UNITED STATES DISTRICT COURT
DISTRICT OF PUERTO RICO

PABLO J. QUINTERO, JOANNIE PRINCIPE, individually and on behalf of all others similarly situated, Plaintiffs,	)	
v.	)	CIVIL ACTION NO. 20-01075-WGY
METRO SANTURCE,INC., d/b/a PAVIA HOSPITAL SANTURCE a corporation, METRO HATO REY, INC., d/b/a PAVIA HOSPITAL HATO REY, and DOES 1-10, Defendants.	)	

YOUNG, D.J.[1] December 9, 2021

MEMORANDUM OF DECISION

I. INTRODUCTION

In this putative class action, two patients, the plaintiffs Pablo J. Quintero and Joannie Principe ("the Patients"), individually and on behalf of all others similarly situated, bring suit against two hospitals, the defendants Metro Santurce, Inc., d/b/a Pavia Hospital Santurce, and Metro Hato Rey, Inc., d/b/a Pavia Hospital Hato Rey ("the Hospitals") because of a ransomware attack that allegedly led to the exposure of their

[1] Of the District of Massachusetts, sitting by designation.

personally identifiable information ("PII") and protected health information ("PHI").[2] See generally Compl. ECF No. 1.

On October 13, 2021, this Court held oral argument on Hospitals' motion to dismiss. See October 13, 2021 Minute Order, ECF No. 32. After hearing, the Court concluded that no injury plausibly was alleged for Constitutional standing purposes. The motion to dismiss for lack of standing was ALLOWED, the remaining grounds of motion to dismiss were DENIED

[2] "The Cybersecurity and Infrastructure Security Agency . . . an agency within the Department of Homeland Security . . . defines 'ransomware' as a type of malicious software . . . that is designed to restrict or deny access to computer data until a ransom, typically in the form of bitcoin, is fully paid by the victim(s)." Helena Roland, The Survival of Critical Infrastructure: How Do We Stop Ransomware Attacks on Hospitals?, 29 Cath. U.J.L. & Tech. 177, 180 (2020). Similarly, the United States Secret Service describes ransomware as "a type of malicious software (malware), which denies access to systems or data and/or exfiltrates data." United States Secret Service Cybercrime Investigation, Preparing for a Cyber Incident: a Guide to Ransomware, https://www.secretservice.gov/sites/default/files/reports/2020-12/Preparing%20for%20a%20Cyber%20Incident%20-%20A%20Guide%20to%20Ransomware%20v%201.0.pdf (last visited September 13, 2021). "Cyber actors hold systems or data hostage until a ransom is paid for a decryption key. Cyber actors also threaten to publish exfiltrated data, or sell it on the dark web." Id. Hospitals are apparently particularly vulnerable to this type of attack. See Roland, supra note 2, at 181-82 (discussing the history and growing problem of ransomware). "In 2019, the United States was hit by an unprecedented number of ransomware attacks that impacted at least 966 government agencies, 1,233 educational establishments, and 764 health care providers at a potential cost in excess of $7.5 billion." Marcus Chung, New Ransomware Innovations Bring Shame and Fear to Health Care, 22 J. Health Care Compliance 37, 38 (2020).

as MOOT and the action was dismissed without prejudice. See id. This memorandum explains the Court's decision.

II. BACKGROUND

A. Procedural History

The Hospitals moved to dismiss the complaint ("the Motion"). Mot. Dismiss ("Mot."), ECF No. 18. The Patients opposed the Motion ("the Opposition"). Pls.' Opp'n Defs.' Mot. Dismiss ("Opp'n"), ECF No. 19. The Hospitals filed a reply and submitted supplemental authority. Reply Supp. Mot. Dismiss ("Reply"), ECF No. 21-1; Mot. Leave Submit Suppl. Authority, ECF No. 29. The Court heard oral argument and allowed the Motion solely on the ground of lack of standing on October 13, 2021. See October 13, 2021 Minute Order.

