Boston College Law Review

Volume 63
Issue 9 *Electronic Supplement*

Article 11

5-2-2022

A Hacker "May" Have Accessed Your Data: Can Victims of Data Breaches Sue Before Alleging Misuse?

John Landzert
Boston College Law School, john.landzert@bc.edu

A HACKER "MAY" HAVE ACCESSED YOUR DATA: CAN VICTIMS OF DATA BREACHES SUE BEFORE ALLEGING MISUSE?

Abstract: On February 4, 2021, in *Tsao v. Captiva MVP Restaurant Partners, LLC*, the United States Court of Appeals for the Eleventh Circuit held that the mere existence of a data breach is insufficient to grant plaintiffs standing to sue the company that exposed their personal information. By doing so, the Eleventh Circuit aligned itself with the Second, Third, Fourth, and Eighth Circuits. In contrast, the Sixth, Seventh, Ninth, and D.C. Circuits have granted standing in such cases. This Comment argues that the Eleventh Circuit properly applied Supreme Court jurisprudence at the time it decided *Tsao* and, in light of more recent Supreme Court decisions, came to the correct conclusion.

INTRODUCTION

Almost all Americans have been victims of a data breach.[1] Data breaches have become commonplace over the last ten years, often leaving the public desensitized to news of breaches that continue to increase in size in spite of the substantial harm that cyber-criminals can inflict from identity theft.[2] Nevertheless, some data breach victims seek legal action against companies that have exposed their data to thieves.[3] Because data breaches do not always lead to immediate harm from identity theft, plaintiffs often can only allege that a

[1] Joseph Marks, *The Cybersecurity 202: There Was Another Massive Data Breach. People Will Probably Forget It in a Week.*, WASH. POST (Aug. 19, 2021), https://www.washingtonpost.com/politics/2021/08/19/cybersecurity-202-there-was-another-massive-data-breach-people-will-probably-forget-it-week/ [https://perma.cc/AXX2-LKVN]; *see Data Breach*, BLACK'S LAW DICTIONARY (11th ed. 2019) (defining data breach as a cybersecurity failure to prevent unwanted third parties from accessing and misusing private information held in a computer system).

[2] Marks, *supra* note 1; *see Identity Theft*, BLACK'S LAW DICTIONARY, *supra* note 1 (defining identity theft as the act of stealing and illegitimately using personal information, often for monetary gain); *see also* Drew Fitzgerald & Robert McMillan, *T-Mobile Hacker Who Stole Data on 50 Million Customers: 'Their Security Is Awful,'* WALL ST. J., https://www.wsj.com/articles/t-mobile-hacker-who-stole-data-on-50-million-customers-their-security-is-awful-11629985105?st=825ftmebq9osi49&reflink=share_mobilewebshare [https://perma.cc/5JW3-WDBC] (Aug. 27, 2021) (discussing a data breach affecting over fifty million T-Mobile customers); *Data Breaches: Most Victims Unaware When Shown Evidence of Multiple Compromised Accounts*, UNIV. OF MICH. NEWS (June 21, 2021), https://news.umich.edu/data-breaches-most-victims-unaware-when-shown-evidence-of-multiple-compromised-accounts/ [https://perma.cc/5XG9-4ZY3] (finding that study participants did not know about 74% of the breaches that affected them).

[3] *E.g.*, Tsao v. Captiva MVP Rest. Partners, LLC, 986 F.3d 1332, 1335–36 (11th Cir. 2021) (hearing a case where plaintiffs sued a restaurant chain for exposing their data to unwanted third parties as a result of a data breach).

breach left them with an elevated risk of injury.[4] The issue of whether data breach plaintiffs have standing when alleging mere threats of future injury has created a split among several federal circuit courts of appeal.[5]

In 2021, in *Tsao v. Captiva MVP Restaurant Partners, LLC*, the United States Court of Appeals for the Eleventh Circuit decided whether victims of a data breach could establish standing based on the existence of a breach alone.[6] Part I of this Comment surveys the legal landscape of Article III standing and discusses the factual and procedural background of *Tsao*.[7] Part II examines the split that has emerged regarding standing in data breach cases in the Second, Third, Fourth, Sixth, Seventh, Eighth, Ninth, Eleventh, and D.C. Circuits.[8] Part III argues that the Eleventh Circuit came to the correct conclusion despite using a legal framework that will likely no longer apply to future data breach cases.[9]

I. ARTICLE III STANDING AND *TSAO V. CAPTIVA MVP RESTAURANT PARTNERS, LLC*

In 2021, in *Tsao v. Captiva MVP Restaurant Partners, LLC*, the United States Court of Appeals for the Eleventh Circuit weighed in on whether victims

---

[4] *See* 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 29 (2007), http://www.gao.gov/assets/270/262899.pdf [https://perma.cc/4WXH-KTVX] (stating that hackers could wait more than a year before using stolen information); *Tsao*, 986 F.3d at 1335–36 (hearing a case where plaintiffs alleged an imminent risk of identity theft without alleging actual misuse of data).

[5] *See Standing*, BLACK'S LAW DICTIONARY, *supra* note 1 (defining standing as the right of a party to use the judiciary to enforce a "legal claim . . . duty or right"). *Compare Tsao*, 986 F.3d at 1344 (denying standing to data breach victims alleging an elevated risk of identity theft), *In re* SuperValu, Inc., 870 F.3d 763, 771–72 (8th Cir. 2017) (same), Beck v. McDonald, 848 F.3d 262, 276 (4th Cir. 2017) (same), Reilly v. Ceridian Corp., 664 F.3d 38, 42 (3d Cir. 2011) (same), *and* Whalen v. Michaels Stores, Inc., 689 F. App'x 89, 90–91 (2d Cir. 2017) (same); *with* Attias v. CareFirst, Inc., 865 F.3d 620, 629 (D.C. Cir. 2017) (granting standing to data breach victims alleging an elevated risk of identity theft); Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 693 (7th Cir. 2015) (same); Krottner v. Starbucks Corp., 628 F.3d 1139, 1143 (9th Cir. 2010) (same); Galaria v. Nationwide Mut. Ins. Co., 663 F. App'x 384, 388 (6th Cir. 2016) (same). *See generally* R. Andrew Grindstaff, Note, *Article III Standing, the Sword and the Shield: Resolving a Circuit Split in Favor of Data Breach Plaintiffs*, 29 WM. & MARY BILL RTS. J. 851 (2021) (discussing the circuit split); Bradford C. Mank, *Data Breaches, Identity Theft, and Article III Standing: Will the Supreme Court Resolve the Split in the Circuits?*, 92 NOTRE DAME L. REV. 1323 (2017) (same); Christian Levis, Amanda Fiorilla & Luke Goveas, *Data Breach Plaintiffs Still Face Circuit Conflict on Standing*, BLOOMBERG L. (June 15, 2021), https://news.bloomberglaw.com/banking-law/data-breach-plaintiffs-still-face-circuit-conflict-on-standing [https://perma.cc/W2XZ-PX86] (same); Kelly Melchiondo, Bilzin Sumberg, *Standing in a Data Breach Case May Depend on Where a Plaintiff Stands*, JDSUPRA (Mar. 5, 2021), https://www.jdsupra.com/legalnews/standing-in-a-data-breach-case-may-3493573/ [https://perma.cc/AR6L-C2JR] (same).

[6] 986 F.3d at 1344.

[7] *See infra* notes 10–53 and accompanying text.

[8] *See infra* notes 54–83 and accompanying text.

