United States Court of Appeals
For the Second Circuit

August Term 2020

Submitted: November 25, 2020
Decided: April 26, 2021

No. 19-4310

DEVONNE MCMORRIS,

Plaintiff-Appellant,

ROBIN STEVEN, SEAN MUNGIN, on behalf of themselves, all others similarly situated, and the general public,

Plaintiffs,

v.

CARLOS LOPEZ & ASSOCIATES, LLC, CARLOS LOPEZ,

Defendants-Appellees.

Appeal from the United States District Court
for the Southern District of New York
No. 18-cv-6500, Jesse M. Furman, *Judge*.

Before: CALABRESI, KATZMANN, AND SULLIVAN, *Circuit Judges*.

Plaintiff-Appellant Devonne McMorris appeals from an order of the United States District Court for the Southern District of New York (Furman, *J.*) dismissing her claims against Defendants-Appellees Carlos Lopez & Associates, LLC ("CLA") and Carlos Lopez for lack of Article III standing. McMorris, along with two other non-appealing plaintiffs, had initially filed a class-action complaint alleging a variety of state-law claims against CLA and its principal based on an errant email sent to all of CLA's employees containing the sensitive personally identifiable information ("PII") of approximately 130 current and former CLA workers. On appeal, McMorris argues that the district court erred by dismissing her claims because, even though she did not allege that her PII had actually been misused as a result of CLA's errant email, she alleged an increased risk of identity theft sufficient to confer Article III standing. We agree that in the context of unauthorized data disclosures, plaintiffs may establish an Article III injury in fact based solely on a substantial risk of identity theft or fraud, even when those plaintiffs have not yet been the victims of such identity theft or fraud. Nevertheless, the district court correctly concluded that McMorris failed to establish an injury in fact in this case.

AFFIRMED.

Abraham Z. Melamed, Derek Smith Law Group, PLLC, New York, NY, *for Plaintiff-Appellant Devonne McMorris*.

Joseph R. Palmore, Morrison & Foerster LLP, Washington, DC (Michael B. Miller, Lena H. Hughes, Janie Buckley, Morrison & Foerster LLP, New York, NY, *on the brief*), *for Defendants-Appellees Carlos Lopez & Associates, LLC and Carlos Lopez*.

RICHARD J. SULLIVAN, *Circuit Judge*:

Plaintiff-Appellant Devonne McMorris appeals from an order of the United States District Court for the Southern District of New York (Furman, *J.*) dismissing her claims against Defendants-Appellees Carlos Lopez & Associates, LLP and Carlos Lopez for lack of subject-matter jurisdiction because McMorris and her co-plaintiffs failed to allege an injury in fact sufficient to confer Article III standing. For the reasons set forth below, we affirm.

I. Background

This case involves the intersection of two phenomena that have become increasingly common in our digitized world: data breaches and inadvertent mass emails.

Carlos Lopez & Associates, LLP ("CLA") provides mental and behavioral health services to veterans, service members, and their families and communities.[1]

[1] We draw the following facts from McMorris's operative complaint and from the transcript of the oral argument before the district court, as is proper when considering a dismissal for lack of subject-matter jurisdiction. *See Libertarian Party of Erie Cnty. v. Cuomo*, 970 F.3d 106, 120–21 (2d Cir. 2020) (explaining that, when considering a motion to dismiss "for lack of statutory or constitutional power to adjudicate the action," a court may refer to evidence outside the pleadings), *petition for cert. filed*, No. 20-1151 (Feb. 23, 2021). In the present context involving a facial challenge to the district court's jurisdiction, we assume the facts in the complaint to be true "unless contradicted by more specific allegations or documentary evidence," and "we construe all reasonable inferences to be drawn from those factual allegations in [McMorris's] favor." *Amidax Trading Grp. v. S.W.I.F.T. SCRL*, 671 F.3d 140, 145 (2d Cir. 2011).

In June 2018, a CLA employee accidentally sent an email to all of the approximately 65 employees at the company. Attached to the email was a spreadsheet containing sensitive personally identifiable information ("PII") – including Social Security numbers, home addresses, dates of birth, telephone numbers, educational degrees, and dates of hire – of approximately 130 then-current and former CLA employees. Two weeks later, CLA emailed its then-current employees to address the accidental email, but it did not contact any former employees regarding the disclosure or take any other corrective action.