B. Facts Alleged in the Complaint

In the "Factual Allegations" section of the complaint, the Patients allege that "[o]n February 12, 2019, . . . [the Hospitals] . . . suffered a computer hack in which money was demanded in exchange for the release of the computer systems." Compl. ¶ 19.[3] "During this hack, critical patient PII was exposed to the hackers." Id. ¶ 19. "On June 18, 2019, over four months later, [the Hospitals] began sending letters to the breach victims to inform them of the data breaches." Id. ¶ 20.

[3] The Court will refer to this incident as the Ransomware Attack.

According to the Patients, the Hospitals promised to safeguard the patient's information, but nonetheless "allowed [the] hackers to obtain it" during the Ransomware Attack. Id. ¶ 22. This is the entirety of the complaint's factual allegations with respect to the Ransomware Attack. In the "Nature of Action" section of the complaint, the Patients also allege "[o]n information and belief, the security breach compromised [their] full names, addresses, dates of birth, gender, financial information, and social security numbers." Id. ¶ 4.

The letters, referenced in the complaint (though not attached, but submitted separately by the Hospitals), are substantively identical and state:

> On February 12, 2019, we learned that your information was involved in an incident that impacted the Hospital's network . . . . We immediately took steps to ensure the security of your information. None of your information was lost as a result of the incident, and to date there is no evidence to suggest that any of your information was exfiltrated from the network or that there has been any attempt to misuse your information.
>
> The security of your information is of the highest importance to us, and we are handling this incident with the greatest of care. Immediately after the incident, we began an investigation and retained forensic and other consultants to assist us to remediate the effects of the incident, including working with law enforcement. All data, including your information, was restored on April 6, 2019 without any corruption or exfiltration of the data. Moreover, the Hospital and its consultants found no evidence to suggest that your information was viewed, accessed or disclosed as a result of the incident. We will continue to monitor the situation and will advise

> you if we become aware of any new developments. We are also reinforcing our existing security protocols and providing additional training to our employees to reduce the likelihood of a similar event occurring in the future.

Mot. Tendering Ex. Mot. Dismiss, Ex. 1, June 18, 2019 Letter Pablo Quintero ("Letter Pablo Quintero") 1, ECF No. 28-1; Id. Ex. 2, June 18, 2019, Letter Joannie Principe ("Letter Joannie Principe") 1, ECF No. 28-2. Notably, the Patients allege in the complaint that the notification was late, but not that the contents of the letter are inaccurate. Compl. ¶ 20.

The complaint is, however, rife with allegations that the Patients' PII and PHI was "exposed," and the Patients and class are in imminent risk of harm for identity theft and identity fraud. Compl. ¶¶ 10, 19, 51, 57, 58, 60. There are allegations that PII was "disclosed" and "accessed." Id. ¶¶ 66, 115; see also id. ¶ 114. There are vague allegations in the "Nature of the Action" section that the Patients and putative class members PII was "harvested," id. ¶¶ 2, 5, and that unattributed "patient information was stolen," id. ¶ 6. The Patients, on information and belief, claim that PII was "accessed by hackers." Id. ¶ 10.

The allegations of actual theft and misuse of data are, however, conclusory, vague, and logically disconnected from the specific factual allegation concerning the alleged Ransomware Attack. For example, the Patients claim that the Hospitals promised they would not disclose PII or PHI to "any unauthorized

third parties" but "[in fact] allowed them to obtain it." Id. ¶ 22. The Plaintiff's complaint also contains a heading claiming, "the Data Breach has Resulted and Will Result in Identity Theft and Identity Fraud." Id. 11. That section, however, notably contains allegations that do not support identify theft or fraud at all. In a later section, there is a conclusory allegation that the Hospitals' actions and omissions caused "theft and dissemination into the public domain of [the Patients'] . . . PII," but this allegation is tempered by allegations of "potential fraud and identity theft." Id. ¶ 61. While this last allegation certainly could be read on its face that information was sold "on the Internet black market" this allegation is again, when read in context, pure speculation. Id.

