

United States Court of Appeals For the First Circuit

No. 24-2018

BETZAIDA SANTOS-PAGÁN,

Plaintiff, Appellant,

MINERVA M. HERNÁNDEZ-UMPIERRE,

Plaintiff,

v.

BAYAMON MEDICAL CENTER,

Defendant, Appellee,

DOES 1 TO 10,

Defendants.

APPEAL FROM THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF PUERTO RICO

[Hon. Bruce J. McGiverin, U.S. Magistrate Judge]

Before

Gelpí, Thompson, and Montecalvo,
Circuit Judges.

Jesenia A. Martinez, with whom Wilshire Law Firm, PLC, David C. Indiano-Vicic, Joanne J. Pimentel de Jesus, and Indiano & Williams, P.S.C., were on brief, for appellant.

Michael Craig McCall, with whom Law Offices of Michael Craig McCall, José A. Morales Boscio, and Morales Boscio Law Offices PSC were on brief, for appellee.

June 11, 2026

MONTECALVO, Circuit Judge. Plaintiff-Appellant Betzaida Santos Pagán¹ ("Santos") filed a putative class action in the U.S. District Court for the District of Puerto Rico against Defendant-Appellee Bayamón Medical Center ("BMC"), asserting various claims arising from a data breach. She alleged that the personally identifiable information ("PII") and protected health information ("PHI") of 522,493 BMC patients, including her own, was exposed in that breach. In relevant part, the district court dismissed the appeal for lack of Article III standing, concluding that Santos's complaint did not plausibly allege that her purported injury was traceable to BMC's data breach. For the reasons stated below, we affirm.

I. Background

BMC is a hospital located in Bayamón, Puerto Rico. As part of its operations, BMC collects and maintains records of its patients' PII and PHI, including "full names, Social Security numbers, dates of birth, and medical diagnoses." On May 21, 2019, BMC learned that it had been subject to a ransomware attack -- a type of data breach in which hackers use malicious software to access and encrypt files on a device or server to: (1) render unusable the files and the system dependent on them; and (2) demand

¹ While the Appellant's name appears as "Santos-Pagán" on the appellate docket, we refer to her here as "Santos Pagán" because that is how she has referred to herself in this appeal.

a ransom in exchange for decrypting those files. About two months later, on July 19, 2019, BMC disclosed the data breach to its patients in a notice letter, which explained that hackers had accessed patients' PII and PHI during the breach. The notice letter also stated that, after an investigation into the breach, BMC learned that patients' PII and PHI were "simply encrypted" and there was "no indication[] that the information itself ha[d] been used by an unauthorized person." Santos, a Puerto Rico resident and former BMC patient, received BMC's notice letter.

On May 22, 2020, Santos and Minerva Hernández Umpierre² ("Umpierre"), another former BMC patient, filed a putative class action against BMC in the U.S. District Court for the District of Puerto Rico, invoking the court's jurisdiction under the Class Action Fairness Act of 2005 ("CAFA"), 28 U.S.C. § 1332(d)(2). The complaint asserted claims under Puerto Rico law for breach of an express or implied contract, breach of the covenant of good faith and fair dealing, and negligence. The plaintiffs alleged the data breach stemmed directly from BMC's failure to properly safeguard patient PII from unauthorized access. They asserted that this failure: (1) placed the plaintiffs and the putative class members "at an imminent, immediate, and continuing risk of harm from

² Like the Appellant's name, Hernández Umpierre's name is hyphenated on the appellate docket, but we refer to her here as "Hernández Umpierre" as that is how the Appellant refers to her in this appeal.

identity theft"; (2) required them to spend time and effort mitigating the breach's potential impact; (3) caused them to incur "out-of-pocket losses" from purchasing credit monitoring services; and (4) diminished their PII's value.

On August 31, 2023, BMC moved for judgment on the pleadings under Federal Rule of Civil Procedure 12(c). It contended, in relevant part, that the plaintiffs lacked Article III standing and had failed to plausibly allege facts supporting jurisdiction under CAFA. As to standing, BMC argued that the complaint did not plausibly allege an injury in fact because it lacked factual allegations that the plaintiffs suffered or would imminently suffer from identity theft or fraud due to the data breach. And, BMC insisted, plaintiffs' merely speculative allegations of a future risk of identity theft or fraud did not constitute injury in fact either.

