[PUBLISH]

IN THE UNITED STATES COURT OF APPEALS

FOR THE ELEVENTH CIRCUIT

No. 18-14959

D.C. Docket No. 8:18-cv-01606-WFJ-SPF

I TAN TSAO,
individually and on behalf of all others similarly situated,

Plaintiff-Appellant,

versus

CAPTIVA MVP RESTAURANT PARTNERS, LLC,
A Florida Limited Liability Company doing business as PDQ,

Defendant-Appellee.

Appeal from the United States District Court
for the Middle District of Florida

(February 4, 2021)

Before JORDAN, TJOFLAT, and TRAXLER,[*] Circuit Judges.

TJOFLAT, Circuit Judge:

[*] The Honorable William B. Traxler, Senior United States Circuit Judge for the Fourth Circuit, sitting by designation.

I Tan Tsao seeks to bring a number of claims against PDQ—a restaurant he patroned—following a data breach that exposed PDQ customers' personal financial information. Tsao's appeal presents two questions. First, did Tsao have standing to sue based on the theory that he and a proposed class of PDQ customers are now exposed to a substantial risk of future identity theft, even though neither Tsao nor the class members have suffered any misuse of their information? Second, and alternatively, were Tsao's efforts to mitigate the risk of future identity theft a present, concrete injury sufficient to confer standing? For both questions, we conclude the answer is no, and we accordingly affirm the District Court's order dismissing the case without prejudice.

I.

PDQ is a group of fast casual restaurants that sells chicken tenders, chicken nuggets, salads, and sandwiches. Like most restaurants today, PDQ accepts payment through a point of sale system where customers can insert credit or debit cards to pay for their meal. When customers pay with a debit or credit card, PDQ collects some data from the cards, including the cardholder's name, the account number, the card's expiration date, the card verification value code ("CVV"), and PIN data for debit cards. PDQ then stores this data in its point of sale system and transmits the information to a third party for processing and for completion of the payment.

Beginning on May 19, 2017, a hacker exploited PDQ's point of sale system and gained access to customers' personal data—the credit and debit card information—through an outside vendor's remote connection tool. PDQ later became aware of the breach, and on June 22, 2018, it posted a notice to customers that it had "been the target of a cyber-attack." The notice stated that "[a]ll PDQ locations in operation" between May 19, 2017, and April 20, 2018, were affected by the attack, and the notice listed the customers' personal information that "may have been accessed": cardholder names, credit card numbers, card expiration dates, and CVVs. Because of the nature of the breach, PDQ stated that it "was not possible to determine the identity or exact number of credit card numbers or names that were accessed or acquired during" the cyber-attack. The notice repeatedly made clear that PDQ customers' information "may" have been accessed.

In October 2017—during the data breach period—plaintiff Tsao made at least two food purchases at a PDQ restaurant in Pinellas, Florida, using two different cards. On October 8, he paid with a Wells Fargo Home Rebate card, and on October 31, he paid with a Chase Sapphire Reserve card. Both of these cards offer Tsao the ability to accrue points or rebates by making certain types of purchases—gas, dining, groceries, and travel, just to name a few. The Chase card also requires Tsao to pay an annual fee of $450.00. Because Tsao made purchases at PDQ during the breach period, the credit card data from these cards may have

been accessed by hackers. So, when Tsao learned of the possible breach in 2018, he contacted both Chase and Wells Fargo and cancelled his cards.

Less than two weeks after PDQ's announcement of the cyber-attack, Tsao filed a class action complaint (the "Complaint") in the Middle District of Florida on behalf of a nationwide class, or alternatively, a separate Florida class. The Complaint lists a variety of injuries that PDQ customers allegedly suffered as a result of the cyber-attack, including "theft of their personal financial information," "unauthorized charges on their debit and credit card accounts," and "ascertainable losses in the form of the loss of cash back or other benefits." Tsao asserts that he and the class members "have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and identity fraud, requiring them to take the time which they otherwise would have dedicated to other life demands such as work and effort to mitigate the actual and potential impact of the Data Breach on their lives." The Complaint also includes some general information from the Federal Trade Commission and Government Accountability Office about the risks associated with cyber-attacks and lists a few noteworthy data breaches involving the restaurant industry.

