PUBLISHED

UNITED STATES COURT OF APPEALS
FOR THE FOURTH CIRCUIT

No. 15-1395

RICHARD G. BECK; LAKRESHIA R. JEFFERY; BEVERLY WATSON; CHERYL GAJADHAR; JEFFERY WILLHITE, on behalf of themselves and all others similarly situated,

Plaintiffs - Appellants,

v.

ROBERT A. MCDONALD, in his official capacity as Secretary of Veterans Affairs; TIMOTHY B. MCMURRY, in his official capacity as the former Medical Director of William Jennings Bryan Dorn VA Medical Center; BERNARD L. DEKONING, in his official capacity as the Chief of Staff of William Jennings Bryan Dorn VA Medical Center; RUTH MUSTARD, RN, Director for Patient Care-Nursing Services of William Jennings Bryan Dorn VA Medical Center; JON ZIVONY, Assistant Director of William Jennings Bryan Dorn VA Medical Center; DAVID L. OMURA, in his official capacity as the Associate Director of William Jennings Bryan Dorn VA Medical Center,

Defendants – Appellees.

No. 15-1715

BEVERLY WATSON, on behalf of herself and all others similarly situated,

Plaintiff - Appellant,

v.

ROBERT A. MCDONALD, in his official capacity as Secretary of Veterans Affairs; TIMOTHY MCMURRY, in his official capacity as the Medical Director of William Jennings Bryan Dorn VA Medical Center; RUTH MUSTARD, RN, in

her official capacity as the Associate Director for Patient Care/Nursing Services of William Jennings Bryan Dorn VA Medical Center; DAVID L. OMURA, in his official capacity as the Associate Director of William Jennings Bryan Dorn VA Medical Center; JON ZIVONY, in his official capacity as the Assistant Director of William Jennings Bryan Dorn VA Medical Center; SUE PANFIL, in her official capacity as the Privacy Officer of William Jennings Bryan Dorn VA Medical Center,

Defendants – Appellees.

Appeals from the United States District Court for the District of South Carolina, at Columbia. Terry L. Wooten, Chief District Judge. (3:13−cv−00999−TLW; 3:14-cv-03594-TLW)

Argued: September 20, 2016 Decided: February 6, 2017

Before NIEMEYER and DIAZ, Circuit Judges, and Irene M. KEELEY, United States District Judge for the Northern District of West Virginia, sitting by designation.

Affirmed by published opinion. Judge Diaz wrote the opinion, in which Judge Niemeyer and Judge Keeley joined.

ARGUED: Douglas J. Rosinski, Columbia, South Carolina, for Appellants. Sonia Katherine McNeil, UNITED STATES DEPARTMENT OF JUSTICE, Washington, D.C., for Appellees. **ON BRIEF**: D. Michael Kelly, Bradley D. Hewett, MIKE KELLY LAW GROUP, LLC, Columbia, South Carolina, for Appellants. Benjamin C. Mizer, Principal Deputy Assistant Attorney General, Mark B. Stern, Civil Division, UNITED STATES DEPARTMENT OF JUSTICE, Washington, D.C.; William N. Nettles, United States Attorney, OFFICE OF THE UNITED STATES ATTORNEY, Columbia, South Carolina, for Appellees.

DIAZ, Circuit Judge:

The Plaintiffs in these consolidated appeals are veterans who received medical treatment and health care at the William Jennings Bryan Dorn Veterans Affairs Medical Center ("Dorn VAMC") in Columbia, South Carolina. After two data breaches at the Center compromised their personal information, the Plaintiffs brought separate actions against the Secretary of Veterans Affairs and Dorn VAMC officials ("Defendants"), alleging violations of the Privacy Act of 1974, 5 U.S.C. § 552a *et seq.* and the Administrative Procedure Act ("APA"), 5 U.S.C. § 701 *et seq.*

In both cases, the Plaintiffs sought to establish Article III standing based on the harm from the increased risk of future identity theft and the cost of measures to protect against it. The district court dismissed the actions for lack of subject-matter jurisdiction, holding that the Plaintiffs failed to establish a non-speculative, imminent injury-in-fact for purposes of Article III standing. We agree with the district court and therefore affirm.

I.

A.

The *Beck* case arises from a report that on February 11, 2013, a laptop connected to a pulmonary function testing device with a Velcro strip was misplaced or stolen from Dorn VAMC's Respiratory Therapy department. The laptop contains unencrypted personal information of approximately 7,400 patients, including names, birth dates, the last four digits of social security numbers, and physical descriptors (age, race, gender, height, and weight).

An internal investigation determined that the laptop was likely stolen and that Dorn VAMC failed to follow the policies and procedures for utilizing a non-encrypted laptop to store patient information. Dorn VAMC officials used medical appointment records to notify every patient tested using the missing laptop and offered one year of free credit monitoring. To date, the laptop has not been recovered.