Three weeks later, the plaintiffs moved for leave to file a first amended complaint ("FAC") that would: (1) "include federal question jurisdiction" by adding allegations that BMC violated the Storage Communications Act ("SCA"), 18 U.S.C. §§ 2701, et seq.; and (2) allege additional facts about the harms Umpierre suffered from the breach, including bank fraud, having to change her telephone number and her mobile payment account information, and inaccurate missed payments on her credit report. The plaintiffs did not seek to add new factual allegations as to

Santos. The district court granted the plaintiffs' motion, prompting them to file the FAC on September 28, 2023.

On November 27, 2023, BMC moved under Rule 12(b)(1) to dismiss Umpierre's claims in the FAC, arguing that she lacked standing because she became a BMC patient weeks after BMC discovered the data breach and therefore could not have had her PII exposed during the breach. The district court granted the motion, dismissing Umpierre's claims without prejudice.

With Santos as the remaining named plaintiff, BMC moved for judgment on the pleadings as to all claims in the FAC. It principally argued that the FAC did not show, for Article III standing purposes, that Santos suffered an injury in fact. For support, it argued that Santos failed to allege she had suffered from identity theft or fraud and that her allegations of a risk of future identity theft or fraud were "sheer speculation."

On April 19, 2024, nearly five years after the initial data breach and four years after her suit was first filed, Santos moved for leave to amend the FAC to add additional facts "discovered after the [FAC] was filed" -- specifically, the harm she suffered from BMC's data breach. The district court granted the motion, allowing Santos to file a second amended complaint ("SAC"). The SAC newly alleged that, "[a]fter [Santos] received [BMC]'s breach notice on July 19, 2019, she discovered an unknown cellphone account opened in her name" which caused her to "expend

time and money, including spending approximately \$800.00 to repair her credit score" and monitoring her credit reports and accounts for unauthorized activity.

BMC moved to dismiss Santos's claims under Rules 12(b) and (c) and alternatively moved for a more definite statement under Rule 12(e). Again, it argued that Santos lacked Article III standing, contending that the SAC still failed to show a concrete injury. BMC explained that Santos did not plead that she suffered any economic damages associated with the opening of the unauthorized cellphone account. Thus, it argued, the SAC did not contain allegations that Santos was an identity theft or fraud victim who suffered an injury in fact, "much less injury resulting from the [data breach] and plausibly traceable to BMC." Additionally, as to Santos's claims that she risked future identity theft or fraud, BMC reiterated that such allegations were speculative. Santos opposed the motion.

On September 30, 2024, the district court³ granted BMC's motion to dismiss for lack of standing and subject matter

³ In December 2023, District Court Judge Francisco A. Besosa issued an order giving the parties two weeks to file a motion stating whether they would consent to have a magistrate judge preside over the case pursuant to 28 U.S.C. § 636(c)(1). Judge Besosa indicated that the parties' "failure to comply with [the] order . . . [would] be considered implicit consent to try the case before a magistrate judge and to the entry of judgment by that magistrate judge." Accordingly, when the parties failed to comply with that order, Judge Besosa referred the case to Magistrate Judge Bruce J. McGiverin. Thus, Magistrate Judge McGiverin issued the

jurisdiction. Regarding standing, the court concluded that Santos did not meet "her burden to show that the fraudulent cellphone account [was] traceable to BMC's cyberattack." And as to subject matter jurisdiction, the court determined that Santos failed to state a claim under the SCA and that her allegations were insufficient to meet her burden of establishing minimal diversity under CAFA. Further, it denied as futile Santos's request for leave to perform jurisdictional discovery in light of its conclusion that Santos failed to establish standing. Thus, it dismissed Santos's SCA claim with prejudice and her Puerto Rico law claims without prejudice. Santos timely appealed.

II. Discussion

On appeal, Santos challenges the district court's determinations on standing and subject matter jurisdiction. But we need not address subject matter jurisdiction because, for the reasons stated below, we affirm the district court's determination that Santos lacks Article III standing.⁴

A. Standard of Review

Under Article III of the Constitution, our judicial power is limited to "Cases" and "Controversies." U.S. Const. art.

motion to dismiss order on appeal. The parties on appeal do not contest Judge McGiverin's authority, under § 636(c)(1), to enter judgment.

⁴ Because the claims in Santos's complaint "all arise from the [BMC] data breach, and neither party argues that the standing inquiry differs with respect to any claim . . . we treat the claims

III, § 2, cl. 1. "One element of the case-or-controversy requirement is that plaintiffs must establish that they have standing to sue." Kerin v. Titeflex Corp., 770 F.3d 978, 981 (1st Cir. 2014) (quoting Blum v. Holder, 744 F.3d 790, 795 (1st Cir. 2014)). Whether standing exists is a legal question that we review de novo. Id. (citing Katz v. Pershing, LLC, 672 F.3d 64, 70 (1st Cir. 2012)). And when we review a "pre-discovery grant of a motion to dismiss for lack of standing, we accept as true all well-pleaded facts . . . and indulge all reasonable inferences in the plaintiff's favor." Id. (citation modified). To demonstrate standing, "a plaintiff must sufficiently plead three elements: injury in fact, traceability, and redressability." Id. The two standing elements at issue here are injury in fact and traceability, so we square our focus on them and address each in turn.