Based on these alleged injuries, the Complaint claims that PDQ (1) breached an implied contract by failing to safeguard customers' credit card data (Count I); (2) was negligent in failing to provide adequate security for the credit card data

(Count II); (3) was *per se* negligent because PDQ violated Section 5 of the Federal Trade Commission Act (15 U.S.C. § 45), which prohibits unfair practices that affect commerce (Count III); (4) was unjustly enriched when it received payments from the customers but failed to provide those customers with adequate data security (Count IV); and (5) violated the Florida Unfair and Deceptive Trade Practices Act by failing to, among other things, maintain "adequate . . . data security practices" (Count VI). The Complaint additionally seeks a declaratory judgment stating that "PDQ's existing data security measures do not comply with its contractual obligations and duties of care" and that PDQ, in order to comply with those obligations, is required to implement and maintain a variety of security measures (Count V).

PDQ moved to dismiss the Complaint on August 28, 2018. PDQ argued that the Complaint failed to state a claim under Federal Rules of Civil Procedure 12(b)(1), (b)(6), and (b)(7) "for failure to satisfy Article III standing, to state a claim upon which relief can be granted, and/or for failure to join indispensable parties." On the standing issue, PDQ emphasized that, although customer data may have been "compromised" or "exposed" during the cyber-attack, Tsao failed to identify "a single incident involving an actual misuse of the credit card information, much less any misuse . . . causing any of the customers any <u>actual injury</u>" (emphasis in original). Instead, PDQ argued, Tsao's claims were

"premised on a fear that his credit card information may be misused at some point in the future," and since he cancelled his cards before any misuse occurred, he was foreclosed from alleging damages. And even if Tsao did incur some out-of-pocket expenses to mitigate the risk of misuse, PDQ claimed that such "manufacture[d] standing" was not enough to satisfy Article III.

Tsao's response to the motion to dismiss focused heavily on three types of injuries he allegedly suffered in his efforts to mitigate the perceived risk of future identity theft: lost cash back or reward points, lost time spent addressing the problems caused by the cyber-attack, and restricted card access resulting from his credit card cancellations. On the first point—the loss of cash back or reward points—Tsao argued that, because he cancelled his Chase and Wells Fargo cards in anticipation of possible misuse, he temporarily "lost the opportunity to accrue" the rewards connected to those cards. And on the latter two points—lost time and restricted account access—Tsao asserted that he "expended time and effort" to cancel his cards and to deal with the impact of the cyberattack, and since he cancelled the cards, he lost access to his "preferred accounts." Importantly, however, Tsao did not point to any specific instances in which his—or any other class member's—identity was stolen, cards were fraudulently charged, or data was misused. Rather, the thrust of Tsao's response was that he had standing (1)

because he and the class were at an elevated risk of identity theft, or, alternatively, (2) because he took "proactive[]" steps to mitigate the risk of identity theft.

On November 1, 2018, the District Court dismissed Tsao's Complaint without prejudice for lack of standing. The Court noted that although Tsao claimed that his private data was "compromised" and "exposed" to criminals, not once did he allege "that his credit cards were used in any way by a thief or that his identity was stolen." Nor did Tsao identify "a single specific, concrete injury in fact that he or anyone else [] suffered as a result of any misuse of customer credit card information." These conclusory allegations of harm, the Court found, were speculative at best, and mere "[e]vidence of a data breach, without more, [was] insufficient to satisfy injury in fact under Article III standing."

This appeal followed. Tsao's briefing mostly retreads the arguments he made below—that he and the class are at an elevated risk of future identity theft and that he lost cash back and rewards point, time, and account access—in an effort to satisfy Article III's standing requirement. But after a careful review of the record and with the benefit of oral argument, we affirm the District Court's dismissal for lack of standing.

II.

Whether plaintiffs have standing to sue is a threshold jurisdictional question that we review de novo. *Debernardis v. IQ Formulations, LLC*, 942 F.3d 1076,

1083 (11th Cir. 2019). On a facial attack to a complaint for lack of standing, we take the allegations of the complaint as true. *McElmurray v. Consol. Gov't of Augusta-Richmond Cty.*, 501 F.3d 1244, 1251 (11th Cir. 2007).

III.

Tsao's arguments focus on two general theories of standing. First, he argues that he *could* suffer future injury from misuse of the personal information disclosed during the cyber-attack (though he has not yet), and this risk of misuse alone is enough to satisfy the standing requirement. Then, he argues that he has *already* suffered some "concrete, particularized" mitigation injuries—for example, lost time, lost rewards points, and loss of access to accounts—that are sufficient to confer standing. Below, we reject both of these theories of standing. But before we dive into Tsao's arguments, an overview of our standing case law is in order.

A.

