IN THE SUPERIOR COURT OF THE STATE OF DELAWARE

CECILIA ABERNATHY, FLINT DELON, TINA MURPHY and JEFFREY WASKO, INDIVIDUALLY AND ON BEHALF OF ALL OTHERS SIMILARLY SITUATED,	)	
Plaintiffs,	)	C.A. No. N20C-05-057 MMJ CCLD
v.	)	
BRANDYWINE UROLOGY CONSULTANTS, P.A.,	)	
Defendant.	)	

Submitted: October 30, 2020
Decided: January 21, 2021

On Defendant's Motion to Dismiss

GRANTED

OPINION

Gary M. Klinger, Esq., (Argued) Mason Lietz & Klinger LLP, Chicago, Illinois, Gary E. Mason, Esq., David K. Lietz, Esq., Mason Lietz & Klinger LLP, Washington, District of Columbia, Jared T. Green, Esq., Seitz, Van Ogtrop & Green, P.A., Wilmington, Delaware, *Attorneys for Plaintiffs and the Proposed Class*.

William E. Manning, Esq., Saul Ewing Arnstein & Lehr LLP, Wilmington, Delaware, Turner A. Broughton, Esq. (Argued), Brendan D. O'Toole, Esq. (Argued), Amanda Bird, Esq., Williams Mullen, Richmond, Virginia, *Attorneys for Defendant.*

JOHNSTON, J.

FACTUAL AND PROCEDURAL CONTEXT

Parties

This case arises from a data breach. On January 27, 2020, Brandywine Urology Consultants, P.A. ("Defendant") discovered that it was the victim of a ransomware attack (the "Attack") on its network.[1] The Attack blocked access to Defendant's computer system and data, which included sensitive patient medical records.[2] During the Attack, cyberthieves accessed and encrypted records that included patient names, addresses, Social Security numbers, medical file numbers, claim data, and other financial and personal data.[3] During and after the attack, there was no attempt to extract a ransom.

Plaintiffs Cecilia Abernathy, Flint Delong, Tina Murphy, and Jeffrey Wasko (collectively, "Plaintiffs") bring this suit individually and on behalf of a Proposed Class.[4] Defendant is a Delaware-based urology practice.[5] Plaintiffs are patients of Defendant.[6]

[1] Defendant's Opening Brief in Support its Motion to Dismiss ("OB"), at 9.
[2] Plaintiff's Response and Opposition to Defendant's Motion to Dismiss at 1-2.
[3] *Id*. at 2.
[4] Compl. at 1. Plaintiffs have not made a request to certify the class at this stage.
[5] OB at 10.
[6] Resp. at 2.

Defendant's Response to the Attack

Defendant states that it took immediate steps to "isolate and mitigate the intrusion to its network" after the Attack was discovered.[7] Defendant removed the malicious software from its network.[8] Defendant also hired an outside security firm to investigate whether protected health information ("PHI") on the network had been compromised by the Attack.[9] After examining the extent of the Attack, the security firm confirmed that no PHI had been compromised.[10]

On March 27, 2020, Defendant notified all of its patients of the Attack.[11] On March 28, 2020, Defendant issued an updated Notice of Potential Data Breach (the "Notice").[12] The Notice informed Defendant's patients that it was possible, though Defendant believed that it was "unlikely," that their personal and financial information was compromised.[13] The Notice also stated that Defendant would inform patients as soon as possible of the results of its ongoing investigation.[14]

[7] OB at 9-10.
[8] *Id*. at 10.
[9] *Id*.
[10] *Id*.
[11] *Id*.
[12] *Id*.
[13] *Id*.
[14] *Id*.

Procedural History

Plaintiffs filed suit on May 06, 2020.[15] Plaintiffs assert claims for: (1) negligence; (2) invasion of privacy; (3) breach of express contract; (4) breach of implied contract; (5) negligence *per se*; (6) breach of fiduciary duty; (7) noncompliance with the Delaware Computer Security Breach Act; and (8) violation of the Delaware Consumer Fraud Act.

Defendant filed a Motion to Dismiss and supporting brief on July 15, 2020. Plaintiffs filed their Response on August 28, 2020. Defendant filed its Amended Reply on September 25, 2020.