III. ANALYSIS

The salient issue in the Hospitals' motion is whether a pure ransomware attack -- an attack that holds data hostage but does not steal it -- is an injury sufficient to confer constitutional standing. As this Court ruled at the hearing, the complaint, when read as a whole, indicates to this Court that, while there are sufficient allegations of a pure ransomware attack, there are speculative and conclusory statements, not supported by sufficiently pleaded facts, that

data was accessed, stolen, and misused. Accordingly, the Court ruled that the Patients have no constitutional standing.

A. The Motion to Dismiss Standard

"The proper vehicle for challenging a court's subject-matter jurisdiction is Federal Rule of Civil Procedure 12(b)(1)." Valentin v. Hosp. Bella Vista, 254 F.3d 358, 362 (1st Cir. 2001). As posed here, it appears that the Hospitals are challenging the sufficiency of the allegations. Therefore, this Court "must credit the [Patients'] well-pleaded factual allegations (usually taken from the complaint, but sometimes augmented by an explanatory affidavit or other repository of uncontested facts), draw all reasonable inferences from them in [their] favor, and dispose of the challenge accordingly." Id. at 363.

The First Circuit applies "the plausibility standard applicable under Rule 12(b)(6) to standing determinations at the pleading stage." Hochendoner v. Genzyme Corp., 823 F.3d 724, 730 (1st Cir. 2016). That is, the Patients "bear[] the burden of establishing sufficient factual matter to plausibly demonstrate his standing to bring the action. Neither conclusory assertions nor unfounded speculation can supply the necessary heft." Id. at 731; see Katz v. Pershing, LLC, 672 F.3d 64, 70 (1st Cir. 2012) ("In considering the pre-discovery grant of a motion to dismiss for lack of standing, we accept as

true all well-pleaded factual averments in the plaintiff's complaint and indulge all reasonable inferences therefrom in his favor." (citations, quotations and punctuation omitted)). At the bottom, this Court must determine "whether all the facts alleged, when viewed in the light most favorable to the plaintiffs, render the plaintiff's entitlement to relief plausible." Ocasio-Hernandez v. Fortuno-Burset, 640 F.3d 1, 14 (1st Cir. 2011) (emphasis original). That is, the Court must "evaluate the cumulative effect of the factual allegations." Id.

"Federal courts are courts of limited jurisdiction and . . . because standing is a prerequisite to a federal court's subject matter jurisdiction, the absence of standing may be raised at any stage of a case." Hochendoner, 823 F.3d at 730. "Each element of standing 'must be supported in the same way as any other matter on which the plaintiff bears the burden of proof, i.e., with the manner and degree of evidence required at the successive stages of the litigation.'" Id. (emphasis in original) (quoting Lujan v. Defs. of Wildlife, 504 U.S. 555, 561 (1992)). "Where, as here, a case is at the pleading stage, the plaintiff must 'clearly . . . allege facts demonstrating' each element." Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1547 (2016) (quoting Warth v. Seldin, 422 U.S. 490, 518 (1975)). Where no class is yet certified, the Court "evaluate[s] only whether the

[named] plaintiff[s have] . . . constitutional . . . standing to pursue the action."[4] Katz v. Pershing, LLC, 672 F.3d 64, 71 (1st Cir. 2012) (citing Nat'l Org. for Women, Inc. v. Scheidler, 510 U.S. 249, 255 & n. 3 (1994)).