[9] *See infra* notes 84–97 and accompanying text.

of data breaches have standing to sue under Article III of the United States Constitution without alleging misuse of their information by third parties.[10] In many cases involving data breaches, plaintiffs are unable to show that the hacker has already misused their data, often leaving plaintiffs in the position of alleging only an elevated risk of future harm of identity theft.[11] Section A of this Part discusses the legal landscape of Article III standing jurisprudence.[12] Section B provides the factual and procedural background of *Tsao*.[13]

A. Standing in Cases of Threatened Injuries

Article III of the United States Constitution limits the power of federal courts to decide "[c]ases" and "[c]ontroversies."[14] Although it is not explicitly stated in the Constitution, the Supreme Court has understood Article III to require a plaintiff to have standing.[15] To establish standing, a plaintiff must allege an injury in fact that is reasonably connected to the alleged behavior of the defendant and for which judicial action can probably provide a remedy.[16] The Court has implemented these limitations to avoid overextending the reach of the judiciary and to maintain the separation of powers.[17] To meet the injury in fact requirement, a plaintiff must establish a violation of an interest that the law safeguards which is (1) "concrete and particularized" as well as (2) "actual

---

[10] *See* 986 F.3d at 1344 (holding that a mere data breach absent a showing of misuse is insufficient to confer Article III standing); *see also In re SuperValu, Inc.*, 870 F.3d at 771–72 (citing U.S. GOV'T ACCOUNTABILITY OFF., *supra* note 4, at 21) (rejecting standing using a June 2007 report on data breaches from the United States Government Accountability Office ("GAO Report") which found that a fraction of data breaches lead to actual misuse of data); *Beck*, 848 F.3d at 272 (finding the substantial risk standard for threatened injuries from *Clapper v. Amnesty Int'l USA*, 568 U.S. 398 (2013), to control in data breach cases); *Remijas*, 794 F.3d at 693 (articulating that victims of a data breach are at a substantial risk of identity theft because hackers likely obtained the information for that purpose).

[11] Mank, *supra* note 5, at 1325; *see Hacker*, BLACK'S LAW DICTIONARY, *supra* note 1 (defining hacker as a person who accesses someone else's computer system and covertly uses data held within it).

[12] *See infra* notes 14–39 and accompanying text.

[13] *See infra* notes 40–53 and accompanying text.

[14] U.S. CONST. art. III, § 2; *see also* Spokeo, Inc. v. Robins, 578 U.S. 330, 337 (2016) (discussing Article III's limit on federal courts to hearing only "[c]ases" and "[c]ontroversies").

[15] *See* Lujan v. Defs. of Wildlife, 504 U.S. 555, 560 (1992) (stating that the doctrine of standing is an essential component of the cases and controversies limitation of Article III); *see also Spokeo*, 578 U.S. at 338 (stating that "[s]tanding to sue is a doctrine rooted" in the cases and controversies limitation).

[16] *Lujan*, 504 U.S. at 560–61; *see Injury*, BLACK'S LAW DICTIONARY, *supra* note 1 (defining injury as "a violation of another's legal right, for which the law provides a remedy"). At the pleading stage, a plaintiff bears the burden of demonstrating clearly alleged facts that prove each element. *Spokeo*, 578 U.S. at 338.

[17] *See Spokeo*, 578 U.S. at 337–38 (discussing the Court's interpretation of "[c]ases" and "[c]ontroversies" as including the doctrine of standing to enforce the proper role of the judiciary); *see also* Raines v. Byrd, 521 U.S. 811, 818 (1997) (quoting Simon v. E. Ky. Welfare Rts. Org., 426 U.S. 26, 37 (1976)) (stating that "[n]o principle is more fundamental to the judiciary's proper role" than the cases and controversies limitation); Whitmore v. Arkansas, 495 U.S. 149, 155 (1990) (articulating that the doctrine of standing filters the disputes that are suitable for courts to hear).

or imminent," as opposed to one which is speculative.[18] In some cases, the threat of a future injury may constitute a concrete injury if the threatened injury is imminent.[19] Through several decisions in the past decade, the Supreme Court has addressed the injury in fact requirement in cases of risks of future harm.[20]

First, in 2013, in *Clapper v. Amnesty International USA,* the United States Supreme Court denied standing to plaintiffs alleging threat of future injury for failing to show that their threatened injury was "certainly impending."[21] In *Clapper*, a group of plaintiffs filed a class action lawsuit in response to an amendment to the Foreign Intelligence Surveillance Act of 1978 (FISA).[22] The class action group included media entities and others who alleged that their work obliged them to maintain sensitive interactions with foreign individu-

---

[18] *Lujan*, 504 U.S. at 560–61 (first citing Allen v. Wright, 468 U.S. 737, 756 (1984), *abrogated by* Lexmark Int'l, Inc. v. Static Control Components, Inc., 572 U.S. 118 (2014); then citing Warth v. Seldin, 422 U.S. 490, 508 (1975); then citing Sierra Club v. Morton, 405 U.S. 727, 740–41, n.16 (1972); and then citing *Whitmore*, 495 U.S. at 155)); *see Spokeo*, 578 U.S. at 339 (citing *Lujan*, 504 U.S. at 560 n.1) (explaining that a particularized injury is specific to the plaintiff in a manner that impacts them personally); *see also* Ass'n of Data Processing Serv. Orgs., Inc. v. Camp, 397 U.S. 150, 152 (1970) (requiring that "the plaintiff alleges that the challenged action . . . caused him injury in fact"); William A. Fletcher, *The Structure of Standing*, 98 YALE L. J. 221, 230 (1988) (discussing the role of *Data Processing* as one of the first cases to require injury in fact as a fundamental element of Article III standing). The Court uses the plain meaning of concrete to require an injury to be real; nevertheless, intangible injuries, such as threats of future injuries, may be concrete. *See Spokeo*, 578 U.S. at 340–41 (stating that, to ascertain whether an intangible injury is concrete, it is helpful to examine whether the intangible injury is strongly correlated with a harm often recognized as a foundation for standing in English or American courts, or alternatively whether Congress has raised the intangible harm to a legally cognizable classification (citing *Lujan*, 504 U.S. at 578)).

[19] *See* Clapper v. Amnesty Int'l USA, 568 U.S. 398, 409 (2013) (holding a future threat can be concrete if it is imminent); *cf.* TransUnion LLC v. Ramirez, 141 S. Ct. 2190, 2210 (2021) (declining to hold that a future injury can be concrete in a case for damages as opposed to injunctive relief).

[20] *See* Susan B. Anthony List v. Driehaus, 573 U.S. 149, 158 (2014) (stating that plaintiffs asserting an imminent harm may demonstrate a "certainly impending" or "substantial risk" of injury (citing *Clapper*, 568 U.S. at 409, 414, n.5)); *Clapper*, 568 U.S. at 401 (stating that a threatened harm may constitute a concrete injury if it is "certainly impending" (quoting *Whitmore*, 495 U.S. at 158)).

[21] 568 U.S. at 414.