Richard Beck and Lakreshia Jeffery (the "*Beck* plaintiffs")[1] filed suit on behalf of a putative class of the approximately 7,400 patients whose information was stored on the missing laptop. Relevant to this appeal, the *Beck* plaintiffs sought declaratory relief and monetary damages under the Privacy Act, alleging that the "Defendants' failures" and "violations" of the Privacy Act "caused Plaintiffs . . . embarrassment, inconvenience, unfairness, mental distress, and the threat of current and future substantial harm from identity theft and other misuse of their Personal Information." J.A. 12. They further allege that the "threat of identity theft" required them to frequently monitor their "credit reports, bank statements, health insurance reports, and other similar information, purchas[e] credit watch services, and [shift] financial accounts." J.A. 12.

In addition to their Privacy Act claims, the *Beck* plaintiffs sought broad injunctive relief under the APA, requiring the VA to account for all Privacy Act records in the possession of Dorn VAMC and to recover and permanently destroy any improperly maintained records. The *Beck* plaintiffs also sought to enjoin the Defendants from transferring patient information from computer systems to any portable device "until and

[1] The *Beck* plaintiffs later amended their complaint to add as named plaintiffs Beverly Watson, Cheryl Gajadhar, and Jeffery Willhite.

unless Defendants demonstrate to the Court that adequate information security has been established." J.A. 23. Finally, the *Beck* plaintiffs alleged separate common-law negligence claims.

The Defendants moved to dismiss for lack of subject-matter jurisdiction or, in the alternative, for failure to state a claim. The district court granted the motion as to the common-law negligence claims, but declined to dismiss the Privacy Act and APA claims.

Following extensive discovery, the Plaintiffs moved for partial summary judgment and for class certification. The Defendants renewed their motion to dismiss the Plaintiffs' claims for lack of subject-matter jurisdiction and, in the alternative, moved for summary judgment. The district court granted the Defendants' motion to dismiss, holding, pursuant to *Clapper v. Amnesty International USA*, 133 S. Ct. 1138, 1155 (2013), that the *Beck* plaintiffs lacked standing under the Privacy Act because they had "not submitted evidence sufficient to create a genuine issue of material fact as to whether they face a 'certainly impending' risk of identity theft." J.A. 1059.

The *Beck* plaintiffs' fear of harm from future identity theft, said the district court, was too speculative to confer standing because it was "contingent on a chain of attenuated hypothetical events and actions by third parties independent of the defendants." J.A. 1059 (citing *Clapper*, 113 S. Ct. at 1148). The *Beck* plaintiffs also failed to satisfy the "lesser standard" of "substantial risk" of future harm referenced in *Clapper*: The plaintiffs' calculations that 33% of those affected by the laptop theft would have their identities stolen and that all affected would be 9.5 times more likely to

experience identity theft "d[id] not suffice to show a substantial risk of identity theft." J.A. 1060.

The district court also rejected the *Beck* plaintiffs' attempt to "create standing by choosing to purchase credit monitoring services or taking any other steps designed to mitigate the speculative harm of future identity theft." J.A. 1061. These measures, according to the court, did not amount to an injury-in-fact because they were taken solely "to mitigate a speculative future harm." J.A. 1061.

Turning to the *Beck* plaintiffs' request for injunctive relief under the APA, the district court acknowledged that the claim that "there have been at least seventeen data breaches at Dorn [VAMC] during the course of th[e] [*Beck*] litigation" was "undoubtedly concerning." J.A. 1064. Nonetheless, the court concluded that Dorn VAMC's "past Privacy Act violations are insufficient to establish Plaintiffs' standing to seek injunctive relief" where it was "no more than speculation for Plaintiffs to assert that their personal information will again be compromised by a future Privacy Act violation *and* that they will be injured as a result." J.A. 1064.

The district court ruled in the alternative that the Defendants were entitled to summary judgment on the merits, because: (1) the *Beck* plaintiffs had not suffered "actual damages" as required to recover damages under the Privacy Act, and (2) the APA could not be read to "provide for the broad judicial oversight" of the VA's entire privacy program sought by the Plaintiffs. J.A. 1067–68.

B.

The *Watson* case arises from Dorn VAMC's July 2014 discovery that four boxes of pathology reports headed for long-term storage had been misplaced or stolen. The reports contain identifying information of over 2,000 patients, including names, social security numbers, and medical diagnoses. Dorn VAMC officials alerted those affected and, as they did following the laptop's disappearance, offered each of them one year of free credit monitoring. The boxes have not been recovered.

While the *Beck* litigation was pending, Beverly Watson[2] brought a putative class-action lawsuit on behalf of the over 2,000 individuals whose pathology reports had gone missing. Watson sought money damages and declaratory and injunctive relief, alleging the same harm as did the *Beck* plaintiffs. The Defendants moved to dismiss the complaint for lack of subject-matter jurisdiction and for failure to state a claim.