After the PII spreadsheet was circulated, three individuals whose information had been shared – Robin Steven, Sean Mungin, and Devonne McMorris ("Plaintiffs") – filed a class-action complaint against CLA and its principal, Carlos Lopez. In their operative complaint, Plaintiffs asserted state-law claims for negligence, negligence per se, and statutory consumer protection violations on behalf of classes in California, Florida, Texas, Maine, New Jersey, and New York. They alleged that CLA "breached its duty to protect and safeguard [their] personal information and to take reasonable steps to contain the damage caused where such information was compromised." App'x 2. Although Plaintiffs did not allege that they had been the victims of fraud or identity theft as a result

of the errant email, they claimed that, because their PII had been disclosed to all of CLA's then-current employees, they were "at imminent risk of suffering identity theft" and becoming the victims of "unknown but certainly impending future crimes." *Id.* at 6, 9. Moreover, while they did not allege that the PII in the spreadsheet was ever shared with anyone outside of CLA or taken or misused by any third parties, Plaintiffs claimed that they cancelled credit cards, purchased credit monitoring and identity theft protection services, and spent time assessing whether they should apply for new Social Security numbers after the email incident.

CLA moved to dismiss Plaintiffs' claims for, among other things, lack of Article III standing. But before the deadline for Plaintiffs' response to the motion to dismiss, the parties reached a class settlement, which they asked the district court to approve. In advance of the scheduled class settlement fairness hearing, the district court *sua sponte* ordered further briefing on whether Plaintiffs possessed Article III standing.

At the fairness hearing held on November 14, 2019, the court informed the parties of its preliminary conclusion that Plaintiffs lacked Article III standing because they failed to allege "an injury that is concrete and particularized and

certainly impending." App'x 67. The district court emphasized that "the parties concede that there is no evidence that any class members' identity was actually stolen . . . , let alone misused," and that the sharing of Plaintiffs' PII "was not the result of any intentional act by third parties," such as "hacking or some sort of criminal conduct from which it could be inferred that those [who] retained data intended to and were likely to misuse it." *Id.* at 69. Rather, "the gravamen of the claim in this case is that defendants essentially acted with insufficient care by sharing [PII] of class members with employees within the company." *Id.*

On November 22, 2019, the district court issued a written opinion formally denying the outstanding motion for approval of the class settlement and dismissing the case for lack of subject-matter jurisdiction. *See Steven v. Carlos Lopez & Assocs., LLC*, 422 F. Supp. 3d 801, 807 (S.D.N.Y. 2019). In that opinion, the district court noted that, unlike several other circuits, the Second Circuit has not yet addressed whether plaintiffs alleging the theft or inadvertent disclosure of their data may establish standing to bring claims against the entity that held their data based on an increased risk of future identity theft or fraud. *See id.* at 804. The district court explained, however, that even if the Second Circuit were to recognize such a theory, "it would be of no help to Plaintiffs in this case" because they failed

to allege facts indicating that they faced "certainly impending" identity theft or fraud, or even a "substantial risk" of such harm. *Id.* (internal quotation marks omitted). The district court recognized that, unlike the cases in which other circuits have held that data breach victims have established standing based on a risk of future identity theft, Plaintiffs here did not allege that their data had been misused in any way or compromised as the result of an intentionally targeted data theft. *See id.* at 804–05. Indeed, the district court observed that "it is arguably a misnomer to even call this case a 'data breach' case," since, "[a]t best, the data was 'misplaced'" by an internal CLA employee rather than taken by a third party. *Id.* at 806 n.3 (internal citations omitted).

The district court also held that Plaintiffs could not establish an Article III injury in fact based on "the time and money spent monitoring or changing their financial information and accounts." *Id.* at 807. The court explained that, since Plaintiffs failed to allege a substantial risk of identity theft or that such harm was certainly impending, they could not establish standing by, in essence, inflicting harm on themselves based on a speculative fear of future identity theft. *See id.*

After concluding that Plaintiffs lacked Article III standing, the district court held that it was "powerless to approve the parties' proposed class settlement" and

dismissed the case for lack of subject-matter jurisdiction. *Id.* (internal quotation marks omitted). Following the district court's decision, McMorris (without the other named Plaintiffs) appealed.