B. The Named Patients Lack Standing

"Article III confines the federal judicial power to the resolution of 'Cases' and 'Controversies.'" TransUnion LLC v. Ramirez, 141 S. Ct. 2190, 2203 (2021). "For there to be a case or controversy under Article III, the plaintiff must have a 'personal stake' in the case -- in other words, standing." Id. (citation and quotation omitted). To establish standing, "a plaintiff must show (i) that he suffered an injury in fact that is concrete, particularized, and actual or imminent; (ii) that the injury was likely caused by the defendant; and (iii) that the injury would likely be redressed by judicial relief." Id. at 2203 (citing Lujan, 504 U.S. at 560-61 (1992)); see Suárez-Torres v. Panaderia Y Reposteria España, Inc., 988 F.3d 542, 549 (1st Cir. 2021). Put succinctly, "[i]f the plaintiff does not claim to have suffered an injury that the defendant caused and the court can remedy, there is no case or controversy for the federal court to resolve." TransUnion, 141 S. Ct. at 2203 (citation and quotation omitted).

[4] The parties agree that statutory standing is not an issue before the Court. See Mot. 12; Opp'n 9.

A concrete injury is one that "real, and not abstract." TransUnion, 141 S. Ct. at 2204 (quoting Spokeo, Inc. v. Robins, 578 U.S. 330, 340 (2016)). While "[t]raditional tangible harms, such as physical and monetary harms" are "obvious," intangible harms while less obvious, include "reputational harms, disclosure of private information, and intrusion upon seclusion." Id.

A concrete injury must be "actual or imminent, not conjectural or hypothetical," which "ensures that the harm has either happened or is sufficiently threatening; it is not enough that the harm might occur at some future time." Katz, 672 F.3d 64, 71 (1st Cir. 2012). Indeed, "[s]tanding is not an 'ingenious academic exercise in the conceivable. A plaintiff must allege that he has been or will in fact be perceptibly harmed . . . , not that he can imagine circumstances in which he could be affected.'" Id. at 80 (quoting United States v. Students Challenging Regulatory Agency Procs. (SCRAP), 412 U.S. 669, 688–89 (1973)).

"An allegation of future injury may suffice if the threatened injury is 'certainly impending,' or there is a 'substantial risk' that the harm will occur." Susan B. Anthony List v. Driehaus, 573 U.S. 149, 158 (2014) (emphasis added) (quoting Clapper v. Amnesty Int'l. USA, 568 U.S. 398, 409, 414 n.5 (2013)). It is a "disjunctive . . . test: injury is

imminent if it is certainly impending or if there is a substantial risk that harm will occur." Reddy v. Foster, 845 F.3d 493, 500 (1st Cir. 2017) (emphasis in original).

The First Circuit has not yet addressed the issue of the possibility of future misuse of data in a pure ransomware attack. Moreover, it "has not yet confronted the question . . . [of] whether victims of a data breach who allege that they will face the possibility of future identity theft because cyber-criminals have already used the stolen PII have suffered an injury in fact." Portier v. NEO Tech. Sols., 3:17-CV-30111-TSH, 2019 WL 7946103, at *6 (D. Mass. Dec. 31, 2019) (Robertson, M.J.) (emphasis added) report and recommendation adopted, No. 3:17-CV-30111, 2020 WL 877035 (D. Mass. Jan. 30, 2020).[5]

As Magistrate Judge Robertson correctly articulated in Portier v. NEO Technology Solutions, there is an apparent circuit split on this issue. Id. "The Sixth, Seventh, Ninth, and D.C. Circuits have found that allegations of the threatened risk of future identity theft constitute an injury in fact if the threat is 'sufficiently imminent.'" Id.

The First, "Second and Eighth Circuits have found that plaintiffs who merely alleged an increased risk of future harm

[5] Notably, Portier was a case where there was an allegation of actual theft and use of the data; it was not a ransomware case. Portier, 2019 WL 7946103, at *1.

did not have standing." Id.; see Katz, 672 F.3d at 80 (holding in the context of a non-ransomware case, that when "the plaintiff alleges only that there is an increased risk that someone might access her data and that this unauthorized access (if it occurs) will increase the risk of identity theft and other inauspicious consequences . . . . the risk of harm that she envisions is unanchored to any actual incident of data breach." In this case, "[t]his omission [was] fatal: because [the plaintiff did] not identify any incident in which her data [had] ever been accessed by an unauthorized person, [and, thus could] not satisfy Article III's requirement of actual or impending injury").