The district court granted the Defendants' motion to dismiss for lack of subject-matter jurisdiction, relying on *Clapper* to hold that Watson lacked Article III standing under the Privacy Act because she "ha[d] not alleged that there ha[d] been any actual or attempted misuse of her personal information," thus rendering her allegation that her information "will eventually be misused as a result of the disappearance of the boxes . . . speculative." J.A. 1091.

According to the district court, for Watson to suffer the injury she feared, the court would have to assume that: (1) the boxes were stolen by someone bent on misusing the

[2] Ms. Watson is also a named plaintiff in *Beck*.

personal information in the pathology reports; (2) the thief would select Watson's report from the over 3,600 reports in the missing boxes; (3) the thief would then attempt to use or sell to others Watson's personal information; and (4) the thief or purchaser of Watson's information would successfully use the information in the report to steal Watson's identity. This "attenuated chain of possibilities" did not satisfy Watson's burden to show that her threatened injury was "certainly impending." J.A. 1092. As it did in *Beck*, the district court rejected Watson's allegations that any costs incurred to fend off future identity theft constituted an injury-in-fact.

Turning to Watson's claim for injunctive relief under the APA, the district court concluded that her allegations, based on Dorn VAMC's "historic inability or unwillingness to protect Plaintiff's personal information" were insufficient to show that, absent injunctive relief, she would be "in real and immediate danger of sustaining a direct injury as a result of some official conduct." J.A. 1096.

All Plaintiffs appeal the district court's ruling as to Article III standing.[3] The *Beck* plaintiffs also appeal the district court's alternative ruling that the Defendants are entitled to summary judgment on the Privacy Act and APA claims. Because we find that the Plaintiffs do not have Article III standing, we do not address the merits.

[3] We granted an unopposed motion to consolidate the cases.

II.

We review de novo the district court's decision to dismiss for lack of standing. *24th Senatorial Dist. Republican Comm. v. Alcorn*, 820 F.3d 624, 628 (4th Cir. 2016).

Article III of the U.S. Constitution limits the jurisdiction of federal courts to "Cases" and "Controversies." U.S. Const. art. III, § 2. "One element of the case-or-controversy requirement is that plaintiffs must establish that they have standing to sue." *Clapper*, 133 S. Ct. at 1146 (internal citations and quotation marks omitted). To invoke federal jurisdiction, a plaintiff bears the burden of establishing the three "irreducible minimum requirements" of Article III standing:

> (1) an injury-in-fact (i.e., a concrete and particularized invasion of a legally protected interest); (2) causation (i.e., a fairly traceable connection between the alleged injury in fact and the alleged conduct of the defendant); and (3) redressability (i.e., it is likely and not merely speculative that the plaintiff's injury will be remedied by the relief plaintiff seeks in bringing suit).

David v. Alphin, 704 F.3d 327, 333 (4th Cir. 2013) (internal alterations and quotation marks omitted).

In a class action, we analyze standing based on the allegations of personal injury made by the named plaintiffs. *See Doe v. Obama*, 631 F.3d 157, 160 (4th Cir. 2011) (citing *Warth v. Seldin*, 422 U.S. 490, 501 (1975)). "Without a sufficient allegation of harm to the named plaintiff in particular, plaintiffs cannot meet their burden of establishing standing." *Id.*

A defendant may challenge subject-matter jurisdiction in one of two ways: facially or factually. *See Kerns v. United States*, 585 F.3d 187, 192 (4th Cir. 2009). In a facial

challenge, the defendant contends "that a complaint simply fails to allege facts upon which subject matter jurisdiction can be based." *Id.* (quoting *Adams v. Bain*, 697 F.2d 1213, 1219 (4th Cir. 1982)). Accordingly, the plaintiff is "afforded the same procedural protection as she would receive under a Rule 12(b)(6) consideration," wherein "the facts alleged in the complaint are taken as true," and the defendant's challenge "must be denied if the complaint alleges sufficient facts to invoke subject matter jurisdiction." *Id.*

In a factual challenge, the defendant argues "that the jurisdictional allegations of the complaint [are] not true," providing the trial court the discretion to "go beyond the allegations of the complaint and in an evidentiary hearing determine if there are facts to support the jurisdictional allegations." *Id.* (first alteration in original) (quoting *Adams*, 697 F.2d at 1219). In this posture, "the presumption of truthfulness normally accorded a complaint's allegations does not apply." *Id.*

Critically, the procedural posture of the case dictates the plaintiff's burden as to standing. *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 561 (1992) ("[E]ach 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."). Here, the district court dismissed *Watson* on the pleadings and *Beck* at summary judgment.

"At the pleading stage, general factual allegations of injury resulting from the defendant's conduct may suffice, for on a motion to dismiss we presume that general allegations embrace those specific facts that are necessary to support the claim." *Id.* (internal citations omitted). As such, we accept as true Watson's allegations for which

there is sufficient "factual matter" to render them "plausible on [their] face." *See Ashcroft v. Iqbal*, 566 U.S. 662, 678 (2009) (internal citations omitted). We do not, however, apply the same presumption of truth to "conclusory statements" and "legal conclusions" contained in Watson's complaint. *See id.*; *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555–56 (2007).