STANDARD OF REVIEW

Lack of Standing

Rule 12(b) provides for dismissal of a claim when a court lacks subject matter jurisdiction or a plaintiff lacks standing to appear and be heard.[16] Factual challenges under Rule 12(b)(1) permit a court to consider matters outside the pleading, such as testimony and affidavits.[17] The burden is on the plaintiff to demonstrate that it meets the elements for standing.[18]

[15] Compl. at 1.
[16] Super. Ct. Civ. R. 12(b)(1)-(2).
[17] *Id*.
[18] *Lujan v. Defs. Of Wildlife*, 504 U.S. 555, 561 (1992).

Failure to State a Claim Upon Which Relief Can Be Granted

In a Rule 12(b)(6) Motion to Dismiss, the Court must determine whether the claimant "may recover under any reasonably conceivable set of circumstances susceptible of proof."[19] The Court must accept as true all well-pleaded allegations.[20] Every reasonable factual inference will be drawn in the non-moving party's favor.[21] If the claimant may recover under that standard of review, the Court must deny the Motion to Dismiss.[22]

ANALYSIS

Defendant's Contentions

Defendant argues that Plaintiffs lack standing to bring this case. Defendant contends that Plaintiffs have failed to allege an injury in fact. Further, Plaintiffs' alleged injuries cannot be traced back to Defendant. Defendant asserts that Plaintiffs have failed to state a claim for Counts 1-5. As for Plaintiffs' other claims, Defendant argues that: (1) the economic loss doctrine bars any recovery; (2) the breach of fiduciary duty claim must be dismissed because the Court lacks subject matter jurisdiction; (3) the Delaware Computer Security Breach Act claim must be dismissed because Plaintiffs lack standing and Defendant satisfied the

[19] *Spence v. Funk*, 396 A.2d 967, 968 (Del. 1978).
[20] *Id*.
[21] *Wilmington Sav. Fund Soc'y v. Anderson*, 2009 WL 597268, at *2 (Del. Super.) (citing *Doe v. Cahill*, 884 A.2d 451, 458 (Del. 2005)).
[22] *Spence*, 396 A.2d at 968.

statute's notice requirement; and (4) the Delaware Consumer Fraud Act claim must be dismissed because Plaintiffs have failed to state a claim under the statute.

Plaintiffs' Contentions

Plaintiffs maintain that they have sustained an injury in fact sufficient to confer standing. Plaintiffs specifically allege the following harms: (1) the imminent risk of future harm; (2) mitigation expenses; (3) loss of privacy; (4) anxiety; (5) failure to receive the benefit of a bargain; (6) loss of value of property in personally identifying information; and (7) disruption to Plaintiffs' medical care. Plaintiffs contend that these alleged harms are legally cognizable and can be traced back to Defendant.

In response to Defendant's other arguments, Plaintiffs argue that the economic loss doctrine does not foreclose the possibility of recovery because Defendant denies the existence of any contract. Further, Plaintiffs properly state claims for negligence, negligence *per se*, invasion of privacy, breach of express contract, and breach of implied contract. Plaintiffs maintain that they properly stated a claim under Delaware's Consumer Fraud Act. Plaintiffs concede that the Court lacks subject matter jurisdiction over their fiduciary duty claim. Finally, Plaintiffs elect to withdraw their claim under the Delaware Computer Security Breach Act.

Standing

Plaintiffs bear the burden of establishing all of the elements for standing.[23] Plaintiffs must demonstrate: (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.[24] The requisite injury-in-fact must be concrete, particularized, and actual or imminent—not conjectural or hypothetical.[25] Additionally, it must be "fairly traceable to the challenged action of the defendant."[26]

"A plaintiff alleging that it will suffer future injuries from a defendant's allegedly improper conduct must show that such injuries are certainly impending."[27] In data breach cases, Plaintiffs must provide at least some plausible specific allegations of actual or likely misuse of data to satisfy the standing requirement and avoid dismissal under rule 12(b)(1).[28] "Standing is a threshold question that must be answered by a court affirmatively to ensure that the litigation before the tribunal is a 'case or controversy' that is appropriate for the exercise of the court's judicial powers."[29]

---

[23] *Lujan*, 504 U.S. at 561.
[24] *Id*. at 560-61.
[25] *Id*.
[26] *Id*.
[27] *Clapper v. Amnesty Int'l USA*, 568 U.S. 409, 416-18 (2013).
[28] *Blahous v. Sarrell Regional Dental Center for Pub. Health*, 2020 WL 4016246, at *4 (M.D. Ala.).
[29] *Dover Historical Soc. v. City of Dover Planning Com'n*, 838 A.2d 1103, 1110 (Del. 2003).