In between, "[t]he Third and Fourth Circuits have 'straddled the circuit split with decisions finding no injury in fact based on an increased risk of identity theft based on one set of facts and a cognizable injury in fact on another set of facts.'" Portier, 2019 WL 7946103, at *6; see also Georgia D. Reid, No Standing and No Recourse: The Threat to Employee Data Under Current U.S. Cybersecurity Regulation, 36 Touro L. Rev. 1161, 1183 (2021) (describing circuit split). Despite the apparent split, whether standing exists really depends on a close analysis of the facts alleged. Portier, 2019 WL 7946103, at **15-17.

Due to this apparent split, Magistrate Judge Robertson followed a non-exhaustive, three-factor analysis recently distilled by Judge Scriven in In re 21st Century Oncology Customer Data Security Breach Litigation, 380 F. Supp. 3d 1243, 1251 (M.D. Fla. 2019) ("[A]lthough the circuits have diverged in result, the bases behind the differing decisions have several commonalities."), which attempts to reconcile the perceived split by addressing the following common factors: "(1) the motive of the unauthorized third-party who accessed or may access the plaintiff's sensitive information, (2) the type of sensitive information seized, and (3) whether the information was actually accessed and whether there have been prior instances of misuse stemming from the same intrusion." Id. at 1254-55. The Hospitals, Mot. 9, as well as the Patients, Opp'n 6. (citing Portier factors), follow this rubric and this Court observes that this analytical framework is useful.

Here, the Hospitals appear to concede the second factor -- that the information is sensitive, as it includes social security numbers among other information. Mot. 10 (citing In re 21st Century, 380 F. Supp. 3d at 1253). The Court agrees that the allegations of the complaint support this factor.

As to the first factor, the Court rules that the complaint fails sufficiently to allege motive other than a garden-variety ransomware attack -- targeting the holder of the information by

denying access to the information, the complaint does not allege the hackers intended to steal and sell information. Here, the Hospitals correctly argue that there are no sufficiently pleaded allegations of a motive to steal the PII for identity theft or fraud. Mot. 10 (citing Khan v. Children's Nat'l. Health Sys., 188 F. Supp. 3d 524, 530 (D. Md. 2016)). A review of the complaint reveals only that the attack itself was a ransomware attack -- an exchange of money for return of access to data. Furthermore, the use of statistics in the complaint, a tactic employed "in numerous other cases, do[es] not by [itself] establish that there is 'certainly impending' harm under the specific facts of a given case." Khan, 188 F. Supp. 3d at 533.

As to third factor, the Hospitals argue that there is no evidence of misuse, pointing to Puerto Rico's one-year statute of limitations as a guide. Mot. 10-11 (citing P.R. Laws Ann. tit. 31, §5298). The Hospitals argue, and the Patients confirmed at the hearing, that since the Data Breach they are unaware of evidence of identity theft, fraud, or misuse of the data. Id. Indeed, the letter sent by the Hospitals to the Patients, states that there was no exfiltration of data. See Letter Pablo Quintero 1; Letter Joannie Principe 1. That letter, of course, is not controlling, and the Court is not weighing evidence, but rather parsing the sufficiency of the allegations.