[22] *Id.* at 401, 406; *see Class Action*, BLACK'S LAW DICTIONARY, *supra* note 1 (defining class action as a lawsuit in which an individual or small assemblage of plaintiffs represents a broader class of similarly-situated people in the interest of convenience). FISA establishes warrant processes under the jurisdiction of the Foreign Intelligence Surveillance Court (FISC) for the U.S. government engaging in foreign surveillance on its own citizens. *See* Jonathan D. Forgang, Note, *"The Right of the People": The NSA, the FISA Amendments Act of 2008, and Foreign Intelligence Surveillance of Americans Overseas*, 78 FORDHAM L. REV. 217, 223 (2009) (providing a historical background of FISA). *See generally* Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, 92 Stat. 1783 (1978) (codified as amended at 50 U.S.C. §§ 1801–1885(c) (2018)). The lawsuit in *Clapper* was in response to § 1881a of the FISA Amendments Act of 2008, which created new procedures that no longer compelled probable cause or indication of where the government would conduct electronic surveillance. *Clapper*, 568 U.S. at 404. *See generally* 50 U.S.C. § 1881a (2018); FISA Amendments Act of 2008, Pub. L. No. 110-261, § 702, 122 Stat. 2436, 2438 (2008) (codified as amended at 50 U.S.C. § 1881a (2018)).

als.[23] The plaintiffs filed for an injunction, alleging injury in fact due to the reasonable probability that the United States government would intercept their communications under the Amendment.[24] The Supreme Court rejected plaintiffs' argument, concluding that their claims depended on a chain of hypothetical events insufficient to establish imminent injury.[25] The Court employed a strict standard, requiring "certainly impending" harm to meet the imminence prong of the injury in fact requirement for injunctive relief cases.[26] The Court also indicated, however, that it will sometimes employ a less strict "substantial risk" standard of proof.[27] In applying the certainly impending standard to the case, the Court first stated that it was uncertain whether the government would choose to intercept the plaintiffs' communications.[28] The Court then stated that

---

[23] *Clapper*, 568 U.S. at 406.

[24] *Id.* at 407; *Injunction*, BLACK'S LAW DICTIONARY, *supra* note 1 (defining injunction as the court precluding something from occurring). Plaintiffs alleged that there was a sufficient likelihood that their sensitive communications would be under surveillance such that they had either to stop communications with their foreign contacts or take steps to ensure confidentiality. *Clapper*, 568 U.S. at 406–07.

[25] *Clapper*, 568 U.S. at 410.

[26] *Id.* Although the Court did not specify that the certainly impending standard applies to suits seeking injunctive relief, the Court in *TransUnion LLC v. Ramirez* clarified this distinction. *See id.* (stating that threats of future harm must be "certainly impending" to meet the injury in fact requirement for standing); TransUnion LLC v. Ramirez, 141 S. Ct. 2190, 2210 (2021) (distinguishing the *Clapper* Court's use of the certainly impending standard to establish threat of future injury as applicable to cases for injunctive relief).

[27] *See Clapper*, 568 U.S. at 409, 414 n.5 (holding that the imminence requirement of injury in fact requires a harm to be certainly impending and that, in some cases, a substantial risk of harm may be sufficient for standing if plaintiffs took reasonable measures to lessen that potential harm); Mank, *supra* note 5, at 1332–33 (characterizing the certainly impending standard as "very strict" and the substantial risk standard as "less strict" (first citing John L. Jacobus & Benjamin B. Watson, Clapper v. Amnesty International *and Data Privacy Litigation: Is a Change to the Law "Certainly Impending"?*, RICH. J.L. & TECH., Fall 2014, at 1, 10–15; then citing Bradford C. Mank, Clapper v. Amnesty International: *Two or Three Competing Philosophies of Standing Law?*, 81 TENN. L. REV. 211, 222–40 (2014); then citing Marty Lederman, *Commentary:* Susan B. Anthony List*,* Clapper *Footnote 5, and the State of Article III Standing Doctrine*, SCOTUSBLOG (June 17, 2014), https://www.scotusblog.com/2014/06/commentary-susan-b-anthony-list-clapper-footnote-5-and-the-state-of-article-iii-standing-doctrine/ [https://perma.cc/LR58-NCUN]; and then citing *Clapper*, 568 U.S. at 414 n.5)); *see also* Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 693 (7th Cir. 2015) (holding that plaintiffs demonstrated a substantial risk of identity theft without holding that plaintiffs demonstrated that identity theft was certainly impending); Attias v. Carefirst, Inc., 865 F.3d 620, 629 (D.C. Cir. 2017) (stating that plaintiffs demonstrated a "substantial risk of harm" without addressing whether plaintiffs demonstrated that the harm was certainly impending). The Court in *Clapper* noted that "although imminence . . . [can be an] elastic concept, it cannot be stretched" to allow standing in cases of purely speculative injuries. *Clapper*, 568 U.S. at 409 (quoting Lujan v. Defs. of Wildlife, 504 U.S. 555, 564–65 n.2 (1992)). The Court clarified that "certainly impending" harm means that merely potential harms are insufficient for Article III standing. *Id*. *But see TransUnion*, 141 S. Ct. at 2210 (declining to grant standing for a threat of future injury in a suit for damages).

[28] *Clapper*, 568 U.S. at 411. The Court in *Clapper* stated that the statute in question prohibited the government from surveilling plaintiffs' communications, which made it unsurprising that plaintiffs did not allege actual surveillance. *Id*. The Court then stated that even if plaintiffs could prove that government surveillance was imminent, they could not be sure that the government would use 50

the plaintiffs could not assuredly conclude that a court would even allow the surveillance under the Amendment.[29] In holding that the plaintiffs lacked standing, the Court emphasized its hesitance to grant standing in cases where it must speculate how a non-party would act.[30] The Court also rejected the plaintiffs' claim that their remedial steps to ensure continued confidentiality constituted injury in fact.[31] Rather, the Court held that plaintiffs artificially constructed standing by injuring themselves in order to remedy a mere risk of harm that was not imminent.[32] Shortly thereafter, in 2014, in *Susan B. Anthony List v. Driehaus*, the Supreme Court offered the substantial risk standard alongside certainly impending harm as an applicable standard to establish injury in fact.[33]

In 2021, in *TransUnion LLC v. Ramirez*, the United States Supreme Court distinguished *Clapper's* holding as a case for injunctive relief.[34] In contrast, the plaintiffs in *TransUnion* sought damages for the risk of future injury.[35] The Court held that the plaintiffs' mere potential for an injury, was insufficient to confer standing to support a claim for damages.[36] Rather, the Court stated that

---

U.S.C. § 1881a to approve the surveillance. *Id.* at 412. This is so because the government has a multitude of means under the law to administer similar surveillance. *Id.* at 412–13.

[29] *Id.* at 413.

[30] *Id.* The Court highlighted its holding in *Whitmore v. Arkansas* that a litigant cannot establish standing by attempting to prove that a court will make any singular decision. *Id.* at 413–14 (citing Whitmore v. Arkansas, 495 U.S. 149, 159–60) (1990)).

[31] *Id.* at 416.

[32] *Id.* The Court reasoned that allowing a plaintiff to establish standing by mitigating a less than imminent risk of harm would undermine the Article III requirements. *See id.* (explaining that plaintiffs could avoid demonstrating a certainly impending harm by inflicting harm on themselves).

[33] *See* 573 U.S. 149, 158 (2014) (quoting *Clapper*, 568 U.S. at 409, 414 n.5) (holding that the threat of future injury may confer standing if there is a substantial risk of that injury or if the injury is certainly impending); Tsao v. Captiva MVP Rest. Partners, LLC, 986 F.3d 1332, 1339 n.2 (11th Cir. 2021) (explaining that the Supreme Court provided the substantial risk and certainly impending standards but did not state whether they are independent of each other). In 2016, in *Spokeo, Inc. v. Robins*, the Court again addressed Article III standing requirements, but this time in relation to statutory establishment of standing. 578 U.S. 330, 337 (2016). In *Spokeo*, the Court clarified that a mere procedural violation of a statute does not constitute an injury in fact for standing purposes. *Id.* at 341. This is the case even when Congress has created a right by statute and given plaintiffs a legal remedy to seek redress for a violation of that right. *Id.* The Court then stated that its holding does not mean that a future threat of injury cannot be concrete. *Id.* (citing *Clapper*, 568 U.S. at 398). Rather, the Court stated that it has recognized injuries which are difficult to quantify, citing libel and slander *per se* injuries. *Id.*

[34] *See* 141 S. Ct. 2190, 2210 (2021) (stating that the plaintiff may seek *injunctive* relief to stop imminent threats of injury from materializing). The Court also clarified that *Spokeo* did not hold that a mere potential for injury satisfies the concreteness requirement. *Id.* at 2211. The Court noted that in *Spokeo* it offered libel and slander *per se* as examples of where it has recognized an injury from a threat of harm. *Id.* (citing *Spokeo*, 578 U.S. at 341). The Court then specified that there is a distinction between an injury which has already happened—such as publication of a libelous book—which may be difficult to measure and the "mere risk of future harm." *Id.*

[35] *Id.* at 2202.

