his] Private information . . . as a result of the Data Breach," is "little more than 'an unadorned, the-defendant-unlawfully-harmed-me accusation.'" ECF No. [1] at ¶ 15; *Fraga*, 2022 WL 19486310, at *11 (quoting *Iqbal*, 556 U.S. at 678). As such, the allegation is too conclusory to plausibly establish an injury-in-fact.

Moreover, just like the plaintiffs in *DiPierro*, Plaintiff fails to establish that he "has (or ever had) the intention of selling such information to data brokers, legitimate or otherwise." 737 F. Supp. 3d at 1325. This is a critical missing allegation because "at bottom, Plaintiff['s]

diminished-value theory assumes that the [data] breach afforded companies with whom Plaintiff[ ] would voluntarily trade [his] private information access to that information without Plaintiff[']s] permission." *Id.* (quoting *Fraga*, 2022 WL 19486310 at 12). However, if Plaintiff had no intention to sell his data, then its decrease in value in the eyes of these hypothetical buyers would not harm Plaintiff financially given there was previously no prospect of the data being sold at all. And even assuming Plaintiff's Private Information has some inherent value, given that Plaintiff might indeed elect to sell the information at some point in the future, the assumption that the market for his information would be weaker as a result of these cybercriminals making it available through other means is, at best, "impermissible 'speculation about the unfettered choices made by independent actors not before the court.'" *Id.* (quoting *Food & Drug Admin. v. All for Hippocratic Med.*, 602 U.S. (2024) (additional level of citations and quotations omitted)).[7] Indeed, there is no factual allegation that plausibly establishes that legitimate companies who use or sell Private Information purchase such information in mass on the black market. Accordingly, Plaintiff's diminution of value allegations do not establish a concrete injury.[8]

The anxiety and emotional distress Plaintiff alleges to have suffered due the Data Breach also does not establish standing. Although Plaintiff argues that "increased anxiety and emotional

[7] The Court notes that Plaintiff's diminution of value argument must hinge on the assumption that cybercriminals distributing his Private Information are necessarily weaking the market for that data because there is no reason to assume that Plaintiff could not still exchange his information to receive at least some compensation, special access, or exclusive deals. *See Fraga*, 2022 WL 19486310 at 11.

[8] Courts in this circuit and others have similarly rejected this diminution of value theory to establish standing. *See In re 21st Century Oncology Customer Data Sec. Breach Litig.*, 380 F. Supp. 3d 1243, 1257 (M.D. Fla. 2021); *Torres v. Wendy's Co.*, 195 F. Supp. 3d 1278, 1284–85 (M.D. Fla. 2016); *Provost v. Aptos, Inc.*, No. 1:17-CV-02120-ELR, 2018 WL 1465766, at *4 (N.D. Ga. Mar. 12, 2018); *In re Practicefirst*, 1:21-CV-00790, 2022 WL 354544, at *7 (W.D.N.Y. Feb. 2, 2022); *Cooper v. Bonobos, Inc.*, No. 21-cv-854, 2022 WL 170622, at *5 (S.D.N.Y. Jan. 19, 2022); *Mount v. PulsePoint, Inc.*, No. 13 Civ. 6592, 2016 WL 5080131, at *6–7 (S.D.N.Y. Aug. 17, 2016); *Welborn v. Internal Revenue Serv.*, 218 F.Supp.3d 64, 78 (D.D.C. 2016) (collecting cases) ("Courts have routinely rejected the proposition that an individual's personal identifying information has an independent monetary value.").

distress experienced by plaintiffs as a result of their most sensitive [Private Information] being exposed to criminals is a concrete injury," "courts in this circuit have ordinarily recognized such harms as sufficiently concrete in the data breach context only when allegations of emotional distress are coupled with the substantial risk of future." *DiPierro*, 737 at 1326 (internal citations and quotations omitted). As stated previously, the Court has found there is no substantial risk of future harm. Accordingly, Plaintiff's allegations of emotional distress and anxiety, on their own, are not enough to establish a concrete injury necessary for the purposes of standing.