Under Article III of the Constitution, the jurisdiction of a federal court is limited to "cases" and "controversies." *See Wilding v. DNC Servs. Corp.*, 941 F.3d 1116, 1124 (11th Cir. 2019). To satisfy the "case" or "controversy" requirement, a plaintiff in a matter must have standing to sue. *See Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1546–47 (2016). And for a plaintiff to have standing, it must have "(1) suffered an injury in fact, (2) that is fairly traceable to the challenged conduct of the defendant, and (3) that is likely to be redressed by a favorable judicial

decision." *Id.* at 1547 (citing *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 560–61, 112 S. Ct. 2130, 2136 (1992)). A plaintiff at the pleading stage, as the party invoking federal jurisdiction, bears the burden of establishing these elements by alleging facts that "plausibly" demonstrate each element. *Trichell v. Midland Credit Mgmt., Inc.*, 964 F.3d 990, 996 (11th Cir. 2020)

Of the three standing elements, Tsao's allegations implicate only injury. At the pleading stage, "general factual allegations of injury" are enough. *Lujan*, 504 U.S. at 561, 112 S. Ct. at 2137. But this does not mean that *any* allegations of injury can push a plaintiff across the standing threshold. Rather, a plaintiff must set forth general factual allegations that "plausibly and clearly allege a concrete injury," *Thole v. U. S. Bank N.A*, 140 S. Ct. 1615, 1621 (2020), and that injury must be "'actual or imminent, not conjectural or hypothetical,'" *Spokeo, Inc.*, 136 S. Ct. at 1548 (quoting *Lujan*, 504 U.S. at 560, 112 S. Ct. at 2136). "[M]ere conclusory statements[] do not suffice." *Ashcroft v. Iqbal*, 556 U.S. 662, 678, 129 S. Ct. 1937, 1949 (2009).

This standing framework raises two questions. First, what is a "concrete" injury? In *Spokeo*, the United States Supreme Court offered a straightforward definition: "A concrete injury must be *de facto*; that is, it must actually exist." *Spokeo, Inc.*, 136 S. Ct. at 1548 (quotations omitted). The Supreme Court noted that, when it uses the term "concrete," it intends to "convey the usual meaning of

the term—'real,' and not 'abstract.'" *Id.* (quoting Webster's Third New International Dictionary 472 (1971)). This Court has adhered to that definition, and we have noted that "[a] concrete injury need be only an '*identifiable* trifle.'" *Salcedo v. Hanna*, 936 F.3d 1162, 1167 (11th Cir. 2019) (quoting *United States v. Students Challenging Regul. Agency Proc's. (SCRAP)*, 412 U.S. 669, 689 n.14, 93 S. Ct. 2405, 2417 n.14 (1973)) (emphasis added).

Typically, tangible[1] injuries are "concrete." *See Trichell*, 964 F.3d at 997. Tangible injuries can include both straightforward economic injuries, *see Debernardis*, 942 F.3d at 1084, and more nebulous injuries, like lost time, *see Salcedo*, 936 F.3d at 1173, or the loss of a "fraction of a vote," *id.* at 1167 (quoting *SCRAP*, 412 U.S. at 689 n.14, 93 S. Ct. at 2417 n.14).

But although many types of injuries may qualify as "concrete," there is another restriction on standing: "Where a 'hypothetical future harm' is not 'certainly impending,' plaintiffs 'cannot manufacture standing merely by inflicting harm on themselves.'" *Muransky v. Godiva Chocolatier, Inc.*, 979 F.3d 917, 931 (11th Cir. 2020) (en banc) (quoting *Clapper v. Amnesty Int'l USA*, 568 U.S. 398,

[1] Intangible injuries, such as a mere statutory violation, will sometimes qualify as concrete, but that inquiry depends upon the context of the statutory violation. *See Trichell v. Midland Credit Mgmt., Inc.*, 964 F.3d 990, 997 (11th Cir. 2020). Although intangible injuries are not relevant here, we mention them briefly for the sake of completeness.

416, 133 S. Ct. 1138, 1151 (2013)). This raises the second question: When is an injury "actual or imminent" and not just "conjectural or hypothetical?"

In *Clapper*, the United States Supreme Court addressed whether a group of plaintiffs—people in the United States whose work required them to engage in sensitive international communications that may have been the target of surveillance under a federal statute—suffered an injury in fact because "there [wa]s an objectively reasonable likelihood that their communications w[ould] be acquired under [the statute] at some point in the future." *Clapper*, 568 U.S. at 401, 133 S. Ct. at 1143. The Supreme Court found no injury—and thus no standing—because the plaintiffs "merely speculate[d] and ma[de] assumptions about whether their communications with their foreign contacts w[ould] be acquired" under the statute. *Id.* at 411, 133 S. Ct. at 1148. Such speculation was not enough: "[T]hreatened injury must be *certainly impending* to constitute injury in fact, . . . [a]llegations of *possible* future injury are not sufficient." *Id.* at 409, 133 S. Ct. at 1147 (emphasis in original) (quotations omitted). While this standard does not require a plaintiff to show that it is "literally certain that the harms they identify will come about," it, at the very least, requires a showing that there is a "substantial risk" that the harm will occur. *Id.* at 414 n.5, 133 S. Ct. at 1150 n.5.