[36] *Id.* at 2210–12. The Court held that the risk of harm may be sufficient for standing if the risk independently causes a concrete injury. *Id.* at 2211. The Court gave the example of the tort for inten-

the risk of harm must create some other concrete injury to satisfy Article III standing requirements when damages are sought.[37]

Since *Clapper*, federal circuit courts applying the certainly impending and substantial risk standards have diverged in data breach cases over whether plaintiffs can establish standing by alleging an elevated risk of harm resulting from the breach.[38] In *TransUnion*, the Court provided further guidance on standing requirements for cases of threatened future injuries, but circuit courts have not yet applied *TransUnion* to a data breach case.[39]

B. Facts of Tsao v. Captiva MVP Restaurant Partners, LLC

On May 19, 2017, a hacker breached the credit and debit card processing system at PDQ, a restaurant chain selling popular lunch items.[40] On June 8, 2018, PDQ became aware of the breach and informed its customers on June 22, 2018 that hackers may have accessed the data of an unknown group of customers and may have gained access to their names and credit card information.[41]

I Tan Tsao purchased food from a PDQ restaurant during the period between the initial breach and PDQ's discovery of the breach.[42] Within two

---

tional infliction of emotional distress and suggested that mental health issues resulting from the potential for injury could be sufficient. *Id.* at 2211 n.7.

[37] *See id.* at 2211 (explaining that the injury that results from the risk is the concrete injury, not the risk itself). The Court provided an example of a reckless driver on the road: although the driver has placed others at a risk of harm, there is no concrete harm unless the driver crashes into someone. *Id.*

[38] *Compare* Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 693–94 (7th Cir. 2015) (conferring standing to victims of a data breach for an elevated risk of identity theft), *with* Beck v. McDonald, 848 F.3d 262, 276–78 (4th Cir. 2017) (rejecting standing for victims of a data breach alleging an elevated risk of identity theft).

[39] *See* 141 S. Ct. at 2210 (clarifying that *Clapper* involved a suit for injunctive relief rather than damages).

[40] Tsao v. Captiva MVP Rest. Partners, LLC (*Tsao I*), No. 8:18-cv-1606-T-02SPF, 2018 WL 5717479, at *1 (M.D. Fla. Nov. 1, 2018), *aff'd*, 986 F.3d 1332 (11th Cir. 2021); *see* Plaintiff's Class Action Complaint at 7, *Tsao I*, 2018 WL 5717479 (No. 8:18-CV-01606) [hereinafter Complaint] (describing the business conducted by PDQ). PDQ's point of sale system collects the payment card's data and sends it to a payment processor to complete the sale. Complaint, *supra*, at 7–8. The hacker accessed the data through "'an outside technology vendor's remote connection tool.'" *Id.* at 17 (quoting a notice on data breaches PDQ released to customers online). Captiva Restaurant Partners, LLC does business as PDQ. Brief of Plaintiff-Appellant at 1, *Tsao*, 986 F.3d at 1332 (No. 18-14959).

[41] Complaint, *supra* note 40, at 17–18. The credit card information that was breached included the card holder "name[], credit card number[], expiration date[], and cardholder verification value." *Id.* at 18. In PDQ's notice to customers, PDQ claimed that it was unable to ascertain the number of customers whose information or identities were affected. *Id.* at 18.

[42] *See id.* at 6 (describing Tsao's transactions at PDQ during the breach period). Tsao visited a PDQ restaurant twice in October of 2017 in Pinellas, Florida, first using a Wells Fargo Home Rebate card on October 8th and next a Chase Sapphire Reserve card on October 31st. *Id.* Both cards offered points or cash-back rewards for certain purchases. *Id.* at 3, 7. Cardholders collect points when they make certain purchases with the card and may redeem the points on an online portal hosted by the credit issuer. *See*

weeks of the release of PDQ's notice to customers, Tsao filed a putative class action law suit in the United States District Court for the Middle District of Florida.[43] The suit alleged six counts, including negligence in providing adequate security and breach of an implied contract.[44] Plaintiffs claimed that they were at "imminent . . . risk of harm from identity theft and identity fraud" due to the data breach, which compelled them to take steps to reduce the effects of the breach.[45] PDQ moved to dismiss the claim for lack of standing.[46]

In 2018, in *Tsao v. Captiva MVP Restaurant Partners, LLC (Tsao I)*, the district court agreed with PDQ and dismissed Tsao's claim without prejudice for lack of Article III standing.[47] The court held that plaintiffs did not allege a single incident of information misuse and therefore did not allege an imminent injury.[48] Tsao filed an appeal, arguing that the District Court erred in holding that he had not established an injury in fact.[49] To support this, Tsao first cited the elevated possibility of future harm from a hacker's misuse of his stolen data.[50] Second, Tsao argued that he previously incurred concrete injuries as a result of time and money lost mitigating his risk of harm.[51] The Eleventh Cir-

---

What Are Credit Card Points & How Do They Work, CHASE, http://chase.com/personal/credit-cards/education/rewards-benefits/what-are-credit-card-points-and-how-do-they-work [https://perma.cc/67WZ-P4RN] (explaining credit card reward points).

[43] *Tsao I*, 2018 WL 5717479, at *1; Complaint, *supra* note 40, at 1. Tsao filed the suit on behalf of a nationwide class of PDQ customers or, in the alternative, a class of Florida customers. Complaint, *supra* note 40, at 25.

[44] Complaint, *supra* note 40, at 29–44. The other counts included unjust enrichment, negligence per se, and a statutory violation of the Florida Unfair and Deceptive Trade Practices Act for failing to provide adequate cyber security. *Id.* at 36–44; *see* Mank, *supra* note 5, at 1325 (explaining that data breach suits usually include allegations of insufficient data security). *See generally* FLA. STAT. § 501.204 (2021) (making it unlawful to conduct commerce in an unfair manner).

[45] *Tsao*, 986 F.3d at 1335–36 (quoting Complaint, *supra* note 40). The plaintiffs in *Tsao* used the GAO Report to argue that a data breach can lead to identity theft. *Id.* at 1343; *see* U.S. GOV'T ACCOUNTABILITY OFF., *supra* note 4, at 29 (discussing the risks of future identity theft due to a data breach).

[46] Defendant's Motion to Dismiss Plaintiff's Class Action Complaint with Prejudice at 1, *Tsao I*, 2018 WL 5717479 (No. No. 8:18-cv-01606-T-23SPF). PDQ argued that plaintiffs' suit failed under Federal Rules of Civil Procedure 12(b)(1) and 12(b)(6). *Tsao I*, 2018 WL 5717479, at *1; *see* FED. R. CIV. P. 12(b)(1) (stating that a case may be dismissed for "lack of subject matter jurisdiction"); FED. R. CIV. P. 12(b)(6) (stating that a case may be dismissed for "failure to state a claim upon which relief can be granted").

[47] 2018 WL 5717479, at *3.