Delaware courts have not addressed the question of whether the imminent risk of future harm from a data breach constitutes an injury-in-fact sufficient to confer standing. Defendant argues that it does not. To support its assertion, Defendant relies on *Reilly v. Ceridian Corporation*.[30] In *Reilly*, hackers accessed information stored on the computer system of a payroll processing company. The hackers potentially gained personal and financial information of 27,000 individuals.[31] The Third Circuit noted in that case that "it [was] not known whether the hacker read, copied, or understood the data."[32] There "was no evidence that the intrusion was intentional or malicious" and "no identifiable taking occurred."[33] The Third Circuit was unwilling to recognize the plaintiff's injury because it was too attenuated to confer standing and amounted to nothing more than speculation.[34]

Various federal courts have held that a plaintiff lacks standing to sue the party who failed to protect its data—in a lost data or potential identity theft case—where there is no proof of *actual* misuse or fraud.[35] Although some lower courts

[30] 664 F.3d 38 (3rd Cir. 2001).
[31] *Id*. at 42.
[32] *Id*. at 40.
[33] *Id*. at 44.
[34] *Id*. at 43.
[35] *See, e.g., Blahous*, 2020 WL 4016246, at *5 (data breach, without evidence of use of stolen data, is insufficient to confer standing); *In re: Cmty. Health Sys., Inc.*, 2016 WL 4732630, at *10 (N.D. Ala.) ("[T]he 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

have disagreed, those courts still require a plaintiff to allege a "credible threat."[36] "Furthermore, the passage of months, and then, years, only renders any [] conjectural threat increasingly less imminent."[37]

The Notice that Defendant sent to its patients, including Plaintiffs, stated there was a *possibility* that personal and financial information was compromised during the Attack.[38] However, such notice is not a concession of a plausible, concrete, imminent, or certain threat.[39]

As the direct victim of a hacker, Defendant appeared to take swift and appropriate measures to investigate and mitigate the data breach. The Notice sent to those whose information possibly was breached is part of the standard process under such circumstances. Defendant should not be punished for sending out the

---

"concrete," nor are they "actual or imminent.") (internal citation omitted); *Chambliss v. Carefirst, Inc*, 189 F.Supp.3d 564, 572 (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.").

[36] *See, e.g., Blahous*, 2020 WL 4016246, at *6; *Krottner v. Starbucks*, 628 F.3d 1139, 1143 (9th Cir. 2010) (finding that plaintiffs "alleged a credible threat of real and immediate harm stemming from the theft of a laptop containing their unencrypted personal data" but noting that plaintiffs might not have alleged a credible threat if the allegations had been "more conjectural or hypothetical—for example, if no laptop had been stolen.").

[37] *Blahous*, 2020 WL 4016246, at *6 (citing *Storm v. Paytime, Inc.*, 90 F.Supp.3d 359, 366-67 (M.D. Pa. 2015) and *In re Zappos.com, Inc.*, 108 F.Supp.3d 949, 958 (D. Nev. 2015)).

[38] OB at 10.

[39] The Notice additionally stated that Defendant believed it was unlikely that any information was compromised. An outside security firm later confirmed that no PHI was compromised. Plaintiffs do not contest this finding but rather argue it is still possible that their information may be misused.

Notice. So long as the Notice is accurate, it cannot be the basis for liability, or deemed to be an admission. The Court is reluctant to make any ruling that would chill efforts to notify patients or clients of security breaches out of an abundance of caution.