The Patients respond that they have alleged an injury in fact. Opp'n 3. They cite cases that stand for the proposition that where PII is targeted for theft a reasonable inference can be drawn that the data will be misused. Id. 4 (citing Galaria v. Nationwide Mut. Ins. Co., 663 F. App'x 384, 388 (6th Cir. 2016); Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 692–96 (7th Cir. 2015)); cf. Nathaniel Truitt, A Chance to Stand: Why "Loss-of-Chance" Should Replace the "Certainly Impending" Framework for Data Breach Cases, 46 N. Ky. L. Rev. 22, 29, 27 (2019) (arguing, as do the Patients, that relief ought be untethered from actual fraudulent activity). These cases, of course, are not controlling in this Circuit, but in any event are distinguishable because there were, in each case, allegations of fraud or identify theft.[6] See, e.g., Galaria, 663

[6] At the hearing, the Court asked for the Patients' best case factually analogous to this action, and counsel pointed this Court to Remijas, 794 F.3d 688, and Krottner v. Starbucks Corp., 628 F.3d 1139 (9th Cir. 2010). Those cases are distinguishable. "In Krottner and Remijas, the allegations included either actual examples of the use of the fruits of the data breach for identity theft, even if involving victims other than the named plaintiffs, or a clear indication that the data breach was for the purpose of using the plaintiffs' personal data to engage in identity fraud." Khan, 188 F. Supp. 3d at 530. Moreover, neither were ransomware cases.

The parties each also cite to TransUnion as support for their respective positions. TransUnion provides a recitation of the elements of standing; it is not a ransomware case. TransUnion, 141 S. Ct. at 2203. Rather, on the facts it is a credit reporting case deciding primarily an issue of Article III standing under federal law. Id. at 2207. There, certain class members had their inaccurate credit reports disseminated to

F. App'x at 386 ("[H]ackers broke into [the defendant's] computer network and stole the personal information of Plaintiffs . . . [The defendant] also suggested that Plaintiffs set up a fraud alert and place a security freeze on their credit reports."); Remijas, 794 F.3d at 692 ("Here, the complaint alleges that everyone's personal data has already been stolen; it alleges that the 9,200 who already have incurred fraudulent charges have experienced harm.").

The Patients also cite to Magistrate Judge Robertson's Portier decision and adopt the In re 21st Century analysis that she performed. Opp'n 5-6. They agree with the Hospitals that

---

third parties -- standing existed because of a concrete injury. See id. at 2209. With respect to the remaining class members there was no demonstration of dissemination of any incorrect credit information. See id. at 2212. The Court held that in the absence of actual dissemination, or some claim for independent harm to the risk of their credit reports being exposed, such as emotional distress damages, that risk of future harm was "unavailing" for Article III purposes. Id. at 2212 (emphasis added). Furthermore, there was not a "sufficient risk" of future harm where the risk was "too speculative to support Article III standing. Id. (emphasis added). Indeed, the Court found "persuasive argument that in a suit for damages, the mere risk of future harm, standing alone, cannot qualify as a concrete harm -- at least unless the exposure to the risk of future harm itself causes a separate concrete harm." Id. at 2210-11. As TransUnion argued, "if an individual is exposed to a risk of future harm, time will eventually reveal whether the risk materializes in the form of actual harm." Id. at 2211. Applied here, TransUnion does not change the analysis. There is no allegation of emotional distress, and even if there was the TransUnion Court took no position as to what would be sufficient in that circumstance. Id. at 2211 n. 7. In the context of a pure ransomware case, TransUnion does not enhance the Patients' standing argument.

the information was sensitive -- it included social security numbers. Id. 6. They further argue that:

> [t]he data was stolen by hackers who held [the Hospitals'] system hostage. These were individuals with malevolent intent, looking to profit from their intrusion, and they can be expected to have sold the data on the dark web in addition to holding it hostage. The type of information that was stolen was highly sensitive, including social security numbers. And the data was actually accessed. It was encrypted by the hackers, which required them to access it.