Lastly, the Court must consider Plaintiff's loss of privacy allegations. Plaintiff alleges that he has "anxiety and increased concerns for the loss of privacy." ECF No. [1] at ¶ 16. "Courts have held that allegations of loss of privacy from a data incident, without more, are insufficient to establish an injury in fact." *Baker v. Akumin Corp.*, No. 0:23-CV-62396, 2024 WL 1931480, at *6 (S.D. Fla. Apr. 16, 2024). Here, Plaintiff "pleads no facts showing how the loss of privacy has impacted or damaged him," particularly given that there are no allegations that his Private Information was disclosed.[9] *Baker*, 2024 WL 1931480 at *6; *see TransUnion LLC v. Ramirez*, 594 U.S. 413, 425 (2021) (recognizing that certain intangible harms can be cocreate where they bear "a close relationship to harm traditionally recognized as providing a basis for a lawsuit in American courts"); *In re Mednax, Inc., Customer Data Security Breach Lit.*, 603 F. Supp. 1183 (S.D. Fla. 2022) (explaining that the common law tort for invasion of privacy requires some king of intentional disclosure).[10] "District Courts in this circuit have generally declined to recognize a

[9] To the extent Plaintiff asserts any injury involving a loss of privacy, those allegations merely concern a hypothetical future loss of privacy not any loss that has already occurred. ECF No. [1] at ¶ 16 (alleging only that he has "increased concerns for the loss of privacy") (emphasis added).

[10] While the court in *In re Mednax Servs. Inc.* did find that loss of privacy was a concrete injury, the Court finds that decision distinguishable because specific allegations of actual misuse had been made establishing a substantial threat of actual harm. 603 F. Supp. 3d at 1203.

concrete injury based on conclusory allegations of loss of privacy in the data breach context unless those allegations are coupled with "a substantial and imminent risk of future identity theft" because "[a]ny other result would undermine *Tsao*'s conclusion that '[e]vidence of a mere data breach does not, standing alone, satisfy the requirements of Article III standing'" *DiPierro*, 737 F. Supp. 3d at 1327 (quoting *Tsao*, 986 F. 3d at 1344). Since there is no substantial risk of future injury at this juncture, Plaintiff's loss of privacy allegations are insufficient to establish a concrete injury. Accordingly, Plaintiff has failed to satisfy the injury-in-fact requirement necessary to confer standing and, as such, the Court must dismiss the Complaint for lack of jurisdiction.[11]

IV. CONCLUSION

Accordingly, it is **ORDERED AND ADJUDGED** that

1. Defendant's Motion, **ECF No. [12]**, is **GRANTED**.
2. Plaintiff's Complaint, **ECF No. [1]**, is **DISMISSED WITHOUT PREJUDICE** for lack of jurisdiction.
3. To the extent not otherwise disposed of, any scheduled hearings are **CANCELED**, all pending motions are **DENIED AS MOOT**, and all deadlines are **TERMINATED**.
4. The Clerk of Court shall **CLOSE** this case.

[11] Given that the Court lacks jurisdiction over Plaintiff's claims, the Court may not and need not consider Defendant's alternative theories for dismissal. *See Lewis v. Owner of Popeyes Chicken Louisiana Kitchen*, No. 17-61101-CIV, 2017 WL 4278511, at *1 (S.D. Fla. June 1, 2017) ("Once a federal court determines it lacks subject matter jurisdiction over a case, the court is powerless to continue.") (citing *Univ. of S. Ala. V. Am. Tobacco Co.*, 168 F.3d 405, 409 (11th Cir. 1999)).

DONE AND ORDERED in Chambers at Miami, Florida, on November 3, 2025.

BETH BLOOM
UNITED STATES DISTRICT JUDGE

cc: counsel of record