The injury alleged by Plaintiffs—imminent risk of future harm from the Attack—is nothing more than conjecture and a collection of hypothetical risks. Additionally, the time that has elapsed since the Attack is problematic. In a similar case, the United States District Court for the Middle District of Pennsylvania stated:

> Plaintiffs' alleged harm—that they are now at an increased risk of identity theft—does not suffice to allege an imminent injury. Perhaps this strict imminency standard has some wisdom, for even though Plaintiffs may indeed be at greater risk of identity theft, the data breach in this case occurred in April 2014—*almost a year ago*—and Plaintiffs have yet to allege that any of them have become actual victims of identity theft. Indeed, putting aside the legal standard for imminence, a layperson with a common sense notion of "imminence" would find this lapse of time, without any identity theft, to undermine the notion that identity theft would happen in the near future.[40]

In the same way, Plaintiffs in this case have failed to allege that *any* of them have been victims of *any* actual harm stemming from the Attack. As almost a year has now passed without any harm occurring, it appears unlikely that Plaintiffs would be harmed in the near future.

[40] *Storm*, 90 F.Supp.3d at 366-67 (emphasis added).

The mere fact that the Attack occurred, without more, is insufficient to confer standing on Plaintiffs. Under the facts of this case, the "imminent risk of future harm" alleged by Plaintiffs is not concrete, particularized, actual or imminent. Therefore, Plaintiffs have failed to meet their burden for showing that they have standing.

Other Alleged Damages are Not Sufficient to Confer Standing

Mitigation Damages

Plaintiffs assert that mitigation expenses are legally cognizable damages. Plaintiffs claim that they have incurred out-of-pocket expenses and lost the value of their time spent: (1) monitoring their accounts for fraudulent charges; (2) canceling and issuing credit and debit cards; (3) purchasing credit monitoring and identity theft prevention services; and (4) placing freezes and alerts with credit reporting agencies.[41] However, "allowing [Plaintiffs] to bring this action based on costs they incurred in response to a speculative threat would be tantamount to accepting a repackaged version of [Plaintiffs] first failed theory of standing."[42] The Court finds that mitigation costs do not create an injury sufficient to confer standing on Plaintiffs who allege speculative harms resulting from a data breach.[43]

[41] Compl. ¶¶ 82, 86.
[42] *Clapper*, 568 U.S. at 416.
[43] *See Blahous* at *8 (finding that a plaintiff's alleged monetary damages were insufficient to confer standing); *In re 21st Century Oncology Customer Data Sec. Breach Litig.*, 380 F.Supp.3d, 1243, 1256 (M.D. Fla. 2019) ("[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

Increased Anxiety and Emotional Distress

Plaintiffs argue that they experienced increased anxiety and emotional distress as a result of the Attack.[44] Plaintiffs rely on *Shqeirat v. U.S. Airways Group., Inc.*,[45] in which the United States District Court for the District of Minnesota found that fear of identity theft resulting from disclosure of a social security number was sufficient to support an emotional distress claim.[46] However, in the facts of that case, the plaintiff did not merely speculate that his social security numbers had been disclosed; the information had been published online.[47] Plaintiffs have not shown that any of their information has been disclosed following the Attack.[48] The Court finds that alleged emotional distress following a data breach cannot confer standing where a plaintiff fails to show that information actually has been published or otherwise misused.[49]

---

likewise typically found to be non-cognizable."); *In re SuperValu, Inc. Consumer Data Sec. Breach Litig.*, 870 F.3d 763, 771 (8th Cir. 2017) ("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.").

[44] Compl. ¶¶ 88, 89.

[45] 515 F. Supp. 2d 984 (D. Minn. 2007).

[46] *Id*. at 998.

[47] *Id*. at 997.

[48] The Court additionally notes that under Delaware law, a plaintiff must allege physical manifestations of emotional harm. *See Robb v. Pennsylvania R. Co.*, 210 A.2d 709, 711 (Del. 1965) ("[I]t is accepted as settled that there can be no recovery for fright alone, not leading to bodily injury or sickness, arising from the negligence of another."). Plaintiffs' complaint fails to allege any physical manifestations resulting from the emotional distress caused by the Attack.