II. Discussion

"The existence of standing is a question of law that we review *de novo*." *Shain v. Ellison*, 356 F.3d 211, 214 (2d Cir. 2004). Because federal courts are courts of limited jurisdiction, if a "court determines at any time that it lacks subject-matter jurisdiction, the court must dismiss the action." Fed. R. Civ. P. 12(h)(3). That is so even when a court is asked only to approve a class-action settlement, since "[a] court is powerless to approve a proposed class settlement if it lacks jurisdiction over the dispute." *Frank v. Gaos*, 139 S. Ct. 1041, 1046 (2019). In a class action, "federal courts lack jurisdiction if no named plaintiff has standing." *Id.*

"To establish standing under Article III of the Constitution, a plaintiff must demonstrate (1) that he or she suffered an injury in fact that is concrete, particularized, and actual or imminent, (2) that the injury was caused by the defendant, and (3) that the injury would likely be redressed by the requested judicial relief." *Thole v. U.S. Bank N.A.*, 140 S. Ct. 1615, 1618 (2020). "The party invoking federal jurisdiction bears the burden of establishing" each element of

standing, which "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 successive stages of litigation." *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 561 (1992). This case concerns only the first element of Article III standing: the existence of an injury in fact.

With respect to that element, the Supreme Court has made clear that "allegations of possible future injury" or even an "objectively reasonable likelihood" of future injury are insufficient to confer standing. *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 409–10 (2013) (internal quotation marks, alterations, and emphasis omitted). Rather, a future injury constitutes an Article III injury in fact only "if the threatened injury is certainly impending, or there is a substantial risk that the harm will occur." *Susan B. Anthony List v. Driehaus*, 573 U.S. 149, 158 (2014) (internal quotation marks omitted).

This Court has not yet addressed whether a plaintiff may establish standing based on a risk of future identity theft or fraud stemming from the unauthorized disclosure of that plaintiff's data. Some courts have suggested that there is a circuit split on the issue. *See, e.g.*, *Tsao v. Captiva MVP Rest. Partners, LLC*, 986 F.3d 1332, 1340 (11th Cir. 2021); *Beck v. McDonald*, 848 F.3d 262, 273–74 (4th Cir. 2017); *Katz v.*

Pershing, LLC, 672 F.3d 64, 80 (1st Cir. 2012). But in actuality, no court of appeals has explicitly foreclosed plaintiffs from establishing standing based on a risk of future identity theft – even those courts that have declined to find standing on the facts of a particular case. *See, e.g.*, *In re SuperValu, Inc.*, 870 F.3d 763, 773 (8th Cir. 2017) (declining to hold that "evidence of misuse following a data breach is necessary for a plaintiff to establish standing" despite finding that certain plaintiffs lacked standing); *see also Tsao*, 986 F.3d at 1343 ("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.").[2] Indeed, requiring plaintiffs to allege that they have already suffered identity theft or fraud as the result of a data breach would seem to run afoul of the Supreme Court's recognition that "[a]n allegation of future injury may suffice" to establish Article III standing "if the threatened injury is certainly impending, or there is a substantial risk that the harm will occur." *Susan B. Anthony List*, 573 U.S. at 158 (internal quotation marks

[2] The Third Circuit's decision in *Reilly v. Ceridian Corp.* perhaps comes closest to unilaterally rejecting an "increased-risk" theory of injury in fact in the context of a data breach. *See* 664 F.3d 38, 45 (3d Cir. 2011) ("In data breach cases where no misuse is alleged, however, there has been no injury[.]"). But even there, the Third Circuit distinguished analogous cases from the Ninth and Seventh Circuits on their facts instead of rejecting the "increased-risk" theory altogether. *See id.* at 44 (explaining that, in contrast to those cases, "there [was] no evidence that the intrusion" in *Reilly* "was intentional or malicious" or that any "identifiable taking occurred; all that [was] known [was] that a firewall was penetrated").

omitted). We therefore join all of our sister circuits that have specifically addressed the issue in holding that plaintiffs may establish standing based on an increased risk of identity theft or fraud following the unauthorized disclosure of their data.[3]

Of course, the fact that plaintiffs *may* establish standing based on an "increased-risk" theory does not mean that the Plaintiffs have done so here. As the district court recognized, the courts that have confronted standing in the context of the unauthorized disclosure of data have considered certain factors that weigh in favor of finding an Article III injury in fact. And while none of these factors is alone necessary or sufficient to confer standing, they all bear on whether the risk of identity theft or fraud is sufficiently "concrete, particularized, and . . . imminent." *Thole*, 140 S. Ct. at 1618. We therefore endorse those factors here, most of which are not implicated in this case.

