IN THE UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF ALABAMA
NORTHERN DIVISION

LINDSEY BLAHOUS, *on behalf of herself, as guardian for her minor children L.B., F.B., and D.I. and on behalf of all others similarly situated,*	)	
Plaintiff,	)	
v.	)	Case No. 2:19-cv-798-RAH-SMD (WO)
SARRELL REGIONAL DENTAL CENTER FOR PUBLIC HEALTH, INC.,	)	
Defendant.	)	

MEMORANDUM OPINION AND ORDER

I. INTRODUCTION

For many, the phrase "data breach" provokes dread and invokes disquiet. Suddenly, a person's once private information roams untrammeled, and a degree of uncertainty as to its location and possessor now unexpectedly exists. Of course, for as long as individuals and companies have maintained documentary records and stored private information, data has been poached. Then, as even now, cabinets were jimmied, trashcans were rifled through, and manila envelopes were haphazardly left open, furtively glimpsed. Once companies committed to storing files on local

machines, enterprise databases, and cloud servers, however, breaching a company's every bit of data required no more than gaining access to restricted networks. Soon enough, data breaches became inescapable features of a digitized world.

This case grew from one such breach, its extent and depth still murky. Sometime in January 2019, hackers successfully infiltrated the computer network of Sarrell Regional Dental Center for Public Health, Inc. ("Sarrell" or "Defendant"), installing ransomware that could allow the hackers to demand payment for its deactivation (the "Breach"). Among Sarrell's thousands of unsuspecting patients were Lindsey Blahous ("Blahous") and her three minor children, L.B., F.B., and D.I. ("Minor Plaintiffs") (collectively, "Plaintiffs"). Months later, after its investigation had purportedly yielded no evidence of copied, downloaded, or removed files, Sarrell notified each of the four Plaintiffs of the Breach in four substantively identical missives ("Notice" individually, and collectively, "Notices").

Faulting Sarrell for the personal data that the Breach may have exposed, Blahous sued on behalf of herself, her children, and others similarly situated in both tort and contract. Sarrell responded to Plaintiffs' Complaint, (Doc. 1), with the Defendant's Motion to Dismiss for Lack of Standing and Failure to State a Claim (the "Motion"), (Doc. 21), which sought dismissal pursuant to Rule 12 of the Federal

Rules of Civil Procedure.[1] As explained more fully below, this Court will grant the Motion pursuant to Rule 12(b)(1).

II. FACTUAL AND PROCEDURAL BACKGROUND

A. Data Breaches

Though variously defined by governments and private organizations, the term "data breach" generally encompasses any security incident in which sensitive, protected or confidential data is copied, transmitted, accessed, viewed, stolen, or used by an individual unauthorized to do so. *See, e.g.*, Ala. Code § 8-38-2(1). In the usual case, these attacks target data like financial information, personal health information, personally identifiable information ("PII"), trade secrets, and intellectual property.

States like Alabama have enacted statutes that place obligations on businesses and government agencies regarding the protection of sensitive data they acquire or use such as social security numbers, driver's license numbers, and financial account numbers; defining what constitutes a data breach; providing for what types of notice of a breach and the timing of the notice that must be provided to the parties whose data has been compromised; and creating certain exemptions. *See, e.g.*, Ala. Code §

[1] Any reference in this opinion to "Rule []" or "Rules" is to one or more provisions of the Federal Rules of Civil Procedure.

8-38-1 et seq.; *see also* Fla. Stat. Ann. §§ 282.318, 282.0041, 501.171; Ga. Code Ann. § 10-1-910 et seq.

B. Relevant Facts[2]

Sarrell is "the largest provider of dental services in Alabama," one principally focused on children's "dental and optical" needs. (Doc. 1 , p. 2.) Founded in 2004, its employees, totaling 250 by October 2019, had "serviced more than 845,000 children." (Doc. 1, p. 4.)