[48] *Id.* at *2. The district court dismissed the case without prejudice because plaintiffs failed to establish subject matter jurisdiction under Rule 12(b)(1) and failed to state a claim upon which relief could be granted under Rule 12(b)(6). *Id.* at *2 n.1 (quoting DiMaio v. Democratic Nat'l Comm., 520 F.3d 1299, 1302 (11th Cir. 2008)).

[49] Brief of Plaintiff-Appellant, *supra* note 40, at 10.

[50] *Tsao*, 986 F.3d at 1337.

[51] *Id.* Tsao's mitigation costs included the loss of credit card reward points and cash-back rewards when cancelling his cards, restricted access to payment cards and bank accounts, and loss of time spent cancelling and replacing payment cards. *See id.* (summarizing Tsao's claimed injuries). Tsao conceded

cuit heard the case to determine whether the plaintiff's future threat of identity theft or fraud was imminent under the *Clapper* framework.[52] The court held that plaintiffs did not demonstrate a substantial or certainly impending risk and thus did not establish Article III standing.[53]

II. STANDING ON SHAKY GROUND: THE ELEVENTH CIRCUIT JOINS A CIRCUIT SPLIT

In 2007, in *Pisciotta v. Old National Bancorp*, the United States Court of Appeals for the Seventh Circuit took on a novel issue of Article III standing for data breach victims alleging an elevated risk of future injury.[54] In 2013, in *Clapper v. Amnesty International USA*, the United States Supreme Court clarified the standard for threatened injury, which has since guided circuit courts in similar data breach cases.[55] When the Eleventh Circuit heard *Tsao v. Captiva MVP Restaurant Partners, LLC*, the court joined a split comprised of the Second, Third, Fourth, Sixth, Seventh, Eighth, Ninth, and D.C. Circuits.[56] Section

---

that the monetary cost of the harm may not be significant, but argued that the harms inflicted on him were nonetheless real. Plaintiff-Appellant's Reply Brief at 2, *Tsao*, 986 F.3d at 1332 (No. 18-14959).

[52] *See Tsao*, 986 F.3d at 1339 (using the holding from *Clapper v. Amnesty Int'l USA*, that a plaintiff must demonstrate a certainly impending or substantial risk of future injury to establish standing, to decide on Tsao's claims); Clapper v. Amnesty Int'l USA, 568 U.S. 398, 414 n.5 (2013) (providing the "certainly impending" and "substantial risk" standards of proof). The court also took the case to determine if Tsao's steps in mitigating his risk of potential harm were concrete under the *Spokeo, Inc. v. Robins* standard. *See Tsao*, 986 F.3d at 1338 (using the definition of a concrete injury from *Spokeo*, which states that the injury "must actually exist") (quoting Spokeo, Inc. v. Robins, 578 U.S. 330, 340 (2016)).

[53] *Tsao*, 986 F.3d at 1344.

[54] *See* 499 F.3d 629, 634 (7th Cir. 2007) (conferring Article III standing to data breach victims who did not allege actual data misuse). The Seventh Circuit in *Pisciotta* ultimately held that plaintiffs did not suffer a harm which the state law of Indiana could remedy with damages. *Id.* at 639–40.

[55] *See* 568 U.S. at 409**,** 414 n.5 (providing the certainly impending and substantial risk standards); *see*, *e.g.*, *Tsao*, 986 F.3d at 1338–39 (employing the certainly impending and substantial risk standards in a data breach case).

[56] *See* 986 F.3d at 1340 (discussing the divide among circuits that have decided cases of alleged risk of future injury deriving from a data breach); *In re* SuperValu, Inc., 870 F.3d 763, 771–72 (8th Cir. 2017) (denying standing to data breach victims for failure to demonstrate a "substantial risk" of harm); Attias v. Carefirst, Inc., 865 F.3d 620, 629 (D.C. Cir. 2017) (concluding that data breach victims demonstrated a "substantial risk" of injury); Beck v. McDonald, 848 F.3d 262, 276 (4th Cir. 2017) (rejecting standing for data breach victims for failure to demonstrate a "substantial risk" of injury); Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 693 (7th Cir. 2015) (granting standing to data breach victims who demonstrated a "substantial risk" of identity theft); Reilly v. Ceridian Corp., 664 F.3d 38, 42 (3d Cir. 2011) (denying standing to data breaches victims for failure to demonstrate "certainly impending" harm); Krottner v. Starbucks Corp., 628 F.3d 1139, 1143 (9th Cir. 2010) (granting standing, concluding that plaintiffs demonstrated a "credible threat of harm" (quoting Cent. Delta Water Agency v. United States, 306 F.3d 938, 950 (9th Cir. 2002))); Whalen v. Michaels Stores, Inc., 689 F. App'x 89, 90–91 (2d Cir. 2017) (rejecting standing for data breach victims in a summary order); Galaria v. Nationwide Mut. Ins. Co., 663 F. App'x 384, 388 (6th Cir. 2016) (granting standing to data breach victims, concluding that the plaintiffs should not have to delay litigation until experiencing misuse to sue for damages accrued in mitigation).

A of this Part discusses the emergence of a circuit split before *Clapper*.[57] Section B of this Part discusses the cases after *Clapper* and analyzes the decision of the Eleventh Circuit in 2021, in *Tsao*.[58]

A. A Circuit Split Emerges Over the Imminence Requirement for Standing

Before the Supreme Court clarified the imminence requirement of Article III standing in *Clapper*, some circuit courts had already addressed whether a data breach victim has standing to sue based on an elevated risk of injury.[59] For example, in 2010, in *Krottner v. Starbucks Corp.*, the Ninth Circuit granted standing when plaintiffs alleged an elevated risk of identity theft after a thief took a computer holding Starbucks' employees' private information.[60] The court concluded that the unencrypted private information in the hands of a thief created a "credible threat of . . . harm."[61] The court granted standing, holding that plaintiffs demonstrated a threat of injury that was "real and immediate."[62]

In contrast, in 2011, in *Reilly v. Ceridian Corp.*, the Third Circuit denied standing to plaintiffs alleging an elevated risk of identity theft resulting from a data breach.[63] In that case, a hacker breached the payment system at a payroll processing company and accessed employees' private data and bank account information.[64] In denying standing, the court explained that plaintiffs could not demonstrate that the hacker read the stolen personal information, planned to use

---

[57] *See infra* notes 59–66 and accompanying text.

[58] *See infra* notes 67–83 and accompanying text.

[59] *See, e.g.*, *Reilly*, 664 F.3d at 42 (using the "certainly impending" standard to reject standing); *Krottner*, 628 F.3d at 1143 (using a "credible threat of harm" standard to grant standing (quoting *Cent. Delta Water Agency*, 306 F.3d at 950)); *Pisciotta*, 499 F.3d at 634 (holding that the threat of identity theft is sufficient for standing).

[60] 628 F.3d at 1140–41, 1143. The stolen device stored personal information, including Social Security numbers of about 97,000 Starbucks staff members. *Id.* at 1140. Plaintiff Ishaya Shamasa alleged an unknown attempt to open a bank account under his name, but his bank closed it quickly enough to prevent any losses. *Id.* at 1141. Plaintiffs sought damages for taking steps to mitigate the risk, such as enrolling in credit monitoring. *Id.*

[61] *See id.* at 1143 (holding that plaintiffs can establish standing by demonstrating a credible threat of harm that is "real and immediate" rather than "conjectural or hypothetical"); *cf.* Clapper v. Amnesty Int'l USA, 568 U.S. 398, 401–02 (2013) (using the certainly impending standard). The Ninth Circuit derived its credible threat of harm standard from precedent in a prior threatened injury case. *Krottner*, 628 F.3d at 1142–43 (citing *Cent. Delta Water Agency*, 306 F.3d at 950); *see Cent. Delta Water Agency*, 306 F.3d at 950 (granting standing when plaintiff faced a "credible threat of harm").