By contrast, having developed through discovery a summary judgment record, the *Beck* plaintiffs are not entitled to "rest on such mere allegations, but must set forth by affidavit or other evidence specific facts, which for purposes of the summary judgment motion will be taken to be true." *Lujan*, 504 U.S. at 561 (citing Fed. R. Civ. P. 56) (internal quotations omitted).

III.

A.

We focus our inquiry on the first element of Article III standing: injury-in-fact. "To establish injury in fact, a plaintiff must show that he or she suffered 'an invasion of a legally protected interest' that is 'concrete and particularized' and 'actual or imminent, not conjectural or hypothetical.'" *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1548 (2016) (quoting *Lujan*, 504 U.S. at 560).[4] And while it is true "that threatened rather than actual

[4] In *Spokeo*, the Supreme Court suggested that some violations of the Fair Credit Reporting Act ("FCRA"), though "intangible" harms, may still be sufficiently "concrete" to establish an Article III injury-in-fact. 136 S. Ct. at 1549–50. In *Spokeo*'s aftermath, some plaintiffs have attempted to establish Article III standing by alleging that the violation of a privacy statute, *in and of itself*, is sufficiently "concrete" to establish an (Continued)

injury can satisfy Article III standing requirements," *Friends of the Earth, Inc. v. Gaston Copper Recycling Corp.*, 204 F.3d 149, 160 (4th Cir. 2000) (en banc), not all threatened injuries constitute an injury-in-fact. Rather, as the Supreme Court has "emphasized repeatedly," an injury-in-fact "must be concrete in both a qualitative and temporal sense." *Whitmore v. Arkansas*, 495 U.S. 149, 155 (1990). "The complainant must allege an injury to himself that is distinct and palpable, as opposed to merely abstract." *Id.* (internal citations and quotations omitted). "Although 'imminence' is concededly a somewhat elastic concept, it cannot be stretched beyond its purpose, which is to ensure that the alleged injury is not too speculative for Article III purposes." *Lujan*, 504 U.S. at 564–65, n. 2.

The Court recently explored the "threatened injury" theory of Article III standing in *Clapper v. Amnesty International USA*. That case involved a constitutional challenge to section 1881a of the Foreign Intelligence Surveillance Act of 1978 ("FISA"), which, "upon the issuance of an order from the Foreign Intelligence Surveillance Court," authorizes "for a period of up to 1 year" the Attorney General and the Director of

---

"injury-in-fact," to varying result. *Compare In re Horizon Healthcare Servs. Inc. Data Breach Litig.*, No. 15-2309, 2017 WL 242554, at *11 (3d Cir. Jan. 20, 2017) ("[T]he unauthorized dissemination of . . . private information—the very injury that FCRA is intended to prevent . . . [is] a *de facto* injury that satisfies the concreteness requirement for Article III standing.") *with Gubala v. Time Warner Cable, Inc.*, No. 16-2613, 2017 WL 243343, at *4 (7th Cir. Jan. 20, 2017) (plaintiff's failure to allege or provide evidence of any concrete injury inflicted or likely to be inflicted on the plaintiff as a consequence of Time Warner's continued retention of his personal information in violation of the Cable Communications Policy Act insufficient to confer Article III standing). *Spokeo* is not controlling here, as the Plaintiffs do not allege that Dorn VAMC's violations of the Privacy Act alone constitute an Article III injury-in-fact.

National Intelligence to target for surveillance "persons reasonably believed to be located outside the United States to acquire foreign intelligence information." 133 S. Ct. at 1144 (quoting 50 U.S.C. § 1881a).

The respondents—attorneys and human-rights, labor, legal, and media organizations whose work required them to communicate via telephone and e-mail with individuals located abroad-—sought a declaration that the provision was facially unconstitutional and a permanent injunction against its use. *Id.* at 1146. The respondents alleged two injuries: (1) that § 1881a curtailed their ability to "locate witnesses, cultivate sources, obtain information, and communicate confidential information," and (2) that they had implemented "costly and burdensome measures," including traveling abroad to have in-person conversations, to protect the confidentiality of their sensitive communications from FISA surveillance. *Id.* at 1145–46.

The district court ruled that the respondents lacked standing. *Id.* at 1146. On appeal, the Second Circuit reversed, holding that the "objectively reasonable likelihood" that the respondents' communications would be intercepted at some future time and their allegation that they suffered economic and professional harm as a result were sufficient to confer standing. *Id.*

The Supreme Court rejected the Second Circuit's use of an "objectively reasonable likelihood" standard for Article III standing as inconsistent with the Court's long-established requirement that "threatened injury must be certainly impending to constitute injury in fact." *Id.* at 1147–48 (listing cases). Addressing first the respondents' allegation that the Government would target their private communications,

the Court catalogued the series of hypothetical events that would have to occur to establish an "imminent" injury-in-fact: namely, the speculative possibility that the Government, pursuant to § 1881a's "many safeguards," would successfully target and intercept the communications of those foreigners with whom the respondents worked. *Id.* at 1148–50. The respondents' theory of standing, premised on this "highly attenuated chain of possibilities" could not "satisfy the requirement that threatened injury must be certainly impending." *Id.* at 1148.