[3] We express no view on the separate but related question of whether plaintiffs may allege a *present* injury in fact stemming from the violation of a statute designed to protect individuals' privacy, which primarily involves the application of the Supreme Court's decision in *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540 (2016). *See, e.g.*, *In re Horizon Healthcare Servs. Inc. Data Breach Litig.*, 846 F.3d 625, 634, 636–38 (3d Cir. 2017). Here, Plaintiffs brought claims asserting only a risk of future identity theft or fraud, so we have no reason to address this privacy-based theory of standing. *See id.* at 639 n.20 (distinguishing that case from *Reilly v. Ceridian Corp.* because, in *Horizon*, the plaintiffs were "not complaining solely of future injuries").

First, and most importantly, our sister circuits have consistently considered whether the data at issue has been compromised as the result of a targeted attack intended to obtain the plaintiffs' data. *See, e.g.*, *In re U.S. Off. of Pers. Mgmt. Data Sec. Breach Litig.*, 928 F.3d 42, 57–58 (D.C. Cir. 2019) ("*OPM*"); *In re Zappos.com, Inc.*, 888 F.3d 1020, 1029 n.13 (9th Cir. 2018) ("*Zappos*"); *Galaria v. Nationwide Mut. Ins. Co.*, 663 F. App'x 384, 388–90 (6th Cir. 2016). Where plaintiffs fail to present evidence or make any allegations that an unauthorized third party purposefully obtained the plaintiffs' data, courts have regularly held that the risk of future identity theft is too speculative to support Article III standing. *See, e.g.*, *Beck*, 848 F.3d at 274–75; *Katz*, 672 F.3d at 80; *Reilly v. Ceridian Corp.*, 664 F.3d 38, 44 (3d Cir. 2011). By contrast, where plaintiffs demonstrate that a malicious third party intentionally targeted a defendant's system and stole plaintiffs' data stored on that system, courts have been more willing to find that those plaintiffs have established a likelihood of future identity theft or fraud sufficient to confer standing. As the Seventh Circuit explained in the context of a targeted cyberattack of a department store's customer database: "Why else would hackers break into a store's database and steal consumers' private information? Presumably, the purpose of the hack

is, sooner or later, to make fraudulent charges or assume those consumers' identities." *Remijas v. Neiman Marcus Grp., LLC*, 794 F.3d 688, 693 (7th Cir. 2015).

Second, while not a necessary component of establishing standing, courts have been more likely to conclude that plaintiffs have established a substantial risk of future injury where they can show that at least some part of the compromised dataset has been misused – even if plaintiffs' *particular* data subject to the same disclosure incident has not yet been affected. For example, in the context of a data breach into an online retailer's customer database, the Ninth Circuit explained that although the specific plaintiffs in that case had not experienced any fraudulent activity, allegations that *other* customers whose data was compromised in the same data breach had reported fraudulent charges on their credit cards helped establish that the plaintiffs were at a substantial risk of future fraud. *See Zappos*, 888 F.3d at 1027, 1027 n.7; *see also OPM*, 928 F.3d at 58 ("[A] hacker's 'intent' to use breach victims' personal data for identity theft becomes markedly less important where, as here, several victims allege that they have *already* suffered identity theft and fraud as a result of the breaches."). Similarly, evidence that plaintiffs' data is already being misused, even if that misuse has not yet resulted in an actual or attempted identity theft, can also support a finding that those plaintiffs are at a

substantial risk of identity theft or fraud. As one court in this Circuit recently recognized, allegations that the plaintiffs' PII was available for sale on the Dark Web [4] following a data breach – and could therefore be purchased by cybercriminals at any moment to commit identity theft or fraud – provided strong support for the conclusion that those plaintiffs had established an Article III injury in fact. *See Fero v. Excellus Health Plan, Inc.*, 304 F. Supp. 3d 333, 341, 344–45 (W.D.N.Y. 2018).

Finally, courts have looked to the type of data at issue, and whether that type of data is more or less likely to subject plaintiffs to a perpetual risk of identity theft or fraud once it has been exposed. Naturally, the dissemination of high-risk information such as Social Security numbers and dates of birth – especially when accompanied by victims' names – makes it more likely that those victims will be subject to future identity theft or fraud. *See, e.g.*, *Attias v. CareFirst, Inc.*, 865 F.3d 620, 628 (D.C. Cir. 2017). By contrast, less sensitive data, such as basic publicly

[4] "The Dark Web is a general term that describes hidden Internet sites that users cannot access without using special software." Kristin Finklea, Cong. Rsch. Serv., 7-5700, *Dark Web* 2 (2017). "Not surprisingly, criminals and other malicious actors . . . use the [D]ark [W]eb to carry out technology-driven crimes, such as computer hacking, identity theft, credit card fraud, and intellectual property theft." Ahmed Ghappour, *Searching Places Unknown: Law Enforcement Jurisdiction on the Dark Web*, 69 Stan. L. Rev. 1075, 1090 (2017).