Preceding the Breach, the Minor Plaintiffs visited Sarrell with their mother.[3] (Doc. 1, p. 3; *see also* Doc. 21, p. 16.) On September 12, 2019, Sarrell mailed notices of the Breach to approximately 391,472 patients and their guardians.[4] (Doc. 1, pp. 2-3; Doc. 21, pp.16, 41.) As the Notices explained, "[i]n July 2019, . . . Sarrell [had] detected ransomware on . . . [its] computer that appear[ed] to have been the result of an in intrusion that may have begun in January 2019," a gap of seven months. (Doc. 1-1, p. 2; Doc. 1-2, p. 2; Doc. 1-3, p. 2; Doc. 1-4, p. 2; *see also* Doc. 21, p.16.)

[2] Pursuant to Rule 12(b), the "facts" recounted here and throughout this opinion are presumed true solely for purposes of the Motion's adjudication.

[3] Tellingly, Plaintiffs tender no detail as to the date, time, or frequency of their visits.

[4] The Notices, as appended to the Complaint, omitted the second page. (Doc. 21, p. 16, n.2.) Sarrell included that page as an exhibit to the Motion. (Doc. 21-1.)

According to the Notices, the Breach "may" have resulted in the disclosure of the Plaintiffs' "personal health information." (Doc. 1-1, p. 2.)[5]

In response, "out of an abundance of caution" and as a claimed demonstration of the seriousness with which it takes "the security of patient information," Sarrell "immediately deactivated . . . [its] network, temporarily closed . . . [its] practices, engaged an independent computer security firm to investigate, and did not pay a ransom." (*Id*.) When this investigation concluded, Sarrell's "**investigation ha[d] not found evidence that any files or information were copied, downloaded, or removed from . . . [its] network**" or "discovered any evidence that the information that may be involved in this incident ha[d] been misused." (*Id*. (emphasis in original).) The latter point is repeated in the Notices' penultimate paragraph: "Again, at this time, we have found no evidence that your information had been misused." (Doc. 21-1, p. 5.)

Sarrell further admitted that "[t]he information potentially impacted may [have] include[d a patient's] name, address, and health insurance number," and in one letter, (*see* Doc. 1-2), social security numbers and health treatment information.

[5] For brevity purposes, since all four notices, (Doc. 1-1, p. 2; Doc. 1-2, p. 2; Doc. 1-3, p. 2; Doc. 1-4, p. 2; *see also* Doc. 21, p.16), are virtually identical, the Court will simply refer to the first referenced Notice, (Doc. 1-1, p. 2), for the remainder of this Opinion.

(Doc. 1-1, p. 2.) Sarrell stated that it could not "rule out the possibility that the hacker [had] obtained sensitive information from . . . [its] network." (*Id*.)

The Notices conveyed more than just these details as to the Breach. Opening with an apology for the inconvenience that the Breach and resulting shutdown of its operation "may" have caused, each of these two-page documents contained "information about steps . . . [its recipients could] take to protect . . . [their] information and the resources . . . [Sarrell was] making available..." (*Id*.) Among the most notable, Sarrell offered identity theft protection services, under the MyIDCare™ trademark, through ID Experts®, which included "twelve months of credit and CyberScan monitoring," "a $1,000,000 insurance reimbursement policy," and "fully managed ID theft recovery services." (*Id*.)

Towards the end of each Notice, Sarrell once more urged the recipient to utilize the data protection services. (Doc. 21-1, p. 5.) To be eligible for this benefit, a patient had to be over the age of eighteen and possess established credit within the U.S., a Social Security Number, and a U.S. residential address. (Doc. 1-1, p. 2.) Finally, Sarrell asserted that it had "rebuilt . . . [its] business systems with updated security and virus protection for the entire Sarrell network before reopening . . . [its] practices," and that its systems and network were now "monitored with upgraded capabilities to ensure that . . . [its] system and the information . . . [it] store[s] will remain secure." (*Id*.)