B. Injury in Fact

As we will explain, Santos's complaint sufficiently alleges the injury in fact element.

"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." Id. (citation modified). We have said that "actual misuse of PII may constitute

together throughout our analysis." Webb v. Injured Workers Pharmacy, LLC, 72 F.4th 365, 373 n.3 (1st Cir. 2023).

an injury in fact." Webb v. Injured Workers Pharmacy, LLC, 72 F.4th 365, 373 (1st Cir. 2023). The complaint alleges that third-party access to Santos's PII and PHI caused her to "suffer financial fraud," i.e., the fraudulent cellphone account, which prompted her to spend time and \$800 to mitigate the resulting damage to her credit score. After reviewing Santos's complaint as a whole, and drawing reasonable inferences in her favor, we find that the complaint's plausible allegations of actual misuse of her PII state an injury in fact.⁵ See Kerin, 770 F.3d at 981.

Separate from actual misuse, for the first time in her reply brief, Santos asserted that her actions to mitigate and prevent future harms from her PII misuse, as alleged in her complaint, serve as an alternative basis for demonstrating injury in fact. Whether those alleged actions suffice to plead injury in fact is a nuanced, fact-specific question. See Webb, 72 F.4th at 375. But we need not address it because Santos did not raise or develop those arguments in her opening brief, and therefore we deem them waived. See id. at 374 n.5 (explaining that argument raised for the first time in appellants' reply brief was waived).

⁵ To the extent that Santos seeks to establish standing based on the conclusory allegations in her complaint of "diminution of the value of [her] PHI and PII" or the loss of the "the benefit[] of [her] bargain[]" with BMC, she did not raise those arguments in this appeal and thus we do not address them.

C. Traceability

Whether Santos's complaint plausibly alleges that her injury in fact is traceable to BMC's conduct is the next inquiry. For Article III standing, the traceability requirement does not demand proximate causation, but "requires only that the plaintiff's injury be fairly traceable to the defendant's conduct." Lexmark Int'l, Inc. v. Static Control Components, Inc., 572 U.S. 118, 134 n.6 (2014). And an injury in fact is "fairly traceable" to the defendant's conduct if there is "a causal connection between the injury and the conduct complained of." Conservation L. Found., Inc. v. Acad. Express, LLC, 129 F.4th 78, 90 (1st Cir. 2025) (quoting Lujan v. Defs. of Wildlife, 504 U.S. 555, 560 (1992)). The traceability requirement is not met if the injury is "the result of the independent action of some third party not before the court." Lujan, 504 U.S. at 560 (citation modified).

In Webb, we determined that one of the plaintiffs did plausibly allege a connection between the misuse of her PII, via a fraudulently filed 2021 tax return, and the data breach that the defendant experienced. 72 F.4th at 372-73. In reaching that conclusion, we first noted that there was an "obvious temporal connection" between the filing of the fraudulent 2021 tax return -- presumably filed in 2022 -- and the data breach, which occurred in January 2021. Id. at 370, 374. Additionally, we noted how the plaintiff, in the context of describing her harms from the

breach, alleged that her PII was being used by an unauthorized individual. Id. at 374. Lastly, we highlighted that the plaintiff alleged that she was "very careful about sharing her PII, ha[d] never knowingly transmitted unencrypted PII over the internet or any other unsecured source, and store[d] documents containing her PII in a secure location." Id. (citation modified). From those allegations, we determined an obvious inference could be drawn that the fraudulent tax return was filed using PII obtained from the data breach, not another source. Id.

Like the Webb plaintiff, Santos alleged, when describing the purported harm from the data breach, that her PII was used by unauthorized third parties. But the similarities to the allegations in Webb end there. Outside of the conclusory allegation that the PII used to open the fraudulent cellphone account was obtained from BMC's data breach, the general allegations in Santos's complaint do not "embrace those specific facts . . . necessary to support a link between a plaintiff's fraudulent charge and the data breach[]." See id. (citation modified); see Ruiz v. Bally Total Fitness Holding Corp., 496 F.3d 1, 4 (1st Cir. 2007) (noting that "our obligation to approach the facts from this plaintiff-friendly vantage," when reviewing the district court's grant of a motion to dismiss, "does not require us to credit bald assertions, unsupportable conclusions, and opprobrious epithets" (citation modified)).