available information, or data that can be rendered useless to cybercriminals does not pose the same risk of future identity theft or fraud to plaintiffs if exposed. So, for example, where a plaintiff's credit card number was stolen as part of a data breach, but she promptly cancelled her credit card "and no other [PII] – such as her birth date or Social Security number – [was] alleged to have been stolen," we have found that the plaintiff failed to allege "how she [could] plausibly face a threat of future fraud." *Whalen v. Michaels Stores, Inc.*, 689 F. App'x 89, 90 (2d Cir. 2017) (summary order); *see also Tsao*, 986 F.3d at 1344 (explaining that the plaintiff had "immediately cancelled his credit cards following disclosure of the [data] breach, effectively eliminating the risk of credit card fraud in the future").

These factors are by no means the only ones relevant to determining whether plaintiffs have shown an injury in fact based on an increased risk of future identity theft or fraud. After all, determining standing is an inherently fact-specific inquiry that "requires careful judicial examination of a complaint's allegations to ascertain whether the particular plaintiff is entitled to an adjudication of the particular claims asserted." *Allen v. Wright*, 468 U.S. 737, 752 (1984). Nevertheless, these are the considerations that our sister circuits have most consistently addressed in the context of data breaches and other data exposure incidents, and

we agree that they provide helpful guidance in assessing whether plaintiffs have adequately alleged an injury in fact.

We therefore hold that courts confronted with allegations that plaintiffs are at an increased risk of identity theft or fraud based on an unauthorized data disclosure should consider the following non-exhaustive factors in determining whether those plaintiffs have adequately alleged an Article III injury in fact: (1) whether the plaintiffs' data has been exposed as the result of a targeted attempt to obtain that data; (2) whether any portion of the dataset has already been misused, even if the plaintiffs themselves have not yet experienced identity theft or fraud; and (3) whether the type of data that has been exposed is sensitive such that there is a high risk of identity theft or fraud.

In addition to the "increased-risk" theory of injury in fact, this case presents a related question of standing: where plaintiffs take steps to protect themselves following an unauthorized data disclosure, can the cost of those proactive measures alone constitute an injury in fact? We agree with the district court that the answer is "no." *See Carlos Lopez & Assocs.*, 422 F. Supp. 3d at 807. That is, where plaintiffs have shown a substantial risk of future identity theft or fraud, "any expenses they have reasonably incurred to mitigate that risk likewise qualify

as injury in fact." *OPM*, 928 F.3d at 59; *see also Hutton v. Nat'l Bd. of Exam'rs in Optometry, Inc.*, 892 F.3d 613, 622 (4th Cir. 2018); *Lewert v. P.F. Chang's China Bistro, Inc.*, 819 F.3d 963, 966–67 (7th Cir. 2016). But where plaintiffs "have not alleged a substantial risk of future identity theft, the time they spent protecting themselves against this speculative threat cannot create an injury." *SuperValu*, 870 F.3d at 771; *see also Tsao*, 986 F.3d at 1344–45; *Beck*, 848 F.3d at 276–77; *Reilly*, 664 F.3d at 46. This notion stems from the Supreme Court's guidance in *Clapper*, where it noted that plaintiffs "cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending." 568 U.S. at 416.

With these principles in mind, this case presents a relatively straightforward situation in which Plaintiffs have failed to show that they are at a substantial risk of future identity theft or fraud sufficient to establish Article III standing. First, Plaintiffs never alleged that their data was intentionally targeted or obtained by a third party outside of CLA. While it is true that McMorris and the other Plaintiffs claimed that their PII was disclosed in an unauthorized manner to then-current CLA employees, they did not allege that anyone outside of CLA ever obtained their PII. Far from being a "sophisticated" or "malicious" cyberattack "carried out

to obtain sensitive information for improper use," *OPM*, 928 F.3d at 52 (internal quotation marks omitted), this case merely involves the inadvertent disclosure of PII due to an errant email sent to approximately 65 employees.