Upon receipt of the Notices, Blahous acted, and apparently, suffered. She contacted "all three major credit bureaus in order to put credit freezes on her children's credit." (Doc. 1, p. 4.) She could not do this online, and she thus needed to "obtain [paper] copies of her children's birth certificates to send to the credit bureaus along with a letter confirming her identity." (*Id.*) Through the date of the Complaint, Blahous "continue[d] to monitor her accounts and pristine credit of her minor children,"[6] and "remain[ed] concerned that the exposed PII, which included the birthdays and home addresses of her children, poses significant security and safety concerns"; up to that point at least, she had spent "her valuable time" on "protect[ing] the integrity of her children's physical and fiscal well-being." (*Id.*)

As a result of the exposure of the Plaintiffs' PII, they allegedly suffered four related injuries: (1) an increased risk of their identities being stolen in the future; (2) the costs to mitigate that risk (namely, monitoring their credit); (3) overpayment for dental services, on the theory that an unspecified portion of their payment was for securing their data, which Sarrell allegedly failed to do; and (4) the diminishment of the value of their PII by virtue of the possibility that it was exposed by the ransomware attack. (*Id.*)

[6] This statement is questionable, as not many minor children have any credit profile, much less a "pristine" one.

Plaintiffs' allegations can be summed as follows: The Breach was "*a* direct result of Defendant's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect Patient PII." (*Id.* (emphasis added).) The Plaintiffs claim that Sarrell should have "take[n] adequate and reasonable measures to ensure its data systems were protected against unauthorized intrusions; . . . disclose[d] that it did not have adequately robust computer systems and security practices to safeguard Patient PII; . . . take[n] standard and reasonably available steps to prevent the . . . Breach; . . . monitor and timely detect the . . . Breach; and . . . provide Plaintiff and Class Members prompt and accurate notice of the . . . Breach." (*Id.*) As a result, "Patient PII is now *likely* in the hands of thieves," forcing the Plaintiffs to "spend," now and in the future, "significant amounts of time and money in an effort to protect themselves from the adverse ramification of the . . . Breach" and "forever" endure "*a* heightened risk of identity theft and fraud." (*Id.* (emphasis added).)

B. Procedural Posture

On October 21, 2019, Plaintiffs filed the Complaint and advanced four causes of action—Negligence (Count I); Negligence *Per Se* (Count II); Breach of Implied Contract (Count III); and Breach of Fiduciary Duty (Count IV)—that Plaintiffs hope

to litigate as a class under Rule 23.[7] (Doc. 1, pp. 19-31.) Sarrell filed its Motion to Dismiss on December 18, 2019. (Doc. 21.) Plaintiffs responded on January 17, 2020, (Doc. 26), and Sarrell replied on January 31, 2020, (Doc. 32).

The Motion seeks dismissal of the Complaint's four counts for lack of standing and for failure to state a claim pursuant to Rules 12(b)(1) and (b)(6), respectively.

III. LEGAL STANDARD

Rule 12(b)[8] compels dismissal when a court lacks "subject matter jurisdiction" or a plaintiff lacks standing to appear and be heard. Fed. R. Civ. P. 12(b)(1). In contrast with the constraints imposed on a court's consideration under Rule 12(b)(6), factual challenges under Rule 12(b)(1) allow a court to consider "matters outside the pleadings, such as testimony and affidavits." *McElmurray v. Consol. Gov't of Augusta-Richmond Cnty.*, 501 F.3d 1244, 1251 (11th Cir. 2007). Generally, a court may consider any of the following in order to rule on a Rule 12(b)(1) motion: (1) the complaint alone; (2) the complaint plus undisputed facts evidenced in the record; or (3) the complaint, undisputed facts, and the court's resolution of disputed facts.

[7] Plaintiffs' draftsmanship here leaves much to be desired. Though they eventually set out four claims, only three are mentioned in the Complaint's seven paragraphs. (Doc. 1, p. 3, ¶ 7.)

[8] As the Court is disposing of the Motion under Rule 12(b)(1), the Court need not address the burden of proof or the Defendant's alternative request for dismissal under Rule 12(b)(6).

Butler v. Morgan, 562 F. App'x 832, 834 (11th Cir. 2014) (citing *Williamson v. Tucker*, 645 F.2d 404, 413 (5th Cir. 1981)[9]).

However, when a complaint is challenged for lack of subject matter jurisdiction on its face, all material allegations in the complaint will be taken as true and construed in the light most favorable to the plaintiff. *See McElmurray*, 501 F.3d at 1251. As jurisdiction and standing are critical, the plaintiff, never the movant, always bears the burden of demonstrating both factors. *See Morrison v. Allstate-Indem. Co.*, 228 F.3d 1255, 1273 (11th Cir. 2000).

