University of Miami Law Review

Volume 77 | Number 2 Article 3

2-20-2023

Standing up to Hackers: Article III Standing for Victims of Data Breaches

Kendall Coffey
Coffey Burlington, PL.

ARTICLES

Standing up to Hackers: Article III Standing for Victims of Data Breaches

KENDALL COFFEY*

Despite the increasing amount of data breaches, there is no liability for parties who do not adequately protect victim's information. In federal court, plaintiffs must show that their injury was concrete, particularized, and imminent. But, when plaintiffs' information has been stolen, but not yet criminally used, they may be unable to establish a right to relief. Victims face challenges when seeking damage for this future harm, because despite their destroyed privacy, they may not have evidence of a perpetrator's actual misuse of purloined data. This Article analyzes multiple court decisions, generally in the setting of class-actions, and discusses outcomes of data breach litigation. It then considers whether some courts have embraced an overly restrictive view of standing in these cases.

* Founding member and partner, Coffey Burlington, PL.

INTRODUCTION

The relentless onslaught of data breaches has become so commonplace that, as one judge described it, "[t]here are only two types of companies left in the United States, according to data security experts: 'those that have been hacked and those that don't know they've been hacked.'"[1] As another court described this spiraling phenomenon, "[t]hough variously defined by governments and private organizations, the term 'data breach' generally encompasses any security incident in which sensitive, protected or confidential data is copied, transmitted, accessed, viewed, stolen or used by an individual unauthorized to do so."[2] Despite the frequency and ubiquitous reach of data breaches, there is no federal regime for allocating liability for damages.[3] While a framework of federal and state criminal laws applies to the perpetrators who criminally access confidential information,[4] there is no uniform system for accountability for parties who negligently fail to erect safeguards to prevent hacking.[5] As a result, courts around the country have applied common law principles and, in some cases, state statutes to address civil liabilities for the responsible parties.[6] The theories of recovery have

---

[1] Storm v. Paytime, Inc., 90 F. Supp. 3d 359, 360 (M.D. Pa. 2015).

[2] Blahous v. Sarrell Reg'l Dental Ctr. for Pub. Health, Inc., No. 2:19-CV-798-RAH-SMD, 2020 WL 4016246, at *1 (M.D. Ala. July 16, 2020). In Tsao v. Captiva MVP Rest. Partners, LLC, 986 F.3d 1332, 1343 (11th Cir. 2021), the court noted reports indicating "that identity thieves have stolen $112 billion in the last six years."

[3] See Thorin Kolowski, *The State of Consumer Data Privacy Laws in the US (And Why It Matters)*, N.Y. TIMES (Sept. 6, 2021), https://www.nytimes.com/wirecutter/blog/state-of-privacy-laws-in-us/.

[4] Computer Fraud and Abuse Act of 1986, 18 U.S.C. § 1030(a); *see, e.g.*, Van Buren v. United States, 141 S. Ct. 1648, 1652 (2021); FLA. STAT. § 815 (2022) (regarding computer hacking and fraud); 18 U.S.C. § 1028 (regarding identity theft); FLA. STAT. § 817.568 (2022) (regarding identity theft).

[5] Attias v. CareFirst, Inc., 865 F.3d 620, 623 (D.C. Cir. 2017) (noting that the complaint "raised eleven different state law causes of action, including breach of contract, negligence, and violation of various state consumer-protection statutes").

[6] Because state laws are usually the substantive vehicle for recovery, data breach victims may confront state doctrines of limitation such as the economic

included negligence, implied and express contracts,[7] fiduciary duty, and statutory remedies. In some cases, employees may allege that their employer was given confidential information as a condition of employment and, thereby, established a duty of care to protect that information.[8]

In constructing the damages component, some plaintiffs have asserted emotional stress arising from the exposure or misuse of private information[9] in addition to the monetary expenses of mitigation, such as purchasing insurance and monitoring services to guard against identity theft.[10] Even the time and trouble of dealing with the

---

loss rule. When applicable, this principle provides that parties in a contractual relation cannot sue for negligence "solely in economic damages unaccompanied by physical injury or property damage." Dittman v. Univ. of Pittsburgh Med. Ctr., 196 A.3d 1036, 1049 (Pa. 2018). In *Dittman*, the Supreme Court of Pennsylvania found that the economic loss rule did not preclude the data breach claims but acknowledged that other state courts have applied the doctrine to dismiss data breach claims. *Id.* at 1050. State laws also address whether the actions of a criminal can operate as a superseding cause that relieves the defendant of its liability for negligence. *Id.* at 1042. Because the consequences of criminality by hackers is increasingly foreseeable, though, courts have generally declined to reject negligence claims on this basis. *See id*. at 1050.

[7] In Torres v. Wendy's Int'l, LLC, No. 6:16-cv-210-Orl-40DCI, 2017 WL 8780453, at *1 (M.D. Fla. Mar. 21, 2017), Wendy's customers sued after hackers used malicious software to gain access to Wendy's computers to steal payment card data. The court found that, when a customer uses a credit card with a merchant, there can be "an implicit agreement to safeguard the data necessary to effectuate the contract." *Id.* at *3 (quoting Anderson v. Hannaford Bros. Co., 659 F.3d 151, 159 (1st Cir. 2011)); *see* Smahaj v. Retrieval-Masters Creditors Bureau, Inc., 69 Misc.3d 597, 607 (Sup. Ct. Westchester Cty.) (recognizing express contracts as a theory of recovery for data breach)); *see* Jones v. Com. BanCorp, Inc., No. 06 Civ 835(HB), 2006 WL 1409492 (S.D.N.Y. May 23, 2006) (recognizing cause of action under negligence and fiduciary duty); *see Attias*, 865 F.3d at 623 (raising various state law consumer-protection claims).

[8] *See Dittman*, 196 A.3d at 1048.

[9] Krottner v. Starbucks Corp., 628 F.3d 1139, 1142 (9th Cir. 2010) ("[Plaintiff's] allegation that he 'has generalized anxiety and stress' as a result of the laptop theft . . . is sufficient to confer standing.").