The respondents' second theory of injury, premised on the "costly and burdensome" measures they had undertaken to protect the confidentiality of their communications, also failed to confer standing. *Id.* at 1150–51. The Court reasoned that the respondents' attempts to minimize e-mail and phone conversations, to speak "in generalities rather than specifics," and to travel abroad to have in-person conversations, were all costs "incurred in response to a speculative threat." *Id.* at 1151. The Court declined to "water[] down the fundamental requirements of Article III" by allowing respondents to "manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending." *Id.*

Clapper's discussion of when a threatened injury constitutes an Article III injury-in-fact is controlling here. Before explaining why, we address the Plaintiffs' contention that the district court misread *Clapper* to require a new, heightened burden for proving an Article III injury-in-fact. To the contrary, *Clapper*'s iteration of the well-established tenet that a threatened injury must be "certainly impending" to constitute an injury-in-fact is hardly novel. *E.g.*, *DaimlerChrysler Corp. v. Cuno*, 547 U.S. 332, 345 (2006) (an

asserted injury is "imminent" when it is "certainly impending"); *Lujan*, 504 U.S. at 564–65, n.2 (same); *Whitmore*, 495 U.S. at 158 ("A threatened injury must be 'certainly impending' to constitute injury in fact.").

We also reject the Plaintiffs' claim that "emotional upset" and "fear [of] identity theft and financial fraud" resulting from the data breaches are "adverse effects" sufficient to confer Article III standing. Appellants' Br. at 22 (citing 5 U.S.C. § 552a(e)(10)). That assertion reflects a misunderstanding of the Privacy Act and is an overextension of *Doe v. Chao*, 540 U.S. 614 (2004).

The sole issue in *Chao* was whether a Privacy Act plaintiff must prove actual damages to qualify for the minimum statutory award of $1,000. 540 U.S. at 616. There, a black-lung claimant brought suit under the Privacy Act against the Department of Labor for improperly disclosing his social security number. *Id.* at 617. This court held that the Department was entitled to summary judgment, concluding that the claimant had failed to raise a triable issue of fact about actual damages because he had submitted no corroboration for his claim of emotional distress. *Id.* The Supreme Court affirmed, reasoning that "a straightforward textual analysis" of the Privacy Act required a plaintiff to prove actual damages from an intentional or willful violation of the Act to qualify for the award. *Id.* at 620.

As the Court explained in *Chao*, "the reference in [the Privacy Act] to 'adverse effect' [is] a term of art identifying a potential plaintiff who *satisfies the injury-in-fact and causation requirements of Article III standing*." 540 U.S. at 624 (emphasis added). We decline to interpret dicta in *Chao* discussing the plaintiff's "conclusory allegations"

that he was "torn . . . all to pieces" by the unauthorized disclosure of his social security number as support for the proposition that bare assertions of emotional injury are sufficient to confer Article III standing. *Id.* at 617, 624–25. This court is "bound by holdings" of the Supreme Court, not its "unwritten assumptions." *Fernandez v. Keisler*, 502 F.3d 337, 343–44, n.2 (4th Cir. 2007).

Accordingly, with *Clapper*'s tenets firmly in tow, we address the two grounds for Article III standing pressed by the Plaintiffs for their Privacy Act claims: (1) the increased risk of future identity theft, and (2) the costs of protecting against the same.

Increased Risk of Future Identity Theft

Our sister circuits are divided on whether a plaintiff may establish an Article III injury-in-fact based on an increased risk of future identity theft. The Sixth, Seventh, and Ninth Circuits have all recognized, at the pleading stage, that plaintiffs can establish an injury-in-fact based on this threatened injury. *See Galaria v. Nationwide Mut. Ins. Co.*, No. 15-3386, 2016 WL 4728027, at *3 (6th Cir. Sept. 12, 2016) (plaintiff-customers' increased risk of future identity theft theory established injury-in-fact after hackers breached Nationwide Mutual Insurance Company's computer network and stole their sensitive personal information, because "[t]here is no need for speculation where Plaintiffs allege that their data has already been stolen and is now in the hands of ill-intentioned criminals"); *Remijas v. Neiman Marcus Grp., LLC*, 794 F.3d 688, 692, 694–95 (7th Cir. 2015) (plaintiff-customers' increased risk of future fraudulent charges and identity theft theory established "certainly impending" injury-in-fact and "substantial risk of harm" after hackers attacked Neiman Marcus with malware to steal credit card

numbers, because "[p]resumably, the purpose of the hack is, sooner or later, to make fraudulent charges or assume those consumers' identities"); *Krottner v. Starbucks Corp.*, 628 F.3d 1139, 1142–43 (9th Cir. 2010) (plaintiff-employees' increased risk of future identity theft theory a "credible threat of harm" for Article III purposes after theft of a laptop containing the unencrypted names, addresses, and social security numbers of 97,000 Starbucks employees); *Pisciotta v. Old Nat'l Bancorp*, 499 F.3d 629, 632–34 (7th Cir. 2007) (banking services applicants' increased risk of harm theory satisfied Article III injury-in-fact requirement after "sophisticated, intentional and malicious" security breach of bank website compromised their information).