IV. DISCUSSION

Standing is an essential threshold question for all federal courts under Article III of the U.S. Constitution. *United Food & Commer. Workers Union Local 751 v. Brown Grp.*, 517 U.S. 544, 551 (1996); *Warth v. Seldin*, 422 U.S. 490, 498 (1975). To establish standing, a plaintiff must show (1) an injury in fact, (2) a causal relationship between the injury and the challenged conduct, and (3) a likelihood that the injury will be redressed by a favorable decision. *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 560-61 (1992). The requisite "injury in fact" must be "concrete and particularized and actual or imminent," not "conjectural" or "hypothetical," and must also be "fairly traceable to the challenged action of the defendant." *Id*. Further,

[9] *See Bonner v. Prichard*, 661 F.2d 1206, 1209 (11th Cir.1981) (en banc) (adopting as binding precedent in the Eleventh Circuit, all decisions of the former Fifth Circuit announced prior to October 1, 1981).

it must be "likely, as opposed to merely speculative, that the injury will be redressed by a favorable decision."[10] *Id.* at 561.

"The plaintiff, as the party invoking federal jurisdiction, bears the burden of establishing these elements." *Spokeo, Inc. v. Robins*, __U.S.__, 136 S. Ct. 1540, 1547, (2016) (citing *FW/PBS, Inc. v. Dallas*, 493 U.S. 215, 231 (1990)). "Where, as here, a case is at the pleading stage, the plaintiff must 'clearly ... allege facts demonstrating' each element." *Id*. (quoting *Warth*, 422 U.S. at 518 (1975)).

In applying this standing jurisprudence to data breach cases, the vast majority of federal courts have reached the same conclusion despite differing interpretations of the Supreme Court's decision in *Clapper v. Amnesty International USA*, 568 U.S. 398 (2013). In *Clapper*, which involved alleged electronic surveillance by the National Security Agency, the Court declared that a plaintiff alleging that it will suffer future injuries from a defendant's allegedly improper conduct must show that such injuries are "certainly impending." 568 U.S. at 416–18.

Bound by *Clapper*'s logic, 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

[10] "Prudential standing," the non-constitutional doctrine which often goes hand in hand with constitutional standing analysis, does not apply in this case. *See generally Warth*, 422 U.S. at 499-500 (discussing prudential standing).

data. *E.g.*, *In re: Cmty. Health Sys., Inc*., No. 15-CV-222-KOB, 2016 WL 4732630, at *10 (N.D. Ala. Sept. 12, 2016) (Bowdre, J.) ("[F]or the Plaintiffs in the instant case who did not have allegations of misuse accompanying their claims of an increased risk of harm, the facts pled here do not meet the definition of injury-in-fact; the alleged injuries are "conjectural and hypothetical" and are not "concrete," nor are they "actual or imminent.") (citing *Lujan*, 504 U.S. at 560-61); *see id*. at *9 (noting that "the Eleventh Circuit has not chosen a side in this fray) (citing *Resnick v. AvMed, Inc.*, 693 F.3d 1317, 1323 n.1 (11th Cir. 2012) (finding that the plaintiffs there "alleged only *actual*—not speculative—identify theft," wherefore "we need not address the issue of whether speculative identity theft would be sufficient to confer standing.") (emphasis added); *Taylor v. Fred's, Inc*., 285 F. Supp. 3d 1247, 1267 (N.D. Ala. 2018) (citing *Clapper* and holding against plaintiff in similar context based on defendant's alleged violation of Fair and Accurate Credit Transactions Act of 2003 ("FACTA")); *see also Chambliss v. CareFirst, Inc*., 189 F. Supp. 3d 564, 571 (D. Md. 2016) ("Plaintiffs' efforts to establish the imminence of their theory of harm are unpersuasive," where plaintiff relied on cases which "either concerned information more easily used in fraudulent transactions or relied on factual allegations that the hackers had already misused the stolen data such that the risk of future harm was certainly impending") (also collecting cases); *Whalen v. Michael Stores Inc*., 153 F. Supp. 3d 577, 580–81 (E.D.N.Y. 2015); *In re*