[10] *See* Katz v. Pershing, 672 P3d 64, 79 (1st Cir. 2012). As one court observed, "[i]n recent years, a growing number of courts have recognized that the purchase of credit monitoring services and the costs to deal with fraudulent activity following the theft of PII [personal identifying information], when spent with knowledge that stolen information has already been misused can constitute recognizable injuries." Portier v. NEO Tech. Sols., No. 3:17-cv-30111-TSH, 2019 WL 7946103, at *15 (D. Mass. Dec. 31, 2019).

aftermath of a breach has been claimed.[11] However, unless a substantial risk of identity theft or other comparable harm can be established, most courts are not inclined to equate injury-in-fact to the time and money spent monitoring or changing plaintiffs' financial information and accounts.[12] Yet another theory of damages is the claim of the "benefit of bargain" based on the premise that because a financial services company provided inadequate data security, it failed to fully earn its fees.[13] Because victims whose data privacy has been violated may not suffer sufficient individual injury to justify the substantial expense of litigation, many of these cases are initiated in federal court and enlist a multitude of claimants in order to utilize the class-action mechanism.[14]

Commonly, though, even after a data breach has been verified, there may be no evidence that confidential data has been exploited by, for example, a perpetrator's attempts to use a victim's credit card or to file tax returns in the victim's name. When data breach cases are filed in federal court with evidence of stolen data rather than stolen money, victims may struggle to establish the prerequisites for standing.[15] The federal requirement for standing under Article III of the U.S. Constitution hinges on subject matter jurisdiction since only a "case or controversy" may be litigated in federal court.[16] As a result, future harm presents a constitutional dilemma. The current

---

[11] Although indicating that "wasted time and effort" could at times establish a concrete harm, that assertion rises and falls with the substantiality of risk of future harm. Tsao v. Captiva MVP Rest. Partners, LLC, 986 F.3d 1332, 1344 (11th Cir. 2021).

[12] *See* Dieffenbach v. Barnes & Noble, Inc., 887 F.3d 826, 828 (7th Cir. 2018). *But see* McMorris v. Carlos Lopez & Assocs., LLC, 995 F.3d 295, 299 (2d Cir. 2021) (finding no allegations that data was misused or compromised as the result of an intentionally targeted theft).

[13] *Katz*, 672 F.3d at 76 ("By this, she means that she is paying more to NPC than the (less secure) service . . . is actually worth. It is a bedrock proposition that 'a relatively small economic loss—even an "identifiable trifle"—is enough to confer standing.'" (quoting Adams v, Watson, 10 F.3d 915, 924 (1st Cir. 1993))).

[14] *See* Beck v. McDonald, 848 F.3d 262, 267 (4th Cir. 2017).

[15] *See Tsao*, 986 F.3d at 1345.

[16] Some state courts, including New York state courts, apply limitations on standing that parallel the U.S. Constitutional doctrine. *See*. Keach v. BST & Co. CPAS, LLP, No. 903580-20, 2021 WL 1203026, at *3–4 (N.Y. Sup. Ct. Mar. 30, 2021).

federal jurisprudence requires that the injury be "concrete, particularized, and actual or imminent; fairly traceable to the challenged action; and redressable by a favorable ruling."[17] Federal data breach cases are often confronted by a standing challenge that "primarily concerns the injury-in-fact element which serves to ensure that the plaintiff has a personal stake in the litigation."[18] While victims who suffer an actual incident of identity theft are accorded standing,[19] those whose data has been accessed, but not yet criminally used, may be stranded in litigation limbo—victimized, yet unrecognized as proper plaintiffs.[20] The factual scenarios vary widely based on the nature of the breach, the character of the perpetrator, the type of personal information that was accessed, and the evidence of subsequent misuse experienced by other victims of the same data breach.[21] As a result, while standing to sue has been established in the most compelling cases, for many victims, the right to seek relief is not sustained without evidence of a perpetrator's actual misuse of purloined data.

The broad array of factual scenarios has not lent itself to a single judicial formula for standing. In fact, in an examination of federal appellate decisions, the Eleventh Circuit Court of Appeals observed that the federal appellate circuits were divided on the issue.[22] Similarly, upon its examination of the seemingly divergent views, the

---

[17] Clapper v. Amnesty Int'l USA, 568 U.S. 398, 409 (2012).

[18] Attias v. CareFirst, Inc., 865 F.3d 620, 626 (D.C. Cir. 2017).

[19] *See In Re* SuperValu, Inc., 870 F.3d 763, 772 (8th Cir. 2017) (rejecting plaintiffs' future injury allegations but nonetheless finding one plaintiff had standing after suffering a fraudulent credit card charge).

[20] *See Tsao*, 986 F.3d at 1345 (rejecting standing); *see also* Beck v. McDonald, 848 F.3d 262, 276–77 (4th Cir. 2017) (rejecting standing).

[21] "Cyber-criminals can use W-2 information, including an employee's name, address, and Social Security number, to steal an employee's identity and fraudulently obtain employment, loans, and credit cards and file tax returns in an employee's name." Portier v. NEO Tech. Sols., No. 3:17-cv-30111-TSH, 2019 WL 7946103, at *2 (D. Mass. Dec. 31, 2019). "Cancelling and replacing stolen debit and credit cards limits the damage caused by the theft of debit and credit card information. In contrast, stolen Social Security numbers, which are not usually replaced, have been characterized as the keys to the kingdom for an identity thief." *Id.* at *6.

[22] *See Tsao*, 986 F.3d at 1340 (noting that the Sixth, Seventh, Ninth, and D.C. Circuits recognized standing resulting from data breaches, while the Second, Third, Fourth, and Eighth Circuits rejected standing).

Second Circuit concluded that the disparate results were driven by factual diversities but that "no court of appeals has explicitly foreclosed plaintiffs from establishing standing based on a risk of future identity theft . . . ."[23] However the divergences might be reconciled, it is a critical issue for the many millions who endure unexpected exposure to the tidal wave of cyber crimes.[24]

This Article begins with an overview of court decisions followed by analysis of the key factors that drive outcomes.[25] The focus will be on the leading federal decisions, generally in the setting of class actions.[26] The conclusion will turn to whether some courts have embraced an overly restrictive view of standing in circumstances that may, in fact, be deserving of judicial remedy.[27]

I. THE FEDERAL CIRCUITS TO THE EXPLODING MENACE OF DATA BREACHES

In 2007, a General Accounting Office report ("GAO report") analyzed the accelerating challenges of data breaches and found that identity theft can "encompass[] many types of criminal activities, including a fraud on existing accounts—such as unauthorized use of a stolen credit card number—or fraudulent creation of new accounts—such as using stolen data to open a credit card account in someone else's name."[28] At the time of its issuance, the GAO report found that "[c]omprehensive information on the outcomes of data breaches is not available," but observed that "most breaches have not resulted in detected incidents of identity theft."[29] The reality that

---

[23] McMorris v. Carlos Lopez & Assocs., LLC, 995 F.3d 295, 300 (2d Cir. 2021).