By contrast, the First and Third Circuits have rejected such allegations. *See Katz v. Pershing, LLC*, 672 F.3d 64, 80 (1st Cir. 2012) (brokerage account-holder's increased risk of unauthorized access and identity theft theory insufficient to constitute "actual or impending injury" after defendant failed to properly maintain an electronic platform containing her account information, because plaintiff failed to "identify any incident in which her data has ever been accessed by an unauthorized person"); *Reilly v. Ceridian Corp.*, 664 F.3d 38, 40, 44 (3d Cir. 2011) (plaintiff-employees' increased risk of identity theft theory too hypothetical and speculative to establish "certainly impending" injury-in-fact after unknown hacker penetrated payroll system firewall, because it was "not known whether the hacker read, copied, or understood" the system's information and no evidence suggested past or future misuse of employee data or that the "intrusion was intentional or malicious").

The Plaintiffs say that our sister circuits' decisions in *Krottner*, *Pisciotta*, and *Remijas* support their allegations of standing based on threatened injury of future identity theft.[5] To the contrary, these cases demonstrate why the Plaintiffs' theory is too speculative to constitute an injury-in-fact.

Underlying the cases are common allegations that sufficed to push the threatened injury of future identity theft beyond the speculative to the sufficiently imminent. In *Galaria*, *Remijas*, and *Pisciotta*, for example, the data thief intentionally targeted the personal information compromised in the data breaches. *Galaria*, 2016 WL 4728027, at *1 ("[H]ackers broke into Nationwide's computer network and stole the personal information of Plaintiffs and 1.1 million others."); *Remijas*, 794 F.3d at 694 ("Why else would hackers break into a store's database and steal consumers' private information?"); *Pisciotta*, 499 F.3d at 632 ("scope and manner" of intrusion into banking website's hosting facility was "sophisticated, intentional and malicious"). And, in *Remijas* and *Krottner*, at least one named plaintiff alleged misuse or access of that personal information by the thief. *Remijas*, 794 F.3d at 690 (9,200 of the 350,000 credit cards

[5] The Plaintiffs also rely on the environmental law cases of *Friends of the Earth, Inc. v Laidlaw Environmental Services*, 528 U.S. 167 (2000) and *Friends of the Earth, Inc. v. Gaston Copper Recycling Corp.*, 629 F.3d 387, 394 (4th Cir. 2011) (en banc) to support their view that a "reasonable concern" of harm is sufficient to confer Article III standing. Appellants' Br. at 23. "In the environmental litigation context, [however], the standing requirements are not onerous." *Am. Canoe Ass'n v. Murphy Farms, Inc.*, 326 F.3d 505, 517 (4th Cir. 2003). This is so because "[t]he extinction of a species, the destruction of a wilderness habitat, or the fouling of air and water are harms that are frequently difficult or impossible to remedy" by monetary compensation. *Cent. Delta Water Agency v. United States*, 306 F.3d 938, 950 (9th Cir. 2002). By contrast, in data-breach cases, "there is no reason to believe that monetary compensation will not return plaintiffs to their original position completely." *Reilly*, 664 F.3d at 45.

potentially exposed to malware "were known to have been used fraudulently"); *Krottner*, 628 F.3d at 1141 (named plaintiff alleged that, two months after theft of laptop containing his social security number, someone attempted to open a new account using his social security number).

Here, the Plaintiffs make no such claims. This in turn renders their contention of an enhanced risk of future identity theft too speculative. On this point, the data breaches in *Beck* and *Watson* occurred in February 2013 and July 2014, respectively. Yet, even after extensive discovery, the *Beck* plaintiffs have uncovered no evidence that the information contained on the stolen laptop has been accessed or misused or that they have suffered identity theft, nor, for that matter, that the thief stole the laptop with the intent to steal their private information.[6] Watson's complaint suffers from the same deficiency with regard to the four missing boxes of pathology reports. Moreover, "as the breaches fade further into the past," the Plaintiffs' threatened injuries become more and more speculative. *See Chambliss v. Carefirst, Inc.*, No. 15-2288, 2016 WL 3055299, at *4 (D. Md. May 27, 2016); *In re Zappos.com*, 108 F. Supp. 3d 949, 958 (D. Nev. 2015) ("[T]he passage of time without a single report from Plaintiffs that they in fact suffered the harm they fear must mean something.").