Id. That argument -- access by encryption equals acquisition and misuse -- is a bridge too far, mere speculation, and is not in accord with the modern trend in this area of the law. See Hartigan v. Macy's, Inc., 501 F. Supp. 3d 1, 5 (D. Mass. 2020) (Saris, J.) (finding no substantial risk of future harm where among other things "there [were] no allegations of any fraudulent use or even attempted use of the personal information to commit identify theft with respect to any Macy's customer whose credit information was stolen."); Portier, 2019 WL 7946103, at *8 ("If identity theft has occurred, courts are more apt to find an imminent harm. . . . On the other hand, courts are less likely to find an injury in fact where there are no allegations of fraudulent misuse of the stolen information."); Khan, 188 F. Supp. 3d at 531 ("The majority of district courts faced with challenges to the standing of data breach victims follow this pattern. In the absence of specific incidents of the use of stolen data for identity fraud purposes, district

courts have generally found that the increased risk of identity theft does not confer standing."); In re Zappos.com, Inc., 108 F. Supp. 3d 949, 955 (D.Nev. 2015) (listing cases).

As a final argument, the Patients claim they have lost the benefit of their bargain with the Hospitals to not have their confidential information exposed, Opp'n 7 (citing Carlsen v. GameStop, Inc., 833 F.3d 903, 909 (8th Cir. 2016)), a point left open in this Circuit by Katz, see Katz, 672 F.3d at 77 ("The plaintiff's remonstrances about the benefit of the bargain do not change this calculus. She has no bargain with the defendant and, therefore, no entitlement to any benefit from the defendant."); see also Hartigan, 501 F. Supp. 3d at 6 ("The breach of a contractual right can constitute an injury sufficient to create standing.") (citing Katz, 672 F.3d at 72)). This argument is insufficient here.

In Carlsen v. Gamstop, Inc., the plaintiff had a video game subscription with the defendants. 833 F.3d at 907. The Eighth Circuit cautioned not to conflate standing and a potential cause of action. Id. at 909. That court found an actual injury:

> Here, Carlsen has provided sufficient facts alleging that he is party to a binding contract -- the terms of service, which include the Game Informer privacy policy -- with GameStop, and GameStop does not dispute this contractual relationship. Carlsen also has alleged that GameStop has violated that policy by "systematically disclos[ing] Game Informer's users' PII . . . to third party Facebook and/or allow[ing] Facebook to directly collect that information itself."

> This allegation of breach is both concrete and particularized, as the breach allegedly already has occurred, and any consequences of the breach have occurred specifically to Carlsen as a result of the actions of GameStop's alleged systematic disclosure via the Facebook SDK. Additionally, Carlsen alleged that he has suffered damages as a result of GameStop's breach in the form of devaluation of his Game Informer subscription in an amount equal to the difference between the value of the subscription that he paid for and the value of the subscription that he received, i.e., a subscription with compromised privacy protection. Accordingly, Carlsen has alleged an "actual" injury. See id. at 961; cf. Ben Oehrleins & Sons & Daughter, Inc. v. Hennepin Cty., 115 F.3d 1372, 1379–80 (8th Cir. 1997) (finding even indirect economic injury constitutes an injury in fact where the injury was concrete, particularized, actual, and in no way hypothetical or conjectural).

Id. at 909. The Patients analogize that the devaluation of a video game company's subscription, which included privacy protection, is the same as privacy obligations that are purportedly concomitant with the provision of medical services. Opp'n 7.

In reply, the Hospitals do not attack the benefit of the bargain theory directly, but argue persuasively that the Patients assume that the "PII was accessed and [is] currently in the possession of unknown third parties." Reply 1. Simply put, as argued by the Hospitals, "[w]here, as here, the third party did not exfiltrate PII, there is no harm." Id. 2.