[24] Maxwell Murray, *Stand or Sit? Article III Standing in Cases of Data Breach: A Uniform Solution*, 5 ST. THOMAS J. COMPLEX LITIG. 46, 48 (2019).

[25] *See infra* Section II.

[26] *See id.*

[27] *See infra* Section VI.

[28] 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 2 (2007) [hereinafter GAO REP. NO 07-737].

[29] *Id.* at 21.

privacy is often destroyed but without traceable misuse, has contributed mightily to the widely varying judicial responses to the question of standing.

In 2010, the Ninth Circuit cast its vote in favor of standing in *Krottner v. Starbucks Corp*.[30] Following the theft of a laptop from Starbucks containing the unencrypted names, addresses, and social security numbers of approximately 97,000 Starbucks employees, suit was brought by past and present personnel.[31] The predicate for their injury-in-fact was the increased risk of future harm due to the thief's access to personal identifying information.[32] Finding this to be a "credible threat of real and immediate harm," the Ninth Circuit affirmed the district court, holding that plaintiffs "whose personal information has been stolen but not misused, have suffered an injury sufficient to confer standing . . . ."[33] In reaching its conclusion, the court cited environmental cases in which an exposure to toxic substances would establish "a credible threat of harm" even if no adverse symptoms had yet emerged.[34] In its determination that the risk of future harm could establish standing, the court acknowledged an apparent disagreement with the Sixth Circuit.[35] This would not be the only circuit to disagree with the central thesis of *Krottner*.

In *Reilly v Ceridian Corp.*, the Third Circuit adopted a more restrictive view of future injury as a basis for injury-in-fact.[36] A data hack by an unknown perpetrator prompted law firm employees to sue the payroll processing firm that allegedly failed to adequately protect the names and social security numbers of 27,000 employees at 1,900 companies.[37] In conjunction with law enforcement, the defendant was evidently able to ascertain the information that was apparently accessed by the hacker.[38] The plaintiffs claimed damages that included an increased risk of identity theft, costs to monitor

---

30 Krottner v. Starbucks Corp., 628 F.3d 1339, 1443 (9th Cir. 2010).

31 *Id.* at 1440.

32 *Id.* at 1442–43.

33 *Id.* at 1440, 1443.

34 *See id. at* 1142.

35 *See id.* at 1443 (citing Lambert v. Hartman, 517 F.3d 433, 437 (6th Cir. 2008)).

36 Reilly v Ceridian Corp., 664 F.3d 38, 43 (3d Cir. 2011).

37 *See id.* at 40.

38 *Id.*

credit activity, and emotional distress.[39] In response, the court found the emotional injuries and perceived risk of future harm were too speculative.[40] Because the named plaintiffs did not claim any existing direct loss or assert that they had already been victimized by identity theft, the court found no standing.[41] The Third Circuit rejected the countervailing Ninth Circuit's analysis in *Krottner* as a "skimpy rationale," finding *Krottner*'s analogies to environmental exposure or even medical monitoring to be unpersuasive.[42]

In 2012, the First Circuit in *Katz v. Pershing, LLC*, observed that the appeals courts were in "some disarray" about the increased risk of future harm as constituting the element of injury-in-fact.[43] While acknowledging that even an "identifiable trifle" can suffice, the harm in *Katz* was deemed to be too speculative.[44] The plaintiff had not suffered from the consequences of hacking or even from an accidental disclosure of data.[45] Instead, the issue was the plaintiff's contention that her non-public personal information was inadequately protected against the possibility that future abusers might attempt to access the information.[46] The court found that "despite the dire forebodings in her complaint," her claim was neither imminent nor concrete.[47]

---

[39] *Id.*

[40] *See id.* at 43. By contrast, in 2012, the Eleventh Circuit accorded standing in a data breach case in which data had been used to open bank and brokerage accounts in the victims' names causing actual monetary damages. *See* Resnick v. AvMed. Inc.*,* 693 F.3d 1317, 1322, 1324 (11th Cir. 2012).

[41] *See Reilly*, 664 F.3d at 43. As a district court described this factor, "[f]urthermore, the passage of months, and then, years, only renders any such conjectural threat increasingly less imminent." *See* Blahous v. Sarrell Reg'l Dental Ctr. for Pub. Health, Inc., No. 2:19-cv-798-RAH-SMD, 2020 WL 4016246, at *1, *6 (M.D. Ala. Jul. 16, 2020*)*; *see also In re* Zappos.com, Inc., 108 F. Supp. 3d 949, 958 (D. Nev. 2015) ("[T]he passage of time without a single report from Plaintiffs that they in fact suffered the harm they fear must mean something."); *see* Abernathy v. Brandywine Urology Consultants, P.A., No. N20C-05-057, 2021 WL 211144, at *1 (Del. Super. Ct. Jan. 21, 2021) ("[A]lmost a year ago and Plaintiffs have yet to allege that any of them have become actual victims of identity theft.").

[42] *See Reilly*, 664 F.3d at 44.

[43] Katz v. Pershing, LLC, 672 F.3d 64, 80 (1st Cir. 2012).

[44] *Id.* at 76, 80.

[45] *See id.* at 79.

[46] *See id.*

[47] *See id.* at 79.

II. THE SUPREME COURT AND STANDING FOR FUTURE HARM

Although arising in a different context, in 2013, the Supreme Court in *Clapper v. Amnesty International USA*, significantly impacted the evolving data breach jurisprudence.[48] The issue in *Clapper* was standing to challenge an amendment to the Foreign Intelligence Surveillance Act that would allegedly reduce the legal restrictions upon monitoring communications with foreign terrorism suspects. U.S. citizens challenged the law based on future harm, alleging that they reasonably believed there was a likelihood that their phone conversations could be intercepted.[49] Because the perceived harm was a risk of future injury, however, the Court determined by a five-to-four majority that standing was not present.[50]

In discussing the fundamentals of standing, the Court repeated the premise that, "an injury must be concrete, particularized, an actual or imminent; fairly traceable to the challenged action; and redressable by a favorable ruling."[51] The Court recognized that the government's improper interception of a private telephone or email communication could constitute an injury that is "concrete and particularized."[52] The Court nevertheless found that the risk of future injury for these plaintiffs was too speculative.[53] In its analysis, the Court rejected the test that had been applied by the Second Circuit which found that if there was an "objectively reasonable likelihood" of injury, that likelihood would be sufficient to establish injury-in-fact.[54] In demanding a more substantial risk of future harm, the Court concluded that measures taken and expenditures made by plaintiffs to mitigate future risk could not establish standing unless that future risk was sufficiently concrete and imminent.[55] As the Court emphasized, "respondents cannot manufacture standing by choosing to make expenditures based on hypothetical future harm

---

48 *See* Clapper v. Amnesty Int'l USA, 568 U.S. 398, 408 (2012).
49 *See id.*
50 *See id.* at 422.
51 *See id.* at 409.
52 *See id.* at 410–11.
53 *Id.* at 414.
54 *See id.* at 410.
55 *See id.* at 417.

that is not certainly impending."[56] To be sure, this analysis was lodged in a fundamentally different context than typical data breaches. *Clapper* did not involve the risk of harm by sophisticated criminals who had already hacked into a computer system, but rather it involved the potential risk of improper actions by our own government.[57] Nevertheless, subsequent appeals courts have cited *Clapper* to measure the risks of future criminal activity in data breach cases.