The Plaintiffs counter that there is "no need to speculate" here because they have alleged-and in the *Beck* case the VA's investigation concluded—that the laptop and

[6] Ms. Gajadhar, a named *Beck* plaintiff, testified to three unauthorized credit card charges, later reimbursed by her bank. However, she failed to attribute those charges to the 2013 laptop theft. Nor could she, given that the data on the stolen laptop did not contain any credit card or bank account information.

pathology reports had been stolen. *See* J.A. 824. We of course accept this allegation as true. But the mere theft of these items, without more, cannot confer Article III standing. *See Randolph v. ING Life Ins. & Annuity Co.*, 486 F. Supp. 2d 1, 7–8 (D.D.C. 2007) (deeming as speculative plaintiffs' allegations "that at some unspecified point in the indefinite future they will be the victims of identity theft" where, although plaintiffs clearly alleged their information was stolen by a burglar, they did "not allege that the burglar who stole the laptop did so in order to access their [i]nformation, or that their [i]nformation ha[d] actually been accessed since the laptop was stolen").

Indeed, for the Plaintiffs to suffer the harm of identity theft that they fear, we must engage with the same "attenuated chain of possibilities" rejected by the Court in *Clapper*. 133 S. Ct. at 1147–48. In both cases, we must assume that the thief targeted the stolen items for the personal information they contained. And in both cases, the thieves must then select, from thousands of others, the personal information of the named plaintiffs and attempt successfully to use that information to steal their identities. This "attenuated chain" cannot confer standing.

The Plaintiffs insist that the district court required them to show "concrete evidence that [their] personal information had *already* been misused," thus forcing someone in their position "'to wait for the threatened harm to materialize in order to sue.'" Appellants' Br. at 28 (quoting *Remijas*, 794 F.3d at 694). We disagree. The district court sought only to hold the Plaintiffs to their respective burdens to either "plausibly plead" factual allegations or "set forth particular evidence" sufficient to show

that the threatened harm of future identity theft was "certainly impending." This they failed to do.

Nonetheless, our inquiry on standing is not at an end, for we may also find standing based on a "substantial risk" that the harm will occur, which in turn may prompt a party to reasonably incur costs to mitigate or avoid that harm. *Clapper*, 133 S. Ct. at 1150 n.5. But here too the Plaintiffs fall short of their burden.

The Plaintiffs allege that: (1) 33% of health-related data breaches result in identity theft; (2) the Defendants expend millions of dollars trying to avoid and mitigate those risks; and (3) by offering the Plaintiffs free credit monitoring, the VA effectively conceded that the theft of the laptop and pathology reports constituted a "reasonable risk of harm to those victimized" by the data breaches. Appellants' Br. at 31 (citing 38 C.F.R. § 75.116 (authorizing Secretary of Veterans Affairs to offer credit protection services for mitigative purposes upon finding that "reasonable risk exists" for "potential misuse of sensitive personal information" compromised in a data breach)).

These allegations are insufficient to establish a "substantial risk" of harm.[7] Even if we credit the Plaintiffs' allegation that 33% of those affected by Dorn VAMC data breaches will become victims of identity theft, it follows that over 66% of veterans affected will suffer no harm. This statistic falls far short of establishing a "substantial

[7] The Plaintiffs' claim that data-breach victims are 9.5 times more likely than the average person to suffer identity theft does not alter our conclusion. As the Defendants point out, this general statistic says nothing about the risk arising out of any particular incident, nor does it address the particular facts of this case.

risk" of harm. *E.g.*, *Khan v. Children's Nat'l Health Sys.*, 188 F. Supp. 3d 524, 533 (D. Md. 2016) ("general allegations . . . that data breach victims are 9.5 times more likely to suffer identity theft and that 19 percent of data breach victims become victims of identity theft" insufficient to establish "substantial risk" of harm); *In re Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig.*, 45 F. Supp. 3d 14, 26 (D.D.C. 2014) (no "substantial risk" of harm where "[b]y Plaintiff's own calculations, then, injury is likely not impending for over 80% of victims").

The Plaintiffs' other allegations fare no better. Contrary to some of our sister circuits, we decline to infer a substantial risk of harm of future identity theft from an organization's offer to provide free credit monitoring services to affected individuals.[8] To adopt such a presumption would surely discourage organizations from offering these services to data-breach victims, lest their extension of goodwill render them subject to suit.