This Circuit recently discussed *Clapper*'s "high standard for the risk-of-harm analysis" in the context of speculative allegations of future identity theft.

Muransky, 979 F.3d at 927. In *Muransky*, customers of Godiva chocolate stores alleged violations of the Fair and Accurate Credit Transactions Act ("FACTA"), claiming that Godiva printed too many digits on credit card receipts and thus exposed customers to an elevated risk of identity theft. *Id.* at 922. The injuries alleged were merely "statutory in nature"—that is, the harm to plaintiffs was simply that FACTA had been violated. *Id.* As the litigation wore on, the parties began to negotiate a settlement, fueled largely by the United States Supreme Court's impending decision in *Spokeo v. Robins*, which would decide whether a statutory violation alone could confer standing. *Id.* With *Spokeo* still outstanding, the District Court certified the proposed class, approved a settlement between the parties, and directed notice of the settlement to the class members. *Id.* at 922–23.

But before the District Court could hold a fairness hearing on the class settlement, the Supreme Court issued its decision in *Spokeo*. *Id.* An objector to the Godiva settlement argued that the District Court was obliged to determine whether, in light of *Spokeo*, plaintiffs had standing to sue for a statutory violation, but the District Court ignored the issue and approved the settlement. *Id.* at 923.

This Court, sitting *en banc*, vacated the District Court's order approving the settlement and remanded with instructions to dismiss for lack of standing. *Id.* at 936. We reasoned, in relevant part, that Muransky's naked allegations that he and the class were exposed to an "elevated risk" of identity theft—but not that he and

the class were ever actually the victims of identity theft—were not enough to confer standing. *Id.* at 933. But in an attempt to end run around *Spokeo*, Muransky claimed that he suffered a direct injury in fact when he spent time "destroying or safeguarding" his receipts in an effort to mitigate his risk of future identity theft. *Id.* at 931. Citing *Clapper*, this Court flatly rejected Muransky's argument: "Where a 'hypothetical future harm' is not 'certainly impending,' plaintiffs 'cannot manufacture standing merely by inflicting harm on themselves.' [] Muransky is no different than the *Clapper* plaintiffs in this respect—his management-of-risk claim is bound up with his arguments about actual risk." *Id.* (citing *Clapper*, 568 U.S. at 416, 422, 133 S. Ct. at 1151, 1155).

From *Clapper* and *Muransky*, we can distill two legal principles relevant to Tsao's claims. First, a plaintiff alleging a threat of harm does not have Article III standing unless the hypothetical harm alleged is either "certainly impending" or there is a "substantial risk" of such harm.[2] *Clapper*, 568 U.S. at 409, 414 n.5, 133 S. Ct. at 1147, 1150 n.5; *Muransky*, 979 F.3d at 931. Second, if the hypothetical harm alleged is not "certainly impending," or if there is not a substantial risk of the harm, a plaintiff cannot conjure standing by inflicting some direct harm on itself to

[2] The Supreme Court indicated that both the "certainly impending" and "substantial risk" standards are applicable in future injury cases, albeit without resolving whether they are distinct. *See Susan B. Anthony List v. Driehaus*, 573 U.S. 149, 158, 134 S. Ct. 2334, 2341 (2014). As a result, we discuss both throughout this opinion.

mitigate a perceived risk. *Clapper*, 568 U.S. at 416, 422, 133 S. Ct. at 1151, 1155; *Muransky*, 979 F.3d at 931. With these two principles in mind, we turn to Tsao's claims.

B.

We begin with Tsao's theory that he has Article III standing because he faces a "substantial risk of identity theft, fraud, and other harm in the future as a result of the data breach." Although this Circuit has not addressed the issue head-on, a number of our sister circuits have, and they are divided. On the one hand, the Sixth, Seventh, Ninth, and D.C. Circuits have all recognized—at the pleading stage—that a plaintiff can establish injury-in-fact based on the increased risk of identity theft. *See Attias v. Carefirst, Inc.*, 865 F.3d 620, 629 (D.C. Cir. 2017); *Galaria v. Nationwide Mut. Ins. Co.*, 663 F. App'x 384, 387–89 (6th Cir. 2016); *Remijas v. Neiman Marcus Grp., LLC*, 794 F.3d 688, 692, 694–95 (7th Cir. 2015); *Krottner v. Starbucks Corp.*, 628 F.3d 1139, 1142–43 (9th Cir. 2010); *Pisciotta v. Old Nat'l Bancorp*, 499 F.3d 629, 633–34 (7th Cir. 2007). On the other hand, the Second, Third, Fourth, and Eighth Circuits have declined to find standing on that theory. *See Beck v. McDonald*, 848 F.3d 262, 273–76 (4th Cir.), *cert. denied sub nom. Beck v. Shulkin*, 137 S. Ct. 2307 (2017); *Whalen v. Michaels Stores, Inc.*, 689 F. App'x 89, 90–91 (2d Cir. 2017); *In re SuperValu, Inc.*, 870 F.3d 763, 770–72