To start, the complaint's allegations do not provide plausible support for a reasonable, let alone "obvious," inference of a temporal connection between the opening of the fraudulent cellphone account and the data breach. In Webb, the plaintiff's allegations suggested about a one-year gap between the data breach and the fraudulent tax return and thus presented an "obvious temporal connection." See 72 F.4th at 370, 374. But here, the complaint alleges that Santos discovered a fraudulent cellphone account after she received BMC's notice letter, neither setting forth when that account was opened nor providing a plausible basis to reasonably infer the temporal proximity between the account's opening and the data breach.

Other frailties as to temporal connection are evident in the record. Recall that in her motion for leave to amend her FAC, Santos characterized her allegation that a fraudulent cellphone account was opened in her name as part of "additional facts discovered after the [FAC] was filed" on September 28, 2023. That characterization suggests that Santos discovered the fraudulent cellphone account sometime after September 2023 -- more than four years after the BMC data breach. The wide, years-long temporal gap between the data breach and the presumed period when Santos discovered the fraudulent cellphone account, paired with the lack of any specific facts alleging when that account was opened,

negates a reasonable inference of a temporal connection between the purported fraud and the data breach.⁶

Next, unlike the complaint in Webb, the complaint here does not allege that Santos: (1) was "careful about sharing her PII"; (2) "never knowingly transmitted unencrypted PII over the internet or any other unsecured source"; or (3) "store[d] documents containing her PII in a secure location." 72 F.4th at 374. Santos asserts that the complaint shows that she protects her PII because it alleges that she relied on BMC's promises to safeguard her information before disclosing it to BMC. But the Webb plaintiffs relied on a similar promise from the entity collecting their PII. See id. at 370 ("[The defendant] represented to patients that it would keep their PII secure."). Yet, in Webb, the complaint's allegations illustrated how one of the plaintiffs generally protected and secured her PII from unauthorized access. Id. at 374. And those same allegations supported the reasonable inference that those responsible for misusing her PII did not obtain such PII from sources other than the data breach. See id. Santos's mere reliance on BMC's promise to protect her PII does not contribute to the reasonable inference that those who misused her PII did not obtain it from another source.⁷

⁶ The language of the complaint is so vague about the timing of the fraudulent cellphone account that it is unclear whether the account's opening even occurred after the breach.

⁷ To be clear, we do not hold that every complaint like

Lastly, the complaint does not allege whether the information the fraudster would have needed to open a cellphone account is even the kind of information that Santos provided to BMC or that was exposed in the data breach. Santos disagrees, emphasizing that the complaint alleges that cybercriminals use PII and PHI for crimes including phone or utilities fraud. But still, this allegation does not indicate what type of PII or PHI is used to open a cellphone account and whether that PII was in BMC's files at the time of the breach. Only in Santos's brief does she attempt to make such a showing, stating that "the only personal data needed to open a cellphone account is the data that [Santos] provided to BMC." And even if Santos had proffered that contention in her complaint, it constitutes the type of bald assertion we are not required to credit. Ruiz, 496 F.3d at 4.

In sum, the allegations in Santos's complaint do not plausibly support a reasonable inference that the opening of the fraudulent cellphone account is fairly traceable to the BMC data breach. And, in the absence of a plausible showing of traceability, Santos lacks standing to raise her claims and we therefore lack jurisdiction to review those claims.⁸

Santos's requires allegations listed in the parenthetical numbers above. We simply hold that her attempt to clear standing's traceability hurdle with Webb fails and that her complaint's allegations do not do the job.

⁸ Because there is no plausible support for the allegations that the fraudulent cellphone account was traceable to the BMC

III. Conclusion

For the reasons stated above, we affirm the district court's order dismissing Santos's claims.⁹

breach, it is also not plausible that the alleged consequential harms from the fraud are traceable to the data breach. Therefore, even if Santos preserved (and we agreed with) her argument that her allegations as to the time and costs incurred to mitigate the harms from the fraudulent cellphone account state an injury of fact, her standing argument based on that injury would still flounder at the traceability element.

⁹ Santos's opening brief hints that if we affirm the order dismissing her SAC, we "should nonetheless reverse" the order's dismissal "with prejudice" so that she can amend her complaint yet again. But we deem the argument waived by cursory treatment, noting too that "[t]he slight development in [her] reply brief" comes too late. See Braintree Lab'ys, Inc. v. Citigroup Glob. Mkts. Inc., 622 F.3d 36, 43-44 (1st Cir. 2010).