[49] *See Crisafulli v. Amertias Life Ins. Corp.*, 2015 WL 1969176, at *3-4 (D. N.J.) (finding that "bald assertions" of "emotional distress including anxiety, fear of being victimized, harassment and embarrassment" are insufficient to confer standing); *In re SAIC Backup Tape Data Theft Litig.*, 45 F.Supp.3d 14, 29 (D.D.C. 2014) ("To be sure, the Supreme Court has intimated that

Benefit of the Bargain

Plaintiffs also assert that they did not receive the benefit of the bargain because they did not get the data security that they bargained and paid for. However, a number of courts have rejected an "overpayment" theory of damages as an injury-in-fact for standing purposes.[50] A plaintiff's "claim that some indeterminate part of their premiums went toward paying for security measures … is too flimsy to support standing."[51]

Plaintiffs allege in their complaint that "[p]art of the price [Plaintiffs] paid to Defendant was intended to be used by Defendant to fund adequate security of [Defendant's] computer property and Plaintiffs' [] Private Information. Thus, Plaintiffs [] did not get what they paid for."[52] The complaint does not provide any additional information. It does not provide anything that would show Plaintiffs intended that their money be used to pay for security costs. Nor does it "allege facts showing how the price [Plaintiffs] paid for [medical care from Defendant] incorporated some particular sum that was understood by both parties to be

disclosure of personally identifiable information alone, along with some attendant emotional distress, may constitute 'injury enough to open the courthouse door' in privacy actions . . . But again, disclosure involves publication to a third party.").

[50] *See Fero v. Excellus Health Plan Inc.*, 236 F.Supp.3d 735, 754-55 (W.D.N.Y. 2017) (compiling cases from various jurisdictions that rejected an overpayment theory).

[51] *In re SAIC*, 45 F.Supp.3d at 30.

[52] Compl. ¶ 84.

allocated towards the protection of [] data."[53] Therefore, the Court finds that Plaintiffs' benefit of the bargain argument is insufficient to confer standing.

Loss of Value of Property

Plaintiffs further contend that the loss of value of property in personally identifying information ("PII") is an injury-in-fact. They argue that "their PII [is] a valuable commodity, that a market exists, and that the PII is likely being sold on the dark web."[54] This argument fails for two reasons.

Plaintiffs merely state that they "believe their Private Information was stolen (and subsequently sold) in the Attack" and provide a list of actions hackers may take.[55] While this cited information may support their belief that some information was stolen, Plaintiffs do not provide anything that supports their belief that the information was sold. Therefore, alleged loss of value, in this case, is insufficient to confer standing.

Disruption to Medial Care

Plaintiffs state that "the easiest identifiable harm Plaintiffs allege is the disruption to their medical care and treatment as a result of the ransomware attack."[56] The complaint states that "the [A]ttack disrupted [Defendant's]

[53] *In re Zappos Inc.*, 108 F.Supp.3d at 962 n.5.
[54] Resp. at 15.
[55] Compl. ¶¶ 39-40.
[56] Resp. at 16.

computer network, leaving data stored on [Defendant's] network encrypted and inaccessible, and forcing Defendant to reschedule certain procedures."[57] The complaint goes on to list all of the reasons why ransomware attacks at medical facilities cause disruption to medical treatment.[58] However, again, Plaintiffs fail to provide anything more than speculation and conjecture.

While the complaint provides information about medical disruption in the abstract, it fails to identify *even one* plaintiff who was denied access to their medical records or had their medical treatment otherwise disrupted. The Court finds that the conclusory statements that Plaintiffs had their medical treatment disrupted are insufficient to confer standing.

CONCLUSION

Plaintiffs have not alleged any injury-in-fact; they merely allege possible future injuries. The alleged "imminent risk of future harm" to Plaintiffs is not concrete, particularized, actual, or imminent. Because a year has passed since the Attack without any harm actually occurring, the alleged harm also is not "certainly impending." The various additional damages alleged by Plaintiffs are likewise insufficient to confer standing. Therefore, the Court finds that Plaintiffs lack

[57] Compl. ¶ 35.
[58] *Id*. at ¶¶ 52-57.

standing in this case. Because standing is a threshold requirement, the Court need not resolve the remaining issues.

THEREFORE, Defendant's Motion to Dismiss is hereby **GRANTED**.

IT IS SO ORDERED.

/s/ Mary M. Johnston

The Honorable Mary M. Johnston