[62] *Krottner*, 628 F.3d at 1143.

[63] *See* 664 F.3d at 46 (denying victims of a data breach standing for failure to show imminent harm); *cf. Krottner*, 628 F.3d at 1143 (granting standing to victims of a data breach who had yet to experience harm).

[64] *Reilly*, 664 F.3d at 40. The breach affected about 27,000 employees and exposed their name, Social Security number, and, for some, their birth date and banking details. *Id.* No named plaintiffs alleged misuse of their data. *Id.* at 43; *cf. Krottner*, 628 F.3d at 1141 (stating that a named plaintiff alleged that an unknown person attempted to open a bank account under his name).

it, or was able to misuse it.[65] The court concluded that, in light of that unknown information, the plaintiffs could not demonstrate a certainly impending injury.[66]

B. Clapper v. Amnesty International USA *Provides Guidance, but the Split Remains*

Since the Court's clarification on imminence in cases of threatened injury in 2013, in *Clapper v. Amnesty International USA*, circuit courts have applied the *Clapper* framework to cases of data breach with differing outcomes.[67] First, in 2015, in *Remijas v. Neiman Marcus Group, LLC*, the Seventh Circuit decided a case where hackers seized Neiman Marcus customers' credit card information.[68] The hackers then used 9,200 of the 350,000 breached cards.[69] The Seventh Circuit granted standing, holding that plaintiffs demonstrated a "substantial risk" of injury.[70] The court examined the incentives behind a deliberate cyberattack, concluding that the hackers likely acted in order to use the stolen data.[71] The court then concluded that where plaintiffs in *Clapper* had

---

[65] *Reilly*, 664 F.3d at 42–43.

[66] *Id.* at 43. The court employed the "certainly impending" standard from the 1990 Supreme Court case *Whitmore v. Arkansas*. *Id*. at 42 (quoting Whitmore v. Arkansas, 495 U.S. 149, 158 (1990)); *see also Clapper*, 568 U.S. at 401 (stating that the "certainly impending" standard is well-established).

[67] *Compare* Beck v. McDonald, 848 F.3d 262, 276 (4th Cir. 2017) (concluding that data breach victims did not demonstrate a "substantial risk" of injury), *with* Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 693 (7th Cir. 2015) (concluding that data breach victims demonstrated a "substantial risk" of injury). *See generally Clapper*, 568 U.S. 398 (clarifying the imminence requirement in cases of alleged future injury).

[68] 794 F.3d at 690. Although the hackers accessed the credit card information of shoppers, they did not obtain identifying private information. *Id.*

[69] *Id.* In *Beck v. McDonald*, the court concluded that plaintiffs' contention that 33% of breach victims would suffer from identity theft did not constitute a "substantial risk" of injury. 848 F.3d at 275–76. Nevertheless, the court in *Remijas* concluded that there was a "substantial risk" of injury when hackers used 9,200 out of 350,000 cards, which amounted to 2.6% of breach victims. *See Remijas*, 794 F.3d at 690 (detailing that thieves misused 9,200 of 350,000 stolen cards). The court's discussion of the circuit split in *Tsao* suggests that there may be a difference between alleging that a certain percentage of victims will experience harm and alleging harm to actual victims. *See* Tsao v. Captiva MVP Rest. Partners, LLC, 986 F.3d 1332, 1340 (11th Cir. 2021) (stating that meritorious suits for an elevated risk of identity theft often allege documented misuse or access to identifying information of some victims' data). *Compare Beck*, 848 F.3d at 275–76 (concluding that there was not a "substantial risk" of injury when plaintiffs contended that 33% of victims would experience identity theft but where no misuse had yet occurred), *with Remijas*, 794 F.3d at 690, 693 (concluding victims faced a "substantial risk" of injury when thieves used 2.6% of stolen cards).

[70] *Remijas*, 794 F.3d at 693. Before addressing the plaintiffs who had not experienced misuse, the court began by disregarding Neiman Marcus's opposition to the standing of the 9,200 card users with fraudulent charges. *See id.* at 692 (stating that there is "no merit" in contesting the standing of those 9,200 users).

[71] *Id.* at 693. The court in *Remijas* inferred that hackers' ultimate goal from a targeted data breach would be to use the intercepted data to commit identity theft or fraud. *See id.* (posing the question of what other motives hackers would have for stealing the private information of shoppers). The court also inferred that there was a real risk of harm from Neiman Marcus's offer to provide "one year of [free] credit monitoring" services to patrons who shopped during the breach period. *Id.* at 694. The

only suspected that their communications could be targeted, plaintiffs in *Remijas* had evidence of actual access and misuse.[72]

In 2021, in *Tsao v. Captiva MVP Restaurant Partners, LLC*, the Eleventh Circuit used the *Clapper* framework to hold that evidence of a data breach alone is insufficient to demonstrate an "imminent risk of identity theft."[73] In coming to this conclusion, the Eleventh Circuit first noted that courts have generally only granted standing for an elevated risk of identity theft when plaintiffs had alleged incidents of documented misuse or access to class members' identifying information.[74] The court then discussed the two key findings of the 2007 United States Government Accountability Office Report (GAO Report) on data breaches: (1) that hackers generally cannot open a new account using a person's credit card information without also having accompanying personal information; and (2) that the majority of breaches do not lead to identity theft or fraud.[75]

Even without the GAO Report, the court stated that Tsao failed to demonstrate imminent harm for three reasons.[76] First, the court concluded that Tsao's accusation of an elevated risk of harm lacked facts that demonstrated how victims of the PDQ breach were at risk of identity theft.[77] Second, the court stated

---

court in *Beck* rejected this idea, concluding that the inference would deter companies from providing helpful services. 848 F.3d at 276.

[72] *Remijas*, 794 F.3d at 693; *see Clapper*, 568 U.S. at 414 (stating that plaintiffs could only speculate as to whether their communications would be monitored).

[73] *See* 986 F.3d at 1345 (holding that plaintiff did not establish a "substantial risk" or "certainly impending" harm).

[74] *Id.* at 1340. *Compare* Reilly v. Ceridian Corp., 664 F.3d 38, 42 (3d Cir. 2011) (denying standing because the court could not determine whether hackers had the capacity or intended to misuse the breached information), *with Remijas*, 794 F.3d at 693 (granting standing, finding no reason to guess whether the hackers could or intended to use the stolen information). The court in Tsao stated that the Seventh Circuit's decision in *Pisciotta v. Old National Bancorp* was an "outlier" in granting standing without some evidence of misuse. *Tsao*, 986 F.3d at 1340; *see* Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629, 634 (7th Cir. 2007) (granting standing to data breach victims where no plaintiffs alleged actual misuse). Notably, the Seventh Circuit decided *Pisciotta* before the Supreme Court heard *Clapper*. *See Clapper*, 568 U.S. at 401, 414 n.5 (holding that a threatened injury must be "certainly impending" or at a "substantial risk"); *Pisciotta*, 499 F.3d at 634 (granting standing to victims of a data breach alleging future risk without using the certainly impending or substantial risk framework).

[75] *Tsao*, 986 F.3d at 1343; *see In re* SuperValu, Inc., 870 F.3d 763, 771 (8th Cir. 2017) (noting that four out of the twenty-four biggest data breaches from January 2000 to June 2005 led to identity theft, and that three led to identity fraud) (citing U.S. GOV'T ACCOUNTABILITY OFF., *supra* note 4, at 24–25).