Following *Clapper*, the Fourth Circuit in *Beck v. McDonald* rejected standing for 7,400 patients of a Veterans Affairs Hospital who feared the consequences of a data breach resulting from a stolen laptop.[58] Alleging emotional distress, current mitigation expenses, and substantial future harm from identity theft, the patients attempted to establish the risk of future harm statistically.[59] Their calculations indicated that 33% of those affected by the stolen laptop would have their identities stolen and that, as a class, they suffered a 9.5 times greater risk of identity theft than members of the general public.[60] Along with the increased exposure to future injury, they sought damages for the present need to pay for credit monitoring services.[61] Based on the *Clapper* analysis, though, the Fourth Circuit concluded that the allegations failed "to push the threatened injury of future identity theft beyond the speculative to the sufficiently imminent."[62] Examining the plaintiffs' contention that they faced a 9.5 times greater risk of identity theft, the court found that this was insufficient to establish a "substantial risk" of harm.[63]

Moreover, as in *Clapper*, the court found that a plaintiff's decision to pay for credit monitoring services—in response to what the court determined to be a speculative threat—was an attempt to "manufacture standing merely by inflicting harm upon themselves based on their fears of [a] hypothetical future."[64] Just as *Clapper*

---

56 *Id.* at 402.
57 *See id.* at 414.
58 Beck v. McDonald, 848 F.3d 262, 267 (4th Cir. 2017).
59 *See id.* at 267, 368.
60 *Id.* at 368.
61 *See id.* at 276.
62 *See id.* at 274.
63 *See id.* at 268, 275.
64 *See id.* at 272 (quoting Clapper v. Amnesty Int'l USA, 568 U.S. 398, 402 (2012)).

found that mitigation payments could not be justified if jeopardies were speculative, the court in *Beck* rejected such payments as present damages describing it as a "repackaged version" of the claim for damages based on future harm.[65]

The Supreme Court's decision in *Clapper* was also relied on by the Eleventh Circuit in *Tsao v. Captiva MVP Restaurant Partners, LLC*.[66] In an action by customers against a restaurant chain, the court followed the principle that injury-in-fact for purposes of standing requires that the future injury must be "either 'certainly impending' or [that] there is a 'substantial risk' of such harm."[67] In *Tsao*, the data breach entailed credit card information—not Social Security numbers ("SSNs")—and no misuse of any cards had yet materialized.[68] In its analysis, the court in *Tsao* looked to *SuperValu*,[69] and cited to a GAO report that found without the relevant SSNs, credit card information "generally cannot be used alone to open unauthorized new accounts."[70] As the GAO report observed, "[t]he type of data compromised in a data breach can effectively determine the potential harm that can result."[71] Accordingly, in assessing the victim's exposure when only credit card information is disclosed, the court found the theory of injury to be overly speculative and therefore rejected standing.[72] As with *Clapper* and the Fourth Circuit's data breach holding in *Beck*, the court held that a victim's expenses for credit monitoring in the face of a speculative threat could not establish standing because "a plaintiff cannot conjure standing by inflicting some direct harm on itself to mitigate a perceived risk."[73]

---

[65] *See Beck*, 848 F.3d. at 276–77.

[66] Tsao v. Captiva MVP Rest. Partners, LLC, 986 F.3d 1332, 1339 (11th Cir. 2021).

[67] *Id.* at 1339 (quoting *Clapper*, 568 U.S. at 1147).

[68] *See* Whalen v. Michaels Stores, Inc., 689 F. App'x 89, 90 (2d Cir. 2017) (finding that without SSNs, credit card data is generally perceived to be less susceptible to identity theft).

[69] *Tsao*, 986 F.3d at 1342 (citing *In Re* SuperValu, Inc., 870 F.3d 763, 769–71 (8th Cir. 2017)).

[70] *Id.* (quoting GAO REP. NO 07-737, *supra* note 28, at 30).

[71] *In re* SuperValu, Inc., 870 F.3d at 770 (quoting GAO REP. NO 07-737, *supra* note 28, at 30).

[72] *Tsao*, 986 F.3d at 1339.

[73] *Id.* at 1339.

While also citing to *Clapper's* standards, the court in *Attias v. CareFirst, Inc.*[74] allowed standing for customers of health insurance companies following a cyber-attack. In *Attias*, the court found a substantial risk of future injury because the sensitive nature of personal identifying information, including credit card data, and SSNs, created a high risk of future financial fraud.[75] As the court in *Attias* observed, "it is much less speculative—at the very least, it is plausible—to infer that this party [the perpetrator] has both the intent and the ability to use that data for ill."[76]

Also following *Clapper* was *McMorris v. Carlos Lopez & Associates*.[77] In that case, standing was rejected for potential victims of an inadvertent disclosure.[78] The defendant was a health care provider for veterans that accidentally sent an email to each of sixty-five employees providing sensitive personal information about all the others.[79] Fortunately, it did not appear that any misuse followed the accidental disclosure.[80] Emphasizing the lack of evidence of misuse, as well as the unintentional character of the data breach, the court found that to allow standing would be to "string together a lengthy 'chain of possibilities.'"[81] Moreover, like the Supreme Court held in *Clapper*, the Second Circuit found a plaintiff "cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending."[82]

Intriguingly, *Clapper* did not influence the Seventh Circuit's decision in *Dieffenbach v. Barnes & Noble, Inc*.[83] *Dieffenbach* concerned litigation by customers of Barnes & Noble after "scoundrels

---

[74] *See* Attias v. CareFirst, Inc., 865 F.3d 620, 626 (D.C. Cir. 2017).

[75] *Id.* at 628–29.

[76] *Id.* at 628.

[77] McMorris v. Carlos Lopez & Assocs., LLC, 995 F.3d 295 (2d Cir. 2021).