Zappos.com, Inc., 108 F. Supp. 3d 949, 958–59 (D. Nev. 2015); *Storm v. Paytime, Inc.*, 90 F. Supp. 3d 359, 365 (M.D. Pa. 2015); *Strautins v. Trustwave Holdings, Inc.*, 27 F. Supp. 3d 871, 876–77 (N.D. Ill. 2014); *Green v. eBay Inc.*, No. CIV.A. 14-1688, 2015 WL 2066531, at *6 (E.D. La. May 4, 2015); *Peters v. St. Joseph Servs. Corp.*, 74 F. Supp. 3d 847, 854–56 (S.D. Tex. 2015); *In re Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig.*, 45 F. Supp. 3d 14, 26–27 (D.D.C. 2014) (discussing *Clapper* and also collecting pre-*Clapper* cases finding against plaintiffs in data breach cases where they alleged speculative harm); *In re SuperValu, Inc.*, No. 14-MD-2586 ADM/TNL, 2016 WL 81792, at *4 (D. Minn. Jan. 7, 2016), *aff'd in part, rev'd in part and remanded*, 870 F.3d 763 (8th Cir. 2017) (collecting cases and concluding that this approach now constitutes the majority one among federal courts); *Reilly v. Ceridian Corp.*, 664 F.3d 38, 42–43 (3d Cir. 2011) (pre-*Clapper* case applying the same Article III injury logic to data breach case); *but see In re 21st Century Oncology Customer Data Sec. Breach Litig.*, 380 F. Supp. 3d 1243, 1250, 1251, n.5 (M.D. Fla. 2019) (stating that "(o)ther circuits, however, have addressed the question and have come to differing conclusions" and that there "is a comparable disarray among district courts.").

Other lower courts have disagreed, but even these more forgiving courts still require plaintiffs to allege a "credible threat." *In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, 996 F. Supp. 2d 953, 961-62 (S.D. Cal. 2014)

(surveying case law and deriving rule for data breach cases in part from *San Luis & Delta-Mendota Water Auth. v. U.S. Dep't of Interior*, 905 F. Supp. 2d 1158, 1170–71 (E.D. Cal. 2012), and *Doe 1 v. AOL, LLC*, 719 F. Supp. 2d 1102, 1108–09 (N.D. Cal. 2010)); *accord, e.g.*, *Krottner v. Starbucks*, 628 F.3d 1139, 1142-43 (9th Cir. 2010); *cf. Remijas v. Neiman Marcus Grp., LLC*, 794 F.3d 688, 692–94 (7th Cir. 2015); *In re SuperValu, Inc.*, No. 14-MD-2586 ADM/TNL, 2016 WL 81792, at *6 (collecting cases).

Furthermore, the passage of months, and then, years, only renders any such conjectural threat increasingly less imminent. *See Storm*, 90 F. Supp. 3d at 367; *In re Zappos.com, Inc.*, 108 F. Supp. 3d at 958.

Notably, in 2012, the Eleventh Circuit accorded standing to plaintiffs in a data breach case; but there, the stolen data had been exploited to open bank and brokerage accounts in the unsuspecting plaintiffs' names, causing actual monetary damages. *Resnick v. AvMed, Inc.*, 693 F.3d 1317, 1322–23 (11th Cir. 2012). This approach has been followed by other courts in the circuit. *E.g.*, *In re 21st Century Oncology Customer Data Sec. Breach Litig.*, 380 F. Supp. 3d at 1250–56; *Smith v. Triad of Alabama, LLC*, No. 1:14-CV-324-WKW, 2015 WL 5793318, at *9 (M.D. Ala. Sept. 29, 2015) (Watkins, J.).