(8th Cir. 2017); *Reilly v. Ceridian Corp.*, 664 F.3d 38, 42–44 (3d Cir. 2011).[3] Of course, we are not bound by any of these cases, but a brief overview of their reasoning is helpful.

Generally speaking, the cases conferring standing after a data breach based on an increased risk of theft or misuse included at least some allegations of actual misuse or actual access to personal data. In *Attias*, two plaintiffs alleged that they suffered identity theft when their anticipated tax refunds went missing. *Attias*, 865 F.3d at 626 n.2. In *Galaria*, plaintiffs alleged that their data was accessed and had "already been stolen" by "ill-intentioned criminals." *Galaria*, 663 F. App'x at 388. In *Remijas*, plaintiffs alleged that personal data had "already been stolen" and that "9,200 cards [] experienced fraudulent charges." *Remijas*, 794 F.3d at 692–94. And in *Krottner*, at least one plaintiff alleged that someone "attempted to open a bank account in his name." *Krottner*, 628 F.3d at 1142.

[3] It is worth noting that the First Circuit appears to have gone both ways on this issue. In *Anderson v. Hannaford Bros.*, 659 F.3d 151, 162–67 (1st Cir. 2011), the First Circuit declined to question whether victims of a data breach—who alleged 1,800 instances of credit-card fraud—had standing to sue. But when analyzing *Anderson* in a different data breach case, the First Circuit drew the distinction between instances where confidential data has *actually* been accessed and case where data *might* be accessed. *Katz v. Pershing, LLC*, 672 F.3d 64, 80 (1st Cir. 2012) The Court held that, in the latter scenario, the "theoretical possibility" of access to confidential data "simply does not rise to the level of a reasonably impending threat." *Id.* at 79. Since *Katz*, other Circuits have interpreted First Circuit law to preclude standing based on allegations of future identity theft unaccompanied by criminal activity involving the stolen information, *see Beck*, 848 F.3d at 273, as have district courts within the First Circuit, *see Hartigan v. Macy's, Inc.*, No. CV 20-10551-PBS, 2020 WL 6523124, at *3 (D. Mass. Nov. 5, 2020).

The outlier among the cases conferring standing is *Pisciotta*, 499 F.3d at 634. There, plaintiffs brought a class action against a bank after its website was hacked, alleging that the bank failed to adequately secure the personal information it solicited (including names, addresses, birthdates, and social security numbers) when consumers applied for banking services on its website. *Id.* at 631. The named plaintiffs did not allege any actual misuse or access to their data, but the Seventh Circuit found standing nonetheless: "[T]he injury-in-fact requirement can be satisfied by a threat of future harm or by an act which harms the plaintiff only by increasing the risk of future harm that the plaintiff would have otherwise faced, absent the defendant's actions." *Id.* at 634.

Though the Seventh Circuit's opinion appears to sweep broadly on its face, we are hesitant to read too closely into *Pisciotta* in light of two considerations. First, *Pisciotta* is a pre-*Clapper* decision, and thus it is unclear if the Seventh Circuit would have (or could have) reached the same conclusion with the benefit of the Supreme Court's opinion. Second, none of the Seventh Circuit data breach cases that followed *Pisciotta*—including *Remijas*, 794 F.3d at 693, *Lewert v. P.F. Chang's China Bistro, Inc.*, 819 F.3d 963 (7th Cir. 2016), and *Dieffenbach v. Barnes & Noble, Inc.*, 887 F.3d 826 (7th Cir. 2018)—even cite the case, suggesting that *Pisciotta* should not weigh too heavily in our analysis.