[78] *Id.* at 303.

[79] *Id.* at 297–98.

[80] *Id.* at 298–99.

[81] *Id.* at 304 (quoting Clapper v. Amnesty Int'l USA, 568 U.S. 398, 410 (2012)).

[82] *Id.* at 303 (quoting *Clapper*, 568 U.S. at 416).

[83] *See* Dieffenbach v. Barnes & Noble, Inc., 887 F.3d 826, 828 (7th Cir. 2018).

had compromised some of the machines" containing payment information.[84] The purloined data did not include SSNs or dates of birth ("DOBs") but rather customers' names, card numbers, expiration dates, and PINs.[85] Applying the state laws of California and Illinois, the court validated standing and injury-in-fact by virtue of the expenditures of credit-monitoring services, as well as the time value of money lost when unauthorized withdrawals occurred and credits had to be restored.[86] The court further recognized that the "value of one's own time needed to set things straight is a loss from an opportunity-cost perspective."[87] In focusing on state law principles of damages, the court observed that "[t]here are innumerable ways in which economic injury . . . may be shown."[88] While emphasizing that a "trifling loss suffices under California law," the court concluded that losing the use of funds for three days may be trifling for some, but "to others it may be a calamity . . . ."[89] Perhaps because of California's more flexible principles of damages, the court did not cite the Supreme Court's decision in *Clapper* and did not address *Clapper's* restrictions on future harm as a predicate for injury-in-fact.[90]

In 2021, the Supreme Court further examined the availability of standing for future harm in *TransUnion LLC v. Ramirez*.[91] In *TransUnion*, 8,185 consumers sued the credit reporting agency for falsely indicating that the consumers' name was a "potential match" to names on a list maintained by the Office of Foreign Assets Control, a list that included terrorists, drug traffickers and other criminals.[92] The misleading credit reports were challenged as violations of the

---

[84] *Id.* at 827.

[85] *Id.*

[86] *Id.* at 828–30.

[87] *Id.* at 827.

[88] *Id.* at 829 (quoting Kwikset Corp. v. Superior Court, 246 P.3d 877, 885 (Cal. 2011)).

[89] *Id.* at 829.

[90] *See id.*

[91] TransUnion LLC v. Ramirez, 141 S. Ct. 2190, 2203 (2021). The four Justice dissent was led by Justice Clarence Thomas. *Id.* at 2214 (Thomas, J., dissenting).

[92] *Id.* at 2200–01.

Fair Credit Reporting Act ("FCRA").[93] For roughly twenty-five percent of the class, the Court ruled that those members suffered a cognizable injury-in-fact because those misleading reports had been disseminated to third parties.[94] But for the other seventy-five percent, the Court concluded that no concrete harm could be found where misleading credit information had been collected by TransUnion in its credit files but not conveyed to third-party businesses.[95]

Significantly, even though the Congressional enactments of FCRA had clearly provided remedies for inaccurate credit information, Article III became an obstacle to the will of Congress for the majority of victims because "Article III standing requires a concrete injury even in the context of a statutory violation."[96] As the Court viewed the standing issue: "No concrete harm, no standing."[97] Rather than accept the Congressional determination that compiling inaccurate credit about a consumer standing alone constituted a remediable injury, the Court looked to whether the injury had precedents in a "historical or common law analog where the mere existence of inaccurate information, absent dissemination, amounts to concrete injury."[98] Finding that publication to a third-party was an essential element of common law defamation, the Court found that Congress could not enact a remedy for the majority of class members whose inaccuracies had, after seven months, appeared only in the files of TransUnion.[99]

Justice Clarence Thomas, leading the dissent, urged that when law abiding citizens are flagged by a credit service as "potential terrorists and drug traffickers," the FCRA is clearly violated, and the will of Congress is contravened.[100] He also challenged the majority's premise that one-fourth of the class members affected in a seven-month period was an insufficient degree of risk to establish

---

93 *Id.* at 2200.

94 *Id.* at 2214.

95 *Id.*

96 *Id.* at 2205 (quoting Spokeo, Inc. v. Robins, 578 U.S. 330, 341 (2016)) ("[W]e cannot treat an injury as 'concrete' for Article III purposes based only on Congress's say-so.").

97 *Id.* at 2214.

98 *Id.* at 2209 (quoting Owner-Operator Indep. Drivers Ass'n v. U.S. Dept. of Transp., 879 F.3d 339, 344–45 (D.C. Cir. 2018)).

99 *Id.* at 2210.

100 *See id.* at 2214 (Thomas, J., dissenting).

substantial risk for the others: "If 25 percent is insufficient, then, pray tell, what percentage is?"[101]

III. EVOLVING CRITERIA FOR FEDERAL STANDING WHEN DATA IS BREACHED

While the Supreme Court added obstacles to standing in *Clapper* and *TransUnion*, lower court data breach cases were developing criteria to guide outcomes that did not rely on a single factor. This jurisprudence was crystallized in the Third Circuit's decision, *Clemens v. ExecuPharm Inc*.[102] In *Clemens*, sophisticated hackers had extracted large quantities of sensitive data–including addresses, bank and financial account numbers, passport data, tax and insurance information, and SSNs—of past and present employees of ExecuPharm, a biopharmaceutical company.[103] The victimized personnel sued after it became known that a hacking group known as CLOP perpetrated the data theft.[104] After ransomware demands were rejected by ExecuPharm,[105] CLOP posted the data on underground websites on the Dark Web.[106] This part of the Internet is hidden from search engines and creates an underground black market where criminals traffic stolen data for use in committing identity theft.[107] After learning of the theft of data and the risks of identity theft, the plaintiff undertook mitigation measures including review of financial records, placing firewall alerts, transfers to new accounts, and purchasing credit monitoring services.[108] Along with claims for negligence and breach of an implied contract, the plaintiffs' lawsuit included breach of contract based on the employment agreement by which ExecuPharm agreed to take appropriate

---

101 *Id.* at 2222.

102 Clemens v. ExecuPharm Inc., 48 F.4th 146, 153 (3d Cir. 2022).

103 *Id.* at 157.

104 *Id.* at 150–51.

105 "A ransomware attack is a type of malicious software that blocks access to a computer system or data, usually by encrypting it, until the victim pays a fee to the attacker." Keach v. BST & Co. CPAS, LLP, No. 903580-20, 2021 WL 1203026, at *3 n.1 (N.Y. Sup. Ct. Mar. 30, 2021).

106 *Clemens*, 48 F.4th at 150.