Taken together, the weight of authority shows that a plaintiff must provide at least some plausible specific allegation of actual or likely misuse of data to satisfy

Article III's standing requirement and avoid dismissal under Rule 12(b)(1), a position consistent even with pre-*Clapper* precedent. *See, e.g.*, *Burrows v. Purchasing Power, LLC*, No. 1:12-CV-22800-UU, 2012 WL 9391827, at *2 (S.D. Fla. Oct. 18, 2012) (finding an injury in fact where plaintiff alleged that his identity was stolen when an unknown individual misused his PII to file a tax return and that he was denied tax refund); *see also Krottner*, 628 F.3d at 1142; *In re Google, Inc. Privacy Policy Litig.*, No. C 12-01382 PSG, 2012 WL 6738343, at *6 (N.D. Cal. Dec. 28, 2012) (dismissing plaintiffs' claims based on Google's policy of retaining personal information for lack of Article III standing because there were no allegations plaintiffs' personal information had been disseminated). In fact, "since *Clapper* . . . courts have been even more emphatic in rejecting increased risk as a theory of standing in data-breach cases." *In re Sci. Applications Int'l Corp. Backup Tape Data Theft Litig.*, 45 F. Supp. 3d at 28 (internal quotation marks omitted).

Here, the fact that the Breach occurred cannot in and of itself be enough, in the absence of any imminent or likely misuse of protected data, to provide Plaintiffs with standing to sue. The Complaint lacks any allegations suggesting that any "disclosure" of their data, such as an actual review by a third party, has occurred; in fact, Plaintiffs fail to allege that they or members of the putative class have suffered actual identity theft. Instead, their pleading speaks of possibilities and traffics in maybes. (*E.g.*, Doc. 1, pp. 3, 16.)

The Notice upon whose basis the Plaintiffs sue, included as exhibits to their own pleading, denies that any personal information was copied, downloaded, or removed from the network, despite Plaintiffs' mistaken belief to the contrary. (Doc. 1-1 p. 2.) True enough, the Notices concede that "[t]he information potentially impacted may [have] include[d a patient's] name, address, and health insurance number," as well as, per one of the Notice letters, the patient's Social Security Number and health treatment information, (*see* Doc. 1-2, p. 2), but, Sarrell's investigation had not "discovered any evidence that the information that may be involved in this incident ha[d] been misused" between July and September 2019. (Doc. 1-1, p. 2; Doc. 1-2, p. 2; Doc. 1-3, p. 2; Doc. 1-4, p. 2; *see also* Doc. 21, p. 16.)

Unquestionably, "the possibility that the hacker [had] obtained sensitive information from the network" could not be discounted. (Doc. 1-1, p. 2; Doc. 1-2, p. 2; Doc. 1-3, p. 2; Doc. 1-4, p. 2; *see also* Doc. 21, p. 16.) But the Notices do not say—and the Complaint does not allege—that the hackers both obtained and intend to expose the Plaintiffs' specific personal data.

If, per the Complaint, the allegation—which must be taken as fact—stating the "result of Defendant's failure to implement and follow basic securities strategies" is that "Patient PII is now *likely* in the hands of thieves," but no "evidence that the information that may be involved in this incident ha[d] been misused" has

been found, and given that there is no more than the "possibility that the hackers obtained *sensitive* information," which may include names, addresses, dates of birth, health insurance numbers, and in one case, a social security number and treatment information, despite the Plaintiffs' insistence to the contrary, (Doc. 1-1, p. 2, (emphasis added)), Plaintiffs simply have failed to plausibly point to a *certain* threat of the hackers' making use of their specific personal data as a result of the Breach.

An account of *other* hacks and the potential uses to which hackers may put stolen data, the use of such buzzwords as "secret," and even appeals to protect children and their privacy, cannot obscure the Plaintiffs' failure to point to an injury both particularized and concrete, imminent and plausible.[11] In the absence of an actuality or a likelihood, the mere possibility that the Plaintiffs' PII may have been gathered and disseminated and that their credit may suffer if the hackers opt to sell or release this information to those able and willing to exploit it cannot impart the requisite standing.[12] *E.g.*, *Clapper*, 568 U.S. at 410. Other district courts within the Eleventh Circuit have held the same. *See In re 21st Century Oncology Customer Data Sec. Breach Litig.*, 380 F. Supp. 3d at 1250–56; *I Tan Tsao v. Captiva MVP*

[11] The Plaintiffs' claim that they suffered money damages because they paid for services at Sarrell but would not have done so had they known that Sarrell would get hacked later on, is pure applesauce.