[76] *See Tsao*, 986 F.3d at 1343 (acknowledging that the Government Accountability Office had issued the GAO Report over ten years previously at the time and that some data breaches can be more threatening than others).

[77] *See id.* (stating that plaintiff's alleged facts about unspecific dangers of data breach were not enough to demonstrate imminent harm in his case). The court relied on the holding in *Muransky v. Godiva Chocolatier, Inc.*, where the Eleventh Circuit held that "conclusory allegations of an 'elevated risk of identity theft'. . . '[are] simply not enough' to confer standing." *Id.* (alteration in original) (quoting Muransky v. Godiva Chocolatier, Inc., 979 F.3d 917, 933 (11th Cir. 2020)); *see Muransky*, 979 F.3d at

that plaintiffs' failure to provide evidence of actual misuse of stolen information or identity theft among PDQ customers weakened their case.[78] Third, the court held that, by closing his credit cards, Tsao had already prevented the possibility of credit card misuse.[79] The court thus held that Tsao did not establish standing by alleging an elevated possibility of identity theft.[80] Because the plaintiffs in *Tsao* failed to establish that identity theft was imminent, the court concluded that Tsao's steps to mitigate his risk of harm could not confer standing.[81]

After the decision in *Tsao*, in 2021, in *McMorris v. Carlos Lopez & Associates, LLC*, the Second Circuit held that courts should evaluate three factors to resolve whether a plaintiff has established Article III standing in elevated risk of identity theft cases.[82] The court considered: first, whether there was a directed effort to access the data; second, whether other victims of the breach experienced misuse; and third, whether the kind of information that was compromised rendered the victims at an increased threat of harm.[83]

III. The Eleventh Circuit's Correct Conclusion Using a Framework That Is No Longer Current

In 2021, in *Tsao v. Captiva MVP Restaurant Partners, LLC*, the Eleventh Circuit came to the correct decision using a framework that may no longer be

933 (concluding that plaintiffs alleging an elevated risk of harm who failed to demonstrate the degree of risk or reason for risk did not establish standing).

[78] *Tsao*, 986 F.3d at 1343–44. Although the court in *Tsao* stated that cases where plaintiffs allege documented misuse of data have done better when challenged for standing, the court did not require a named plaintiff to allege misuse to determine standing. *See id.* (holding that documented misuse is not a requirement for standing in data breach cases); *see* Cotter v. Checkers Drive-In Rests., Inc., No. 19-cv-1386, 2021 WL 3773414, at *5 (M.D. Fla. Aug. 25, 2021) (stating that *Tsao* does not demand allegations of misappropriation from a named plaintiff); *see also* McMorris v. Carlos Lopez & Assocs., LLC, 995 F.3d 295, 300 (2d Cir. 2021) (stating that requiring actual misuse of data would contradict the Supreme Court's holding that plaintiffs can establish standing by demonstrating "certainly impending" harm (citing Susan B. Anthony List v. Driehaus, 573 U.S. 149, 158 (2014))). The *Tsao* court nevertheless stated that plaintiffs will likely struggle to demonstrate a "substantial risk" of identity theft without some proof of data misuse. 986 F.3d at 1344.

[79] *Tsao*, 986 F.3d at 1344. The court noted that thieves could still misuse Tsao's name, but concluded that the "risk [was] not substantial." *Id.*

[80] *See id.* (holding that demonstration of a data breach by itself is insufficient to confer standing).

[81] *See id.* at 1345 (citing Clapper v. Amnesty Int'l USA, 568 U.S. 398, 416 (2013)) (stating that under *Clapper*, plaintiffs cannot establish standing "by inflicting injuries on [themselves]" in preparation for "non-imminent harm").

[82] *See McMorris*, 995 F.3d at 302–03 (explaining that these factors were most commonly discussed by other circuits' data breach cases involving injury in fact as a standing issue). In *McMorris*, a company employee mistakenly sent a companywide email containing private information including employees' "Social Security numbers, home addresses, dates of birth, telephone numbers, educational degrees, and dates of hire." *Id.* at 298.

[83] *Id.* at 301–03. The court concluded that evidence of a hack, misuse, and access to personal data such as Social Security numbers bolstered a theory of standing based on an elevated risk of harm. *Id.*

relevant in similar data breach cases.[84] The Eleventh Circuit correctly applied the *Clapper v. Amnesty International USA* framework in *Tsao* by rejecting an alleged "speculative chain of possibilities" that may lead to future harm.[85] Similar to *Clapper*, the *Tsao* court concluded that the plaintiffs' failure to provide evidence that hackers misused the stolen data undercuts their concept of standing.[86] This conclusion aligns with the Supreme Court's stated hesitance to grant standing when the alleged injury involves speculating how an independent third party will behave.[87] As the Third Circuit in *Reilly v. Ceridian Corp.* noted, without evidence of actual misuse, the court can merely guess as to whether a hacker has the capacity to misuse the stolen data or intends to do so.[88] In contrast, in *Remijas v. Neiman Marcus Group, LLC*, the Fourth Circuit inferred that the hackers could and presumably would misuse the stolen information.[89] The court in *Tsao* wisely acknowledged that the thieves in *Remijas* had already used 9,200 stolen cards, providing the Fourth Circuit with sufficient evidentiary support for such inferences.[90] Finally, the Eleventh Circuit's conclusion that Tsao foreclosed any substantial risk of harm by terminating his credit cards aligns with the findings of the GAO Report.[91] Because the hackers in *Tsao* only gained access to shoppers' credit card information, the findings of the GAO Report suggest that Tsao was at almost no risk of identity theft or fraud without additional information.[92]

---

[84] *See* 986 F.3d at 1343; (holding that victims of a data breach seeking damages did not allege a substantial risk of harm); *cf.* TransUnion LLC v. Ramirez, 141 S. Ct. 2190, 2210 (2021) (distinguishing substantial risk as a standard for injunctive relief rather than damages).

[85] *See* Clapper v. Amnesty Int'l USA, 568 U.S. 398, 410, 414 (2013) (holding that a theory of standing that alleges an "attenuated chain of possibilities" does not meet Article III conditions); *Tsao*, 986 F.3d at 1343 (stating that Tsao did not demonstrate how he was at a "'substantial risk' of harm" (citing *Clapper*, 568 U.S. at 409, 414 n.5)).

[86] *Tsao*, 986 F.3d at 1344; *see Clapper*, 568 U.S. at 411 (citing Am. C.L. Union v. Nat'l Sec. Agency, 493 F.3d 644, 655–56, 673–74 (6th Cir. 2007)) (stating that plaintiffs' failure to provide evidence of actual surveillance gave support to the conclusion that plaintiffs' standing theory rested on government surveillance of individuals that were not members of the class).

[87] *See Clapper*, 568 U.S. at 413 (stating that the Court has historically been disinclined to allow standing based on theories that force the court to guess how a non-party would act).

[88] *See* 664 F.3d 38, 42 (3rd Cir. 2011) (concluding that plaintiffs' claims were based on theoretical actions by an unknown third party).

[89] 794 F.3d 688, 693 (7th Cir. 2015) (stating that the presumed purpose of hacking a store's database for customers' personal data is to use their payment cards unlawfully or steal their identity).

[90] *See id.* at 693–94 (stating that thieves used 9,200 stolen cards *so far*); *Tsao*, 986 F.3d at 1340 (stating that cases granting standing to plaintiffs that had not alleged misuse usually had some victims experience actual misuse).