Other Circuits have declined to find standing on an "elevated risk of identity theft" theory where the plaintiffs failed to allege any actual misuse of class members' personal information. The Second Circuit, for example, distinguished a breach of credit-card-specific data from a breach of other forms of personal information in *Whalen v. Michaels Stores, Inc.*, 689 F. App'x at 90. In *Whalen*, Michaels Stores publicly announced a breach of card data, and Whalen filed suit alleging that her card—which was used at Michaels during the breach period—had been "physically presented for payment" at two locations in Ecuador, though no charges were actually incurred. *Id.* To show standing, Whalen pointed to the two attempts to use her cards in Ecuador, the "risk of future identity fraud," and the lost time and money she spent resolving the attempted fraudulent purchases. *Id.* But the Second Circuit held that Whalen failed to allege a concrete injury because (1) Whalen never paid, nor was asked to pay, for the attempted fraudulent charges in Ecuador; (2) she did not identify a threat of future fraud, as her stolen credit card had already been canceled and no other identifying information was stolen; and (3) the complaint did not allege that she expended any time or money to monitor her financial data. *Id.* at 90–91.

Similarly, in *Reilly v. Ceridian Corp.*—a pre-*Clapper* decision—a class of law firm employees brought a putative class action against a payroll processing firm (Ceridian) asserting various claims related to an increased risk of identity theft

and costs to monitor credit activity after Ceridian suffered a security breach. *See* 664 F.3d at 40. After the breach, Ceridian sent letters to the potential identity theft victims, informing them of the breach: "[S]ome of your personal information . . . may have been illegally accessed by an unauthorized hacker. . . . [T]he information accessed included your first name, last name, social security number and, in several cases, birth date and/or the bank account that is used for direct deposit." *Id.* (alterations in original). Although the plaintiffs argued that the breach left them at an "increased risk of identity theft," they did not allege any actual misuse of personal information. *Id.* at 40–41 The Third Circuit, relying on *Lujan*, 504 U.S. at 561, 112 S. Ct. at 2136–37, and *Whitmore v. Arkansas*, 495 U.S. 149, 155, 110 S. Ct. 1717, 1722–23 (1990), found that the plaintiffs' alleged injuries were hypothetical and relied on speculation, and thus they were not "imminent" or "certainly impending." *Reilly*, 664 F.3d at 43. As a result, the plaintiffs did not have standing. *Id.*

The Fourth Circuit has likewise rejected the "increased risk of future identity theft" theory in the context of a data breach. In *Beck v. McDonald*, a class of veterans who received medical treatment and health care at a South Carolina Veterans Affairs Medical Center brought actions alleging violations of various federal statutes following two data breaches at the Medical Center. 848 F.3d at 266. The plaintiffs sought to establish Article III standing based on (1) the harm

from the increased risk of future identity theft and (2) the cost of measures to protect against it. *Id.* at 266–67. The Fourth Circuit, distinguishing *Remijas* and *Krottner* on the ground that those cases included allegations of actual misuse, found that the plaintiffs' alleged injury from the elevated risk of identity theft was "too speculative": "[E]ven 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." *Id.* at 274. The "mere theft" of the plaintiffs' data, without something more, required the consideration of the "attenuated chain of possibilities" rejected by *Clapper*. *Id.* at 275. This theory of harm was simply "too speculative to constitute an injury-in-fact." *Id.* at 274.[4]

And notably, the Eighth Circuit in *In re SuperValu, Inc.* found no standing on an "increased risk of future identity theft" theory, even when a named plaintiff alleged actual misuse of personal information. 870 F.3d at 769–71. There, a class of grocery store customers filed suit against SuperValu and other grocery store owner-operators following two data breaches in which the customers' financial

[4] The Fourth Circuit later found standing in a data breach case where the plaintiffs did allege that hackers "used—and attempted to use—the Plaintiffs' personal information to open Chase Amazon Visa credit card accounts without their knowledge or approval." *Hutton v. Nat'l Bd. of Exam'rs in Optometry, Inc.*, 892 F.3d 613, 622 (4th Cir. 2018). There, as we do here, the Fourth Circuit noted the distinction between cases alleging the possibility of misuse of personal information and cases alleging actual misuse. *See id.*

information was allegedly accessed and stolen. *Id.* at 765. The customers alleged that, as a result of the data breaches, hackers were allowed to gain access to customers' "names, credit or debit card account numbers, expiration dates, card verification value (CVV) codes, and personal identification numbers (PINs)." *Id.* at 766. In support of their theory of standing, the customers relied on a June 2007 United States Government Accountability Office (GAO) report on data breaches, which states that "identity theft" includes "many types of criminal activities, including fraud on existing accounts—such as unauthorized use of a stolen credit card number—or fraudulent creation of new accounts—such as using stolen data to open a credit card account in someone else's name." *Id.* at 770 (citing U.S. Gov't Accountability Off., GAO-07-737, *Personal Information: Data Breaches are Frequent, but Evidence of Resulting Identity Theft is Limited; However, the Full Extent is Unknown* (2007), http://www.gao.gov/assets/270/262899.pdf (hereinafter "GAO Report")). That report points out, however, that compromised credit or debit card information, without additional personal identifying information, "generally cannot be used alone to open unauthorized new accounts." *Id.* (citing GAO Report at 30). The Eighth Circuit additionally noted that the GAO report concludes that "most breaches have not resulted in detected incidents of identity theft." *Id.* at 771 (citing GAO Report at 21).