107 *Id.*

108 *See id.* at 151.

measures to protect data security.[109] Recognizing that, under Article III, standing requires an injury-in-fact, the court acknowledged that an "objectively reasonable likelihood" is not sufficient under *Clapper*.[110] In analyzing the Supreme Court's standing cases, including *TransUnion*, the court observed that "the injury must be 'actual or imminent,' not 'conjectural' or 'hypothetical.'"[111] While certainty is not the test for future harm, the threatened injury must be "certainly impending" or possess a "substantial risk" that the harm will occur.[112] In its analysis of substantial risk, the court derived a number of "non-exhaustive factors" to serve as "useful guideposts" from other decisions, while recognizing that no single factor is dispositive.[113]

The first factor was intentionality, since a sophisticated and malicious hacking scheme is far likelier to produce identity theft than an accidental disclosure.[114] The court also examined whether data had been misused in at least some instances, an element that was probative of risk, but not a prerequisite for standing.[115] The court also designated the character of information as a prime determinant:[116]

---

[109] *See id.* Other claims included breach of fiduciary duty, breach of confidentiality, and declaratory relief. *Id.*

[110] *See id*. at 153.

[111] *See id.* at 152.

[112] *See id.* (citing Susan B. Anthony List v. Driehaus, 573 U.S. 149, 158 (2014)).

[113] *Id.* at 153.

[114] *See id*. When hackers intentionally attack and extract, the risk factor is necessarily intensified. Remijas v. Neiman Marcus Group, LLC, 794 F.3d 688, 693 (7th Cir. 2015) ("Why else would hackers break into a store's database and steal consumers' private information?"); *see also* Galaria v. Nationwide Mut. Ins. Co., 663 F. App'x. 384, 388 (6th Cir. 2016) ("[N]o need for speculation where [*Galaria*] Plaintiffs allege that their data has already been stolen and is now in the hands of ill-intentioned criminals."). Stolen laptop cases are viewed as less determinative of an intention to exploit stolen private data. Randolph v. ING Life Ins. & Annuity. Co., 486 F. Supp. 2d 1, 7 (D.D.C. 2007) (While alleging that a burglar stole their laptops, plaintiffs did not allege that the purpose was to access their information or that their information had actually been accessed.).

[115] *See Clemens*, 48 F.4th at 153–54.

[116] *See id.* at 154; *see also* Portier v. NEO Tech. Sol., No. 3:17-cv-30111-TSH, 2019 WL 7946103, at *2 (D. Mass. Dec. 31, 2019) ("Cyber criminals can use W-

> For instance, disclosure of social security numbers, birthdates and names is more likely to create a risk of identity theft or fraud. By contrast, the disclosure of financial information alone, without corresponding personal information, is insufficient. This is because financial information alone generally cannot be used to commit identity theft or fraud.[117]

Having distilled the essence of extensive and even divergent outcomes into the most critical factors, the court turned to the *TransUnion* test that examined whether an alleged injury has "a 'close relationship' to a harm traditionally recognized as providing a basis for a lawsuit in American courts–such as physical harm, monetary harm, or various intangible harms."[118] After analyzing torts based on violation of privacy and intentional infliction of emotional distress, the court found that emotional distress, as well as expenditures for mitigation measures, established a traditionally recognized concrete injury.[119]

In focusing on the specific facts of *Clemens*, the court emphasized the fact that CLOP, the hacker, was a sophisticated ransomware group whose attacks were particularly perilous for privacy.[120] The threat was further compounded by the reality that the plaintiff's data was already published on the Dark Web, a platform rampant with trafficking in everything from stolen data to weapons, drugs,

---

2 information, including an employee's name, address and Social Security number, to steal an employee's identity and fraudulently obtain employment, loans and credit cards, and file tax returns in an employee's name.").

117 *Clemens*, 48 F.4th at 154 (internal citations omitted).

118 *See id* (quoting TransUnion, LLC v. Ramirez, 141 S. Ct. 2190, 2200 (2021)).

119 *See Clemens*, 48 F.4th at 158. Although not discussed in *Clemens*, state law principles of avoidable consequences and mitigation of damages should also be considered in assessing state common law traditions that support injury in data breach cases. *See infra* notes 135–136. While raised defensively rather than as an affirmative claim, they represent a component of the damages equation that is well-settled under longstanding state law principles. Malanowski v. Jabamoni, 772 N.E.2d 967, 973 (Ill. App. Ct. 2002). ("Mitigation of damages imposes a duty on the injured party 'to exercise reasonable diligence and ordinary care in attempting to minimize his damages after injury has been inflicted.'" (internal citations omitted)).

120 *See Clemens*, 48 F.4th at 157.

and counterfeit funds.[121] Another factor that underscored the substantiality of risk was the nature of financial and personal information that was "particularly concerning as it could be used to perpetrate both identity theft and fraud."[122] Taken together the factors establish a "'substantial risk' that the harm will occur" sufficient to demonstrate an imminent injury and establish standing.[123]

IV. FUTURE STANDING FOR FUTURE HARM

In the aftermath of *Clapper* and *TransUnion*, federal court standing for future harm from data breaches became more elusive in many circumstances. Absent individualized data theft, the oversized impact of *Clapper* has raised the burden of the "case or controversy" requirement of Article III without fully accounting for the risks of cyber criminality. When criminals maliciously acquire personal data, the potential for harm is qualitatively different than the risk of future unconstitutional surveillance by federal authorities who we presume to be acting lawfully.

Nor is the limiting force of *TransUnion* warranted for data disasters. The gravity of the risk posed by cyber criminals cannot be compared to the negligence of sloppy credit reporting. Moreover, even apart from the differences in the character of wrongdoing, the Court's indifference to an injury rate of one-fourth of the plaintiffs' class is puzzling.[124] Given the significant and demonstrable dissemination of inaccuracies which linked consumers to an OFAC list, Justice Thomas' criticisms are truly compelling.[125] Common sense defies relegating a one-fourth victimization rate to insubstantiality. By way of illustration, if homeowners in a community learned that twenty-five percent of their neighbors had been burglarized, people would reasonably spend money for future security measures—and some would even move out of the neighborhood. To suggest that resulting security measures are self-inflicted wounds is manifestly unfair to the victims. As a result, Justice Thomas further challenged

---

121 *See id.*
122 *See id.*
123 *See id.*
124 TransUnion LLC v. Ramirez, 141 S. Ct. 2190, 2200 (2021).
125 *Id.* at 2222 (Thomas, J., dissenting).

the *TransUnion* majority to provide its own magic number to measure substantial risk if twenty-five percent fell short.[126] But none appeared.