This case is therefore comparable to the exposure of data in *Beck*. There, the Fourth Circuit considered two separate incidents in which the plaintiffs' data was exposed: one in which an unencrypted laptop containing sensitive patient information records was either misplaced or stolen from the defendant hospital, and another in which four boxes of pathology reports (containing PII of over 2,000 patients) were also either misplaced or stolen. *See Beck*, 848 F.3d at 267–68. Distinguishing those incidents from others in which plaintiffs alleged that "the data thief intentionally targeted the personal information compromised in the data breaches," the *Beck* court held that the plaintiffs' alleged risk of future identity theft was "too speculative" because it required the court to "engage with the same 'attenuated chain of possibilities' rejected by the [Supreme] Court in *Clapper*." *Id.* at 274–75 (quoting *Clapper*, 568 U.S. at 410). Here, this "chain of possibilities" is similarly attenuated: we would have to assume that then-current employees of CLA (a company that, as the district court noted, regularly deals with the highly sensitive personal information of its clients) would either misuse the data

themselves or leak or expose the spreadsheet containing Plaintiffs' PII to a malicious third party, and, if the latter, that such a third party would then misuse Plaintiffs' PII. As in *Beck*, Plaintiffs' allegations are simply insufficient to establish even a "substantial risk" of such harm. *Id.* at 275 (quoting *Clapper*, 568 U.S. at 414 n.5).

Second, Plaintiffs do not allege that their data (or the data of any other then-current or former CLA employees) was in any way misused because of the accidental email. Again, while plaintiffs need not show that they have already experienced identity theft or fraud to adequately plead an Article III injury in fact, Plaintiffs do not allege any facts suggesting that their PII was misused following the accidental email here, which distinguishes this case from those in which plaintiffs have shown that some part of the exposed dataset was compromised. *See, e.g.*, *OPM*, 928 F.3d at 58–59; *Zappos*, 888 F.3d at 1027; *Galaria*, 663 F. App'x at 389 n.1; *Remijas*, 794 F.3d at 692; *Fero*, 304 F. Supp. 3d at 341–42.[5]

[5] For the first time on appeal, McMorris refers to allegations in a never-filed "Second Amended Complaint" that a handful of CLA employees opened the mistaken email, that at least six employees downloaded the spreadsheet, and that at least one of those employees forwarded the email to a personal email address. McMorris does not dispute that these allegations were never presented to the district court, and they are therefore not part of the "record on appeal." *See* Fed. R. App. P. 10(a). We also decline to supplement the record with these new allegations pursuant to Federal Rule of Appellate Procedure 10(e), which "is not a device for presenting evidence to

Finally, while the information that was inadvertently disclosed by CLA included the sort of PII that might put Plaintiffs at a substantial risk of identity theft or fraud, in the absence of any other facts suggesting that the PII was intentionally taken by an unauthorized third party or otherwise misused, this factor alone does not establish an injury in fact.[6] To hold otherwise would allow plaintiffs to string together a lengthy "chain of possibilities" resulting in injury. *Clapper*, 568 U.S. at 410. Accordingly, we conclude that the sensitive nature of McMorris's internally disclosed PII, by itself, does not demonstrate that she is at a substantial risk of future identity theft or fraud.[7]

---

this Court that was not before the trial judge." *Natofsky v. City of New York*, 921 F.3d 337, 344 (2d Cir. 2019) (internal quotation marks omitted), *cert. denied* 140 S. Ct. 2668 (2020).

[6] Of course, there may be situations in which the nature of the data itself reveals that plaintiffs are *not* substantially at risk of identity theft as a result of the exposure. *See, e.g.*, *SuperValu*, 870 F.3d at 770; *Whalen*, 689 F. App'x at 90 (finding no injury where the compromised data included credit card numbers divorced from any PII). We simply note that plaintiffs do not necessarily suffer an injury in fact any and every time there has been a disclosure involving more sensitive data.

[7] McMorris does not press the alternative theory of injury in fact suggested by her complaint – namely, that she and the other Plaintiffs suffered an injury by means of the time and money spent monitoring or changing their financial information and accounts. Accordingly, she has waived any reliance on this alternative theory of harm. *See Norton v. Sam's Club*, 145 F.3d 114, 117 (2d Cir. 1998). Nevertheless, such a theory would fail for the simple reason that McMorris has failed to show that she is at a substantial risk of future identity theft, so "the time [she] spent protecting [herself] against this speculative threat cannot create an injury." *SuperValu*, 870 F.3d at 771 (citing *Clapper*, 568 U.S. at 416).

III. Conclusion

Because McMorris did not allege that her PII was subject to a targeted data breach or allege any facts suggesting that her PII (or that of any others) was misused, the district court correctly dismissed her complaint for failure to establish an Article III injury in fact.

We have considered McMorris's remaining arguments that are properly before us and find them to be without merit. Accordingly, the district court's judgment is affirmed.