In light of the GAO Report's findings, the Eighth Circuit found that the plaintiffs failed to demonstrate a substantial risk that they would suffer identity theft in the future. *Id.* at 770. The hackers in *SuperValu* were not alleged to have stolen social security numbers, birth dates, or driver's license numbers, and thus, according to the GAO report, the risk of identity theft was "little to no[ne]." *Id.* The Court did find, however, that a lone named plaintiff alleged actual misuse, and thus that plaintiff had standing based on *present*, but not *future* injury. *Id.* at 772.

We are persuaded by the reasoning of the Eighth Circuit in *SuperValu*, and the facts of that case map closely to the facts of this one. Here, as the plaintiffs did in *SuperValu*, Tsao has alleged that hackers *may* have accessed and stolen customer credit card data "including the cardholder name, the account number, expiration date, card verification value ('CVV'), and PIN data for debit cards." And here, just like the plaintiffs in *SuperValu*, Tsao cites to the 2007 GAO Report on data breaches in support of his theory that the PDQ hack may result in future identity theft. But we, like the Eighth Circuit in *SuperValu*, believe the GAO Report actually demonstrates why there is no "substantial risk" of identity theft here. Tsao has not alleged that social security numbers, birth dates, or driver's license numbers were compromised in the PDQ breach, and the card information allegedly accessed by the PDQ hackers "generally cannot be used alone to open unauthorized new accounts." GAO Report at 30. So, based on the GAO Report, it

is unlikely that the information allegedly stolen in the PDQ breach, standing alone, raises a substantial risk of identity theft.

This leaves us with the risk that the hackers, if they accessed and stole Tsao's credit card information, could make unauthorized purchases with his cards or drain his accounts. But again, the GAO Report suggests that most data breaches have not resulted in detected incidents of fraud on existing accounts. *See id.* at 21. Indeed, the GAO Report reviewed the 24 largest data breaches between January 2000 and June 2005 and found that only 4 of the 24 breaches (roughly 16.667%) resulted in some form of identity theft, and only 3 resulted in account theft or fraud (12.5%). *Id.* at 24–25. Given the low rate of account theft, the GAO Report simply does not support the conclusion that the breach here presented a "substantial risk" that Tsao would suffer unauthorized charges on his cards or account draining.

Of course, we recognize that the GAO Report is over a decade old, and it is possible that some breaches may present a greater risk of identity theft than others. But even if we set aside the GAO Report and the reasoning of *SuperValu*, we remain unconvinced that Tsao has met his burden to show that the there is a "substantial risk" of harm, or that such harm is "certainly impending." *Clapper*, 568 U.S. at 409, 414 n.5, 133 S. Ct. at 1147, 1150 n.5. Three considerations color this conclusion.

First, we recently held in *Muransky* that conclusory allegations of an "elevated risk of identity theft"—or, as Tsao puts it, a "continuing increased risk" of identity theft—"[are] simply not enough" to confer standing. *Muranksy*, 979 F.3d at 933. Tsao's allegations about the "increased risk" of identity theft are supported only by reports defining identity theft, outlining the general risks of identity theft, or stating that identity thieves have stolen $112 billion in the last six years. These reports do nothing to clarify the risks to the plaintiffs *in this case*, and Tsao's threadbare allegations of "increased risk" are insufficient to confer standing.

Second, Tsao offers only vague, conclusory allegations that members of the class have suffered any actual misuse of their personal data—here, "unauthorized charges." But again, conclusory allegations of injury are not enough to confer standing. *See Iqbal*, 556 U.S. at 678, 129 S. Ct. at 1949. Of course, as our sister Circuits have recognized, evidence of actual misuse is not necessary for a plaintiff to establish standing following a data breach. *See, e.g.*, *Beck*, 848 F.3d at 275 (stating that district court did not impermissibly require plaintiffs to demonstrate actual misuse). However, without specific evidence of *some* misuse of class members' data, a named plaintiff's burden to plausibly plead factual allegations sufficient to show that the threatened harm of future identity theft was "certainly impending"—or that there was a "substantial risk" of such harm—will be difficult

to meet. *Cf. Resnick v. AvMed, Inc.*, 693 F.3d 1317, 1323 n.1 (11th Cir. 2012) (finding that plaintiffs who suffered "actual" identity theft had standing but noting that "speculative" identity theft may not be sufficient to confer standing). As the case law discussed above confirms, most plaintiffs that have failed to offer at least some evidence of actual misuse of class members' data have fared poorly in disputes over standing. *See* Op. at 14–21.