Further, we read *Clapper*'s rejection of the Second Circuit's attempt to import an "objectively reasonable likelihood" standard into Article III standing to express the common-sense notion that a threatened event can be "reasonabl[y] likel[y]" to occur but still be insufficiently "imminent" to constitute an injury-in-fact. *See* 133 S. Ct. at 1147–48. Accordingly, neither the VA's finding that a "reasonable risk exists" for the

[8] *See, e.g.*, *Galaria*, 2016 WL 4728027, at *3 ("Indeed, Nationwide seems to recognize the severity of the risk, given its offer to provide credit-monitoring and identity-theft protection for a full year."); *Remijas*, 794 F.3d at 694 ("It is telling . . . that Neiman Marcus offered one year of credit monitoring and identity-theft protection to all [potentially affected] customers. It is unlikely that it did so because the risk is so ephemeral that it can safely be disregarded.").

"potential misuse of sensitive personal information" following the data breaches, nor its decision to pay for credit monitoring to guard against it is enough to show that the Defendants subjected the Plaintiffs to a "substantial risk" of harm.

Cost of Mitigative Measures

Next, we turn to the Plaintiffs' allegation that they have suffered an injury-in-fact because they have incurred or will in the future incur the cost of measures to guard against identity theft, including the costs of credit monitoring services. All Plaintiffs allege that they wish to enroll in, are enrolled in, or have purchased credit monitoring services. They also say that, as a consequence of the breaches, they have incurred the burden of monitoring their financial and credit information. Even accepting these allegations as true, they do not constitute an injury-in-fact.

As was the case in *Clapper*, the Plaintiffs here seek "to bring this action based on costs they incurred in response to a speculative threat," i.e. their fear of future identity theft based on the breaches at Dorn VAMC. *Id.* at 1151. But this allegation is merely "a repackaged version of [Plaintiffs'] first failed theory of standing." *Id.* Simply put, these self-imposed harms cannot confer standing. *See, e.g.*, *Remijas*, 794 F.3d at 694 ("Mitigation expenses do not qualify as actual injuries where the harm is not imminent."); *Reilly*, 664 F.3d at 46 ("[P]rophylactically spen[ding] money to ease fears of [speculative] future third-party criminality . . . is not sufficient to confer standing.").

B.

Finally, we address the Plaintiffs' request for broad injunctive relief under the APA.[9] To establish their standing to seek such relief, the Plaintiffs borrow from the statutory language of the Privacy Act, contending that the "substantial harm," "embarrassment," "inconvenience," and "unfairness" caused them by the Defendants satisfies their Article III burden because they have been "adversely affected" within the meaning of the APA. *See* 5 U.S.C. §§ 552a(e)(10), 702.

These citations to the Privacy Act's language are inapposite: The APA's "adversely affected" language does not relieve the Plaintiffs of their burden to prove Article III standing. *See Match-E-Be-Nash-She-Wish Band of Pottawatomi Indians v. Patchak*, 132 S. Ct. 2199, 2210 ("[A] person suing under the APA must satisfy not only Article III's standing requirements," but also the prudential "zone of interests" test) (internal quotations omitted). Rather, we agree with the district court that the Plaintiffs do not have standing to seek injunctive relief under the APA because allegations of Dorn VAMC's past Privacy Act violations are insufficient to establish an ongoing case or controversy. *See City of Los Angeles v. Lyons*, 461 U.S. 95, 101–02 (1974) ("[P]ast exposure to illegal conduct does not in itself show a present case or controversy regarding injunctive relief.") (internal quotations omitted).

A plaintiff who seeks . . . to enjoin a future action must demonstrate that he 'is immediately in danger of sustaining some direct injury' as the result of the challenged

[9] We assume without deciding that injunctive relief is available in these circumstances.

official conduct." *Lebron v. Rumsfeld*, 670 F.3d 540, 560 (4th Cir. 2012) (quoting *Lyons*, 461 U.S. at 102)). And this "threat of injury must be both 'real and immediate,' not 'conjectural' or 'hypothetical.'" *Id.* The Plaintiffs say that Dorn VAMC's "inadequate actions and inactions will repeatedly harm every veteran regardless of anything those individuals can do" where Dorn VAMC "has *never* been in compliance with the Privacy Act," and where there is "no factual basis to believe VA will ever achieve compliance with safeguards requirements left to its own devices." Appellants' Br. at 38–39.

We acknowledge that the named plaintiffs have been victimized by "at least two admitted VA data breaches," and that Ms. Watson's information was compromised in both the 2013 laptop theft and the 2014 pathology reports theft. Appellants' Br. at 39. But "[a]bsent a sufficient likelihood that [Plaintiffs] will again be wronged in a similar way," *Lyons*, 461 U.S. at 111, these past events, disconcerting as they may be, are not sufficient to confer standing to seek injunctive relief. *See Lebron*, 670 F.3d at 560–61 (affirming dismissal of former enemy combatant detainee's request for injunction against future designation as an enemy combatant because the mere "possibility" of re-designation was insufficient to allege a "real" and "immediate" threat). The most that can be reasonably inferred from the Plaintiffs' allegations regarding the likelihood of another data breach at Dorn VAMC is that the Plaintiffs *could* be victimized by a future data breach. That alone is not enough.

IV.

For the reasons given, the judgments of the district court are

AFFIRMED.