Unfortunately, since Justice Thomas spoke only for the dissent, future courts might conclude that even a twenty-five percent incident rate is not substantial enough to justify preventative measures. This seems wrong but it is possible, if not "imminent."[127]

Fortunately, statistics are not the only measure. Following *Clapper* and *TransUnion,* the Third Circuit, in *Clemens,* provided a roadmap with a narrow path to standing.[128] In that case, facts establishing ruthless criminal sophistication and the theft of highly confidential information produced a sufficiently imminent and substantial risk to scale the cliffs of standing under *Clapper* and *TransUnion*.[129] While *Clemens* properly observed that no single factor is determinative, the confluence of malicious expertise and personal identifying information was crucial and sufficient.[130] As another court noted, the entire objective of hackers who steal personal information is to monetize their scheme. "The purpose of the hack is, sooner or later, to make fraudulent charges or assume those consumers' identities."[131]

Otherwise stated, when a burglar holds the keys to one's home, the risk of future harm is palpable and a prudent homeowner would certainly change the locks. Given this manifest reality, courts should not require that thieves strike first before consumers take reasonable steps to protect themselves. Nor should courts dismiss such mitigation as self-inflicted or self-indulgent damages. Clearly, it is the intentionality of criminals and the negligence of data banks that cause such harm, not the victims seeking to avoid identity theft.

---

126 *See id.*

127 *Id.*

128 Clemens v. ExecuPharm Inc., 48 F.4th 146, 159 (3d Cir. 2022).

129 *See id*. at 157.

130 *See id.* These same factors were emphasized in *Attias v. CareFirst, Inc.*, which preceded *TransUnion* and addressed *Clapper*. 865 F.3d, 620, 628 (D.C. Cir. 2017). With these elements present, one can "infer that this party has both the intent and the ability to use that data for ill." *See id.*

131 *See* Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 693 (7th Cir. 2015).

V. A NEED FOR CLARITY AND REMEDY

In the absence of ingenious malevolence and stolen SSNs, the challenges of federal standing for most victims have increased. Cases in which only payment data such as credit card numbers are stolen, rather than SSNs and DOBs, will be even more difficult. In those cases, evidence of actual misuse such as false charges may be required because, ordinarily, credit cards can be promptly cancelled and replaced.[132] As a result, when only credit card information is purloined, unless false charges are actually incurred, standing will often be denied for the lack of a "case or controversy."[133]

Where the motive is uncertain, standing may correspondingly be more challenging. Laptop cases present distinctive standing obstacles because they can be stolen for their hardware, for their data, or for both.[134] Cases of accidental disclosure also present formidable standing challenges because so long as misuse has not materialized, the potentially jeopardized data may never be criminally exploited.[135]

While *Clemens* was an important advance in the aftermath of *Clapper* and *TransUnion*, *Clemens*' narrow path should be broad-

---

[132] Portier v. NEO Tech. Sols., No. 3:17-cv-30111-TSH, 2019 WL 7946103, at *6 (D. Mass. Dec. 31, 2019). Misuse can also be demonstrated where the "compromised personal information was exfiltrated, published and/or otherwise disseminated." Keach v. BST & Co. CPAS, LLP, No. 903580-20, 2021 WL 1203026, at *4–5 (N.Y. Sup. Ct. Mar. 30, 2021).

[133] *Compare* Whalen v. Michaels Stores, Inc., 689 F. App'x 89, 91 (2d Cir. 2017), *with* Lewert v. P.F. Chang's China Bistro, Inc., 819 F.3d 963 (7th Cir. 2016). In *Lewert*, the court found a sufficient basis for standing where the payment data had been stolen through a breach in the restaurant chain's computer system. In *Lewert*, though, a customer who found fraudulent transactions on his debit card spent $106.89 on a credit monitoring service to protect against identity theft. *Lewert*, 819 F.3d at 963. Because actual misuse had occurred, the court found that *Clapper* did not prevent standing and allowed damages for the purchase of credit monitoring services as well as the "time and effort monitoring both his card statements and his other financial information as a guard against fraudulent charges and identity theft." *Id.* at 967.

[134] *Compare* Beck v. McDonald, 848 F.3d 262, 275–77 (4th Cir. 2017) (rejecting standing where no evidence show misuse of stolen laptop) *with* Krottner v. Starbucks, Corp., 628 F.3d 1139, 1140 (9th Cir. 2010) (finding a stolen laptop created real and measurable threat of future harm).

[135] McMorris v. Carlos Lopez & Assocs., LLC, 995 F.3d 295, 305 (2d Cir. 2021).

ened. There is compelling justification for uniform legislation to address the divergent outcomes for standing and also to collect the broad array of state claims into a consistent remedial framework. Especially because so many data breach disasters transcend state and national borders, the current dilemma seemingly demands a federal solution through either Congressional legislation or regulatory promulgations.[136] But the federal state statutes cannot supplant the Supreme Court doctrine concerning standing in cases of future harm. Indeed, the Court in *TransUnion* downsized the remedies of FCRA and limited its protection to those who had already incurred the injury of a false credit report.[137] The standard advanced by the Second Circuit of "reasonably objective likelihood" was specifically rejected by the Supreme Court and is presently not viable in federal court.[138]

Because Congress cannot legislate a federal remedy at odds with the Court's increasingly restrictive standing jurisprudence, the solution instead may lie with state legislation. Many states are not limited by the case or controversy requirement and can turn to state law principles.[139] Although state cases often cite to federal decisions in discussing standing, as a matter of analysis, state courts often have greater discretion.[140] Thus, a recent Florida decision observed that "Florida has no case or controversy requirement. Instead, Florida has a different test for standing, one that—unlike the federal standard—melds together some of the elements of federal standards with

---

[136] The Federal Trade Commission provides guidance for companies to take remedial action following a breach, including model letters to victims and suggested steps for recovery. FED. TRADE COMM'N, DATA BREACH RESPONSE: A GUIDE FOR BUSINESS (2021), https://www.ftc.gov/system/files/documents/plain-language/560a_data_breach_response_guide_for_business.pdf. The FTC's broad enforcement powers to protect consumers may, resources permitting, facilitate its emergence as a principal regulator of data breach safeguards. The Securities and Exchange Commission has taken action against publicly traded companies that misled investors about data breaches. *See* Pearson PLC, Exchange Act Release No. 92676, 2021 WL 3627064 at *1 (Aug. 16, 2021).

[137] TransUnion LLC v. Ramirez, 141 S. Ct. 2190, 2190 (2021).

[138] *See id.* at 2207.