Third, Tsao immediately cancelled his credit cards following disclosure of the PDQ breach, effectively eliminating the risk of credit card fraud in the future. Of course, even if Tsao's cards are cancelled, some risk of future harm involving identity theft (for example, the use of Tsao's name) still exists, but that risk is not substantial and is, at best, speculative.

In short, Tsao has not alleged either that the PDQ data breach placed him at a "substantial risk" of future identity theft or that identity theft was "certainly impending." *Clapper*, 568 U.S. at 409, 414 n.5, 133 S. Ct. at 1147, 1150 n.5. Evidence of a mere data breach does not, standing alone, satisfy the requirements of Article III standing. It follows that Tsao does not have standing here based on an "increased risk" of identity theft.

C.

We turn now to Tsao's claims that he has suffered actual, present injuries in his efforts to mitigate the risk of identity theft caused by the data breach.

Following notice of the PDQ data breach, Tsao notified Wells Fargo and Chase to cancel his credit cards and, in his words, "proactively t[ook] steps to mitigate the damage done by PDQ's mistakes." As a result of these mitigation efforts, Tsao claims that he has suffered three distinct injuries: (1) lost opportunity to accrue cash back or rewards points on his cancelled credit cards, (2) costs associated with detection and prevention of identity theft in taking the time and effort to cancel and replace his credit cards; and (3) restricted account access to his preferred payment cards. Tsao's mitigation efforts are not enough to confer standing.

It is well established that plaintiffs "cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending." *Clapper*, 568 U.S. at 416, 133 S. Ct. at 1151; *see also Muransky*, 979 F.3d at 931 (citing *Clapper* and stating the same). In *Muransky*, this Court held that a plaintiff's mitigation costs—there, "additional time destroying or safeguarding his receipt"—were insufficient to confer standing because there was no substantial risk of identity theft. *Muransky*, 979 F.3d at 931. Although we noted that allegations of "wasted time" could sometimes "state a concrete harm for standing purposes," we noted that Muransky's "management-of-risk claim [wa]s bound up with his arguments about actual risk," *id.* at 930–31 (quotations and citations omitted). As a result, Muransky's "assertion of wasted

time and effort necessarily r[ose] or f[ell] along with" the Court's determination of whether there was a substantial risk of harm. *Id.* at 931.

So too here. The mitigation costs Tsao alleges are inextricably tied to his perception of the actual risk of identity theft following the PDQ data breach. Tsao, by his own admission, voluntarily cancelled his credit cards, and the three types of harm he has identified flowed from that cancellation. By cancelling his cards, he voluntarily forwent the opportunity to accrue cash back or rewards points on those cards. By cancelling his cards, he voluntarily restricted access to his preferred payment cards. And by cancelling his cards, he voluntarily spent time safeguarding his accounts. Tsao cannot conjure standing here by inflicting injuries on himself to avoid an insubstantial, non-imminent risk of identity theft. To hold otherwise would allow "an enterprising plaintiff . . . to secure a lower standard for Article III standing simply by making an expenditure based on a nonparanoid fear." *Clapper*, 568 U.S. at 416, 133 S. Ct. at 1151. The law does not permit such a result.

IV.

We hold that Tsao lacks Article III standing because he cannot demonstrate that there is a substantial risk of future identity theft—or that identity theft is certainly impending—and because he cannot manufacture standing by incurring

costs in anticipation of non-imminent harm. Accordingly, we affirm the District Court's order dismissing the case without prejudice for lack of standing.

AFFIRMED.

JORDAN, Circuit Judge, concurring in the judgment.

Given our recent decision in *Muransky v. Godiva Chocolatier, Inc.*, 979 F. 3d 917 (11th Cir. 2020) (en banc)—a decision from which I dissented—I concur in the judgment. I note only that the court here, rather than viewing Mr. Tsao's allegations favorably, necessarily engages in a value-laden and normative inquiry concerning the question of "substantial risk" at the motion-to-dismiss stage. That to me is problematic for a number of reasons, *see id.* at 964-70 (Jordan, J., dissenting), but *Muransky* apparently has sanctioned such an analytical approach. Hopefully the Supreme Court will soon grant certiorari in a case presenting the question of Article III standing in a data breach case.