[91] *See Tsao*, 986 F.3d at 1344 (stating that any remaining threat of injury resulting from the data breach could only be hypothetical); U.S. GOV'T ACCOUNTABILITY OFF., *supra* note 4, at 30 (stating that identity theft is typically thought to be more injurious to consumers than fraudulent use of a payment card).

[92] *See Tsao*, 986 F.3d at 1344 (stating that Tsao "effectively eliminate[ed]" his risk of credit card fraud and had, at most, a purely theoretical risk of identity theft); U.S. GOV'T ACCOUNTABILITY OFF., *supra* note 4, at 30 (stating that credit or debit card data by itself usually cannot allow a hacker or thief

Circuits rejecting standing to data breach victims that have not alleged misuse also appear correct in light of *TransUnion LLC v. Ramirez*.[93] By distinguishing *Clapper* as a framework for suits seeking injunctive relief, the Supreme Court will likely require victims of a data breach to allege a harm outside of a mere elevated risk of future injury.[94] The Court in *TransUnion* did not explicitly reject the *Clapper* framework for damages suits resulting from a data breach.[95] Nevertheless, the holding in *TransUnion* suggests that plaintiffs alleging risk of harm from a data breach will need to demonstrate a concrete harm resulting purely from that risk to establish standing.[96] At the very least,

---

to create new accounts); *see also* McMorris v. Carlos Lopez & Assocs., LLC, 995 F.3d 295, 303 (2d. Cir. 2021) (holding that courts should evaluate whether the kind of information stolen increases the potential for identity theft).

[93] *See* 141 S. Ct. 2190, 2211 (2021) (clarifying that plaintiffs alleging threats of future injury must demonstrate a current, concrete injury). *See generally* Alexander R. Bilus & Erik VanderWeyden, *After* TransUnion*, Lower Courts Grapple with Article III Standing in Data Breach Lawsuits*, SAUL EWING ARNSTEIN & LEHR LLP (Feb. 15, 2022), https://www.saul.com/publications/alerts/after-transunion-lower-courts-grapple-article-iii-standing-data-breach-lawsuits [https://perma.cc/Z6CG-ZTU9] (discussing the impact of *TransUnion* on data breach standing cases); Avi Gesser & Johanna N. Skrzypczyk, *The Supreme Court* TransUnion *Case Part 1—What It Means for Standing in Cyber Cases*, Debevois & Plimpton (July 8, 2021), https://www.debevoisedatablog.com/2021/07/07/standing-in-data-breach-class-actions-where-things-stand-after-transunion/ [https://perma.cc/M65S-WMVC] (same).

[94] *See TransUnion* at 2211 & n.7 (stating that TransUnion provided a convincing argument that the simple threat of injury by itself is not an injury in fact unless a concrete harm, such as emotional distress, results from that risk). In some cases involving threat of harm from data breaches, plaintiffs have alleged emotional distress as a concrete injury. *See* Reilly v. Ceridian Corp., 664 F.3d 38, 45–46 (3d Cir. 2011) (rejecting standing for data breach victims alleging emotional distress); Krottner v. Starbucks Corp., 628 F.3d 1139, 1142 (9th Cir. 2010) (holding that a data breach victim's "generalized anxiety and stress" were enough to meet standing requirements). In 2022, in *Desue v. 20/20 Eye Care Network, Inc.*, the United States District Court for the Southern District of Florida held that victims of a data breach who alleged emotional distress as a result of their "substantial risk of future harm" established injury in fact, within the *TransUnion* framework, in their suit for damages. No. 21-CIV-61275, 2022 WL 796367, at *5 (S.D. Fla. Mar. 15, 2022).

[95] *See TransUnion*, 141 S. Ct. at 2211–12 (concluding that in addition to the essential issues with allegations of future risk, plaintiffs did not demonstrate an adequate threat of injury).

[96] *See id.* (stating that the mere threat of an injury is not concrete); *see also* Maddox v. Bank of N.Y. Mellon Tr. Co., N.A., 19 F.4th 58 (2d Cir. 2021) (rejecting standing by applying *TransUnion* to a suit for damages for a risk of future harm); *In re* Practicefirst Data Breach Litig., No. 21-CV-00790, 2022 WL 354544, at *4 (W.D.N.Y. Feb. 2, 2022) (applying *TransUnion* to a data breach case but declining to decide whether *TransUnion* modifies the *McMorris v. Carlos Lopez & Associates, LLC* test); Kale v. Procollect, Inc., 547 F. Supp. 3d 793, 797–98 (W.D. Tenn. 2021) (explaining that the Court's clarification in *TransUnion*—that *Spokeo, Inc. v. Robins* did not establish that simply the threat of injury meets the requirements for standing in a damages suit—modifies Sixth Circuit precedent on threats of future injury). *But see* Coffey v. OK Foods Inc., No. 21-CV-02200, 2022 WL 738072, at *3 (W.D. Ark. Mar. 10, 2022) (granting standing to a data breach victim alleging an elevated risk of future harm and distinguishing the case from *TransUnion* because the plaintiff received notice of credit inquiries indicating an attempt at identity theft); Cotter v. Checkers Drive-In Rests., Inc., No. 19-cv-1386, 2021 WL 3773414, at *4 (M.D. Fla. Aug. 25, 2021) (distinguishing *TransUnion* from a data breach case using the elevated risk of injury theory of standing because: (1) *TransUnion* considered statutory damages instead of compensatory damages; and (2) *TransUnion* was not heard at

the holding in *TransUnion* suggests that the Court will apply a more narrow interpretation of substantial risk of harm, giving weight to circuits that rejected standing where plaintiffs did not demonstrate data misuse.[97]

CONCLUSION

In 2021, in *Tsao v. Captiva MVP Restaurant Partners LLC*, the Eleventh Circuit joined a circuit split by holding that victims of a data breach that had yet to experience misuse of their data were not at an imminent risk of injury. In doing so, the Eleventh Circuit sided with the Second, Third, Fourth, and Eighth Circuits in rejecting standing based on evidence of a mere data breach. Although the Eleventh Circuit properly concluded that the plaintiffs had failed to demonstrate an imminent risk of injury, such a conclusion may not be necessary in future data breach cases. This is so because of the Supreme Court's decision in 2021, in *TransUnion LLC v. Ramirez*, which clarified that plaintiffs may establish standing through an imminent risk of injury in suits for injunctive relief. In contrast, the suit in *Tsao*, as with many other suits involving data breaches, sought compensatory damages. Given the Supreme Court's trend towards narrowing standing eligibility in recent years, the Eleventh Circuit's decision in *Tsao* will likely align with standing jurisprudence in future cases.

JOHN LANDZERT

---

the pleading stage); *In re* Blackbaud, Inc., Customer Data Breach Litig., No. 20-mn-02972, 2021 WL 2718439, at *6 n.15 (D.S.C. July 1, 2021) (distinguishing *TransUnion* from a motion to dismiss for lack of Article III standing in a data breach case because *TransUnion* involved a case with a jury verdict).

[97] *See TransUnion* at 2212–13 (holding that only plaintiffs whose information was shared with businesses established a concrete harm); Spokeo, Inc. v. Robins, 578 U.S. 330, 341 (2016) (holding that a simple procedural violation does not necessarily establish the injury in fact condition even when it is a violation of a statute). The Court's holding in *Spokeo* hampers the ability of Congress to enact a remedy for plaintiffs in federal court. Peter C. Ormerod, *A Private Enforcement Remedy for Information Misuse*, 60 B.C. L. REV. 1893, 1896 (2019). Instead, states will likely have to create legal remedies for data breaches in order to incentivize companies to protect personal data. *Id.*; *see Spokeo*, 578 U.S. at 341 (stating that the violation of a statute does not necessarily meet the injury in fact component of standing).