The Court rules that, on balance, to the extent that this was a pure ransomware attack, the bald allegations of the complaint read in their entirety are insufficient to convert

this into a data theft case. See, e.g., Graham v. Universal Health Serv., Inc., CV 20-5375, 2021 WL 1962865, at *4 (E.D. Pa. May 17, 2021) ("The target of a ransomware attack is the holder of the confidential data; the misappropriation of the data, whether by theft or merely limitation on access to it, is generally the means to an end: extorting payment. A court is still left to speculate, as in Reilly, whether the hackers acquired Plaintiffs' PHI in a form that would allow them to make unauthorized transactions in their names, as well as whether Plaintiffs are also intended targets of the hackers' future criminal acts. At this juncture, the most Plaintiffs can plead is that the hackers secured their PHI through a ransomware attack against Universal."). Here, on the current state of the law, the inclusion of a benefit of the bargain claim does not confer standing on this complaint. See Clemens v. ExecuPharm, Inc., CV 20-3383, 2021 WL 735728, at *5 (E.D. Pa. Feb. 25, 2021) (dismissing claim for lack of standing, even though an alternate basis of contractual standing was proposed, where the Third Circuit had not ruled on issue and "the presence of contractual claims [had] not been relevant to courts' analyses of standing in data breach cases in [the] Circuit"); Browne v. US Fertility, LLC, CV 21-367, 2021 WL 2550643, at *3 (E.D. Pa. June

22, 2021);[7] see also Blahous v. Sarrell Reg'l. Dental Ctr. for Pub. Health, Inc., 2:19-CV-798-RAH-SMD, 2020 WL 4016246, at *6 (M.D. Ala. July 16, 2020); Abernathy v. Brandywine Urology Consultants, P.A., C.A. No. N20C-05-057-MMJCCLD, 2021 WL 211144, at *5 (Del. Super. Ct. Jan. 21, 2021).

IV. CONCLUSION

The named Patients in this action have alleged a pure ransomware attack against the Hospitals: a third-party holding the Patients information hostage in exchange for money from the Hospitals. Absent plausible allegations that the information itself was accessed and misused the named Patients lack constitutional standing to sue the Hospitals because the injury is not actual or imminent, but rather is merely conjectural or hypothetical. The hearing confirms that the Patients have not suffered identity theft or fraud. Reading the well-pleaded allegations of the complaint in whole, and taking all inferences in favor of the Patients, what is alleged plausibly to have happened is a pure ransomware attack, with conjectural and

[7] While these cases arise in the Third Circuit, which requires actual misuse, see Reilly v. Ceridian Corp., 664 F.3d 38, 42 (3d Cir. 2011), the Court is persuaded by their reasoning that pure ransomware cases are fundamentally different from data theft cases for purposes of standing, even under alternative theories such as breach of contract. Moreover, the Patients have not pointed this Court to any case where a patient has been able to assert standing under a loss of benefit of the bargain theory absent misuse of the information.

speculative allegations of a theft and a fraud that have not yet materialized.

Accordingly, for the aforementioned reasons, the Hospitals' motion to dismiss for lack of standing pursuant to Fed. R. Civ. P. 12(b)(1) (ECF No. 18) was ALLOWED, as to the remaining grounds it was DENIED as MOOT, and the action was DISMISSED without prejudice.[8]

/s/ William G. Young
WILLIAM G. YOUNG
JUDGE
of the
UNITED STATES[9]

[8] The Court only decides the standing issue because when a "court is confronted with motions to dismiss under both Rules 12(b)(1) and 12(b)(6), it ordinarily ought to decide the former before broaching the latter." Deniz v. Mun. of Guaynabo, 285 F.3d 142, 149 (1st Cir. 2002). Indeed, "deciding a Rule 12(b)(6) motion after finding no subject-matter jurisdiction is gratuitous." United States v. Millenium Laboratories, Inc., 923 F.3d 240, 251 n. 13 (1st Cir. 2019), cert. denied sub nom., Estate of Cunningham v. McGuire, 140 S. Ct. 851 (2020).

[9] This is how my predecessor, Peleg Sprague (D. Mass 1841-1865), would sign official documents. Now that I'm a Senior District Judge I adopt this format in honor of all the judicial colleagues, state and federal, with whom I have had the privilege to serve over the past 43 years.