[12] In this regard, this Court finds Plaintiffs' extended riff on the court's obligation to protect this nation's children both overdrawn and inapposite. No amount of purple prose can provide a person without a cognizable injury the standing to sue.

Rest. Partners, LLC, No. 8:18-CV-1606-T-02SPF, 2018 WL 5717479, at *2 (M.D. Fla. Nov. 1, 2018); *Provost v. Aptos, Inc.*, No. 1:17-CV-02120-ELR, 2018 WL 1465766, at *3 (N.D. Ga. Mar. 12, 2018); *Torres v. Wendy's Co.*,195 F. Supp. 3d 1278, 1283 (M.D. Fla. 2016); *Smith*, 2015 WL 5793318, at *7; *see also Reilly*, 664 F.3d at 44-45; *Khan v. Children's Nat'l Health Sys.*, 188 F. Supp. 3d 524, 532–33 (D. Md. 2016); *Key v. DSW, Inc.*, 454 F. Supp. 2d 684, 687–90 (S.D. Ohio 2006).

This wide array of authority leaves the Plaintiffs with but the slenderest of reeds upon which to rest their standing argument: that of their alleged money damages. Yet even here, the Plaintiffs' actual incurred costs to address the data breach are insufficient to demonstrate standing.

As another district court in this circuit found, data breach mitigation costs do not create an Article III injury for plaintiffs who allege *speculative* harms resulting from the poaching of their personal data. *21st Century Oncology*, 380 F. Supp. 3d at 1256) ("where 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.") (citing *In re SuperValu*, 870 F.3d at 771) ("Because 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."); *see Clapper*, 568 U.S. at 416 ("Thus, allowing respondents to bring this action based on costs they incurred in response to a speculative threat would be tantamount to

accepting a repackaged version of respondents' first failed theory of standing.").[13] The same principle applies here, and the Plaintiffs' alleged monetary damages are thus insufficient to provide them Article III standing. *See*, *cf. Resnick*, 693 F.3d at 1322 (one plaintiff's sensitive information was used by an unknown third party to open Bank of America accounts and to activate credit cards which were used to make unauthorized purchases and to open an account with E*Trade Financial, which was later overdrawn).

So in the end, without more, the Complaint must be dismissed for Plaintiffs' lack of standing. *See Stapleton on behalf of C.P. v. Tampa Bay Surgery Ctr., Inc*., No. 8:17-CV-1540-T-30AEP, 2017 WL 3732102, at *3 (M.D. Fla. Aug. 30, 2017) ("Plaintiffs allegations rely on a chain of inferences that is too attenuated to constitute imminent harm."); *see also In re iPhone Application Litig*., No. 11-MD-02250-LHK, 2011 WL 4403963, at *4-7 (N.D. Cal. Sept. 20, 2011) (no standing in a data breach case because plaintiffs had not alleged any "particularized example" of economic injury or harm to their computers, but instead offered only abstract

[13] The Seventh Circuit also addressed this issue in *Remijas*, 794 F.3d at 694, explaining that "(m)itigation expenses do not qualify as actual injuries where the harm is not imminent." (citing *Clapper*, 568 U.S. at 414) (concluding that "costs that they have incurred to avoid [injury]" are insufficient to confer standing). "Plaintiffs 'cannot manufacture standing by incurring costs in anticipation of non-imminent harm.'" *Id*. "If the law were otherwise, an enterprising plaintiff would be able to secure a lower standard for Article III standing simply by making an expenditure based on a nonparanoid fear." *Id*.

concepts, such as "opportunity costs," "value-for-value exchanges," "consumer choice," and "diminished performance").

V. CONCLUSION

Based on the foregoing, it be and is hereby

ORDERED as follows:

(1) To the extent the Defendant seeks dismissal pursuant to Rule 12(b)(1), the Defendant's Motion to Dismiss (Doc. 21) is GRANTED;

(2) This case is DISMISSED without prejudice.

A separate judgment shall issue.

DONE, this 16th day of July, 2020.

/s/ R. Austin Huffaker, Jr.
R. AUSTIN HUFFAKER, JR.
UNITED STATES DISTRICT JUDGE