[139] *See infra* note 141 and accompanying text.

[140] *See id.*

the merits of the asserted claims."[141] Especially if states deployed greater flexibility concerning standing, ordinary principles of mitigation of damages and avoidable consequences could be applied. Section 918 of the Second Restatement of Torts, addressing the issue of avoidable consequences, provides "one injured by the tort of another is not entitled to recover damages for any harm that he could have avoided by the use of reasonable effort . . . ."[142] Similarly, the closely related doctrine of mitigation of damages imposes a duty "to exercise reasonable diligence and ordinary care in attempting to minimize [one's] damages after injury has been inflicted . . . ."[143]

---

[141] Hall v. Cooks, 346 So. 3d 183, 191 (Fla. Dist. Ct. App. 2022). ("The general test for standing is whether a [valuable] . . . litigant has a 'direct and articulable' interest in a case's outcome.") Accordingly, in many states, jurisdiction in state court is not limited by the U.S. Constitution's "case or controversy" requirement. *See, e.g.*, Lansing Schs. Educ. Ass'n. v. Lansing Bd. of Educ., 792 N.W.2d 686, 693–94 (Mich. 2010) (noting that the Michigan Constitution does not contain the "case or controversy" limitation thereby authorizing the Michigan courts to embrace more flexible criteria for standing.); *see, e.g.*, Weatherford v. San Rafael, 395 P.3d 274, 278 (Cal. 2017) ("Unlike the Federal Constitution, our state Constitution has no case or controversy requirement imposing an independent jurisdictional limitation on our standing doctrine."); State v. McElveen, 802 A.2d 74 (Conn. 2002) ("Our state constitution contains no case or controversy requirement analogous to that found in the United States constitution . . . [and] the state constitution does not confine the judicial power to actual cases and controversies." (internal citations omitted)); Lebran v. Gottlieb Mem'l Hosp., 930 N.E.2d 895, 917 n.4 (Ill. 2010) ("This court is not required to follow federal law on issues of standing, and has expressly rejected federal principles of standing."); U.S. Bank Nat'l Ass'n. v. Nelson, 163 N.E.3d 49, 51 (N.Y. 2020) (Wilson, J., concurring) ("The New York Constitution contains no case or controversy requirement; hence, federal constitutional standing doctrine is of little or no relevance."); Green v. Giuliani, 21 N.Y.S.2d 467, 470 (N.Y. Sup. Ct. 2000) ("That standing requirement in Federal Court, which is 'grounded in the Federal constitutional requirement of a case or controversy . . . [is] a requirement that has no analogue in the State Constitution.'"); Firearm Owners Against Crime v. Papenfuse, 261 A.3d 467, 481–82 (Pa. 2021) (observing that federal standing under Article III has constitutional limits and instead applying discretionary analysis to assure that the proper plaintiffs are before the court). *But see* Hibler v. Conseco, Inc., 744 N.E.2d 1012, 1014 (Ind. Ct. App. 2001) (explaining that while the Indiana Constitution does not include a "case or controversy requirement," federal limits on standing "are instructive" because federal and state justiciability principles fulfill the same goals.).

[142] RESTATEMENT (SECOND) OF TORTS § 918(1) (AM. L. INST. 1979).

[143] *Mitigation of Damages*, BLACK'S LAW DICTIONARY (5th ed. 1979). As one court explained, "The doctrine of mitigation of damages applies in both tort and contract cases. This duty to mitigate damages is sometimes called the 'doctrine of

Rather than treating such efforts as a consumer's self-inflicted wound, avoidable consequences and mitigating damages should be viewed as critical components of data breach cases.

In fashioning remedies, legislatures could examine the existing state jurisprudence that already provides negligence standards for responsible parties.[144] Those criteria could build upon the state laws already in place that impose criteria and penalties for failure to give notification of data breaches.[145] Factors such as the nature of the breach, the character of the perpetrator (if known), existing evidence of misuse, and the nature of purloined information (along with other relevant factors) should be enumerated in any such legislation. Data breach criteria should allow damages for the cost of reasonable measures that are taken based on a reasonable likelihood of future harm.

CONCLUSION

The frequent encounters between the dizzying pace of data breaches and chronically complex Article III jurisprudence have created diverse results across the federal circuits.[146] While the Supreme Court has not yet spoken to future harm for victims of cyber theft, the holdings in *Clapper* and, especially, in *TransUnion* signal

---

avoidable consequences.' It limits the amount of recoverable damages in that a party cannot recover damages resulting from consequences that he could have avoided by reasonable care, effort, or expenditure." S. Bldg. Servs., Inc. v. City of Fort Smith, 427 S.W.3d 763, 769 (Ark. Ct. App. 2013) (citation omitted).

[144] State courts are also "far from uniform" concerning standing under present laws. Keach v. BST & Co. CPAS, LLP, No. 903580-20, 2021 WL 1203026, at *3–4 (N.Y. Sup. Ct. Mar. 30, 2021).

[145] *E.g.*, FLA. STAT. § 501.171 (2022). Many states have laws like Florida's governing the definition of a "covered entity" to notify affected parties. While Florida's law does not create a private cause of order, it provides definitional sections for a breach: a "covered entity," "customer records," and "personal information." *Id.* at § 501.171(1)(a)–(c), (g). Florida's law includes Social Security numbers, driver's licenses, financial accounts, and health information, among other data. *Id.* at § 501.171(1)(g). Florida has also enacted a State Cyber Security Act applicable to state agencies and providing goals such as strategic planning to create guidelines and procedures to better protect against future breaches. FLA. STAT. § 282.318 (2022).

[146] *See supra* Section II.

an uphill climb on a narrow path.[147] Even so, as *Clemens* and several other cases indicated, when sophisticated hackers obtain personal identifying information, such as SSNs, the prospect of future harm emerges more vividly.[148] Ordinarily, congressional action could provide clarity for victims. But as *TransUnion* established, the remedial will of Congress—even with a twenty-five percent victimization track record—may not satisfy the Court's demands concerning future harm.[149] Since a uniform federal remedy may not meet Article III standing challenges, the states could utilize their own state constitutional identities for issues such as standing.[150] States have already moved forward with laws concerning the obligation to provide notifications of data disaster after the breach.[151] The states should be challenged by consumers to add to existing data breach laws by including private rights of action imposing accountability when companies fail to adequately safeguard customers and employees from the ceaseless waves of cyber crimes.

147 *See supra* Section III.
148 *See supra* Section IV.
149 *See supra* Section V.
150 *See supra* Section VI.
151 *See* FLA. STAT. § 501.171.