ARTICLE III STANDING — INJURY IN FACT — THIRD CIRCUIT HOLDS THAT DATA BREACH CREATES IMMINENT INJURY IN HEIGHTENING THE RISK OF IDENTITY THEFT OR FRAUD. — *Clemens v. ExecuPharm Inc.*, 48 F.4th 146 (3d Cir. 2022).

When victims of data breaches sue, courts are often sympathetic to their fears of identity theft and fraud.[1] But such worst-case outcomes materialize only in the future, if at all, which runs up against standing doctrine's requirement of an actual or imminent injury. This tension has bedeviled courts for a decade, dating back at least to the Supreme Court's tightening of "imminence" in *Clapper v. Amnesty International USA*.[2] Recently, in *Clemens v. ExecuPharm Inc.*,[3] the Third Circuit held that a plaintiff whose personal data had been stolen but who had yet to suffer any financial loss had nevertheless pleaded an imminent injury because there was a "substantial risk" that harm would occur.[4] *Clemens* is notable for distinguishing, if not overruling, circuit precedent seeming to require actual misuse of personal data.[5] But on a broader view, it is just the latest in a long string of data breach cases that have reached conflicting conclusions on standing under largely identical facts.[6] While *Clemens* falls on the more defensible side of this divide, it represents yet another missed opportunity for courts to evolve this area of law in response to the rising epidemic of data insecurity.

Jennifer Clemens provided ExecuPharm, Inc., her former employer, with "significant amounts of her personal and financial information," which ExecuPharm promised to "take appropriate measures to protect."[7] But in March 2020, a criminal ransomware group accessed ExecuPharm's servers and exfiltrated thousands of employee records with "full names, home addresses, social security numbers, . . . [and] credit card and bank information."[8] The hackers made "some of [this] information . . . available for download on the 'dark web,'"[9] the

---

[1] *See, e.g.*, *In re* Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig., 45 F. Supp. 3d 14, 26 (D.D.C. 2014) ("[I]t is reasonable to fear the worst in the wake of such a theft, and it is understandably frustrating to know that the safety of your most personal information could be in danger."); *In re* Zappos.com, Inc., 108 F. Supp. 3d 949, 961 (D. Nev. 2015) ("Plaintiffs' fears of identity theft and fraud are rational . . . .").

[2] 568 U.S. 398 (2013). *Clapper* held that an imminent injury must be more than "objectively reasonable," *id.* at 410, and may not rest upon a "speculative chain of possibilities," *id.* at 414.

[3] 48 F.4th 146 (3d Cir. 2022).

[4] *Id.* at 157 (quoting Susan B. Anthony List v. Driehaus, 573 U.S. 149, 158 (2014)).

[5] *See id.* at 153 (discussing Reilly v. Ceridian Corp., 664 F.3d 38 (3d Cir. 2011)).

[6] *See* Beck v. McDonald, 848 F.3d 262, 273 (4th Cir. 2017) (collecting cases).

[7] Clemens v. ExecuPharm, Inc., No. 20-3383, 2021 WL 735728, at *1 (E.D. Pa. Feb. 25, 2021).

[8] *Id.* The modus operandi of ransomware outfits is to break into a company's network; copy its files; encrypt those files, rendering them unusable; and offer to decrypt those files for a hefty fee, on threat of deleting them or publishing them to the world. *See* Sean Steinberg, *Ransomware Goes to Business School*, SLATE (May 19, 2022), https://slate.com/technology/2022/05/ransomware-customer-service-history.html [https://perma.cc/J46P-BDKK].

[9] *Clemens*, 2021 WL 735728, at *1.

underbelly of the Internet where stolen data is traded. ExecuPharm notified Clemens of the breach, stating that it "believe[d] sensitive information ha[d] been accessed" and "shared on the dark web" and that she "may [have] be[en] among the group of former employees impacted."[10]

Clemens sued ExecuPharm in the Eastern District of Pennsylvania, seeking individual and class relief on a variety of contract and tort theories.[11] She alleged several common law injuries: "[S]ubstantial and imminent risk of future harm" from identity theft or fraud, "significant time and effort" spent on mitigation, and harm to her "private contract rights."[12] Crucially, however, Clemens did not "allege [that] she ha[d] [actually] experienced any identity theft or fraud."[13]

Seizing on this fact, the district court granted ExecuPharm's motion to dismiss.[14] After reciting the familiar Article III standing test — injury in fact, traceability, redressability — the court homed in on injury in fact, which requires an injury that is "concrete," "particularized," and "actual or imminent."[15] It found this case indistinguishable from *Reilly v. Ceridian Corp.*,[16] a precedent holding that the increased risk of identity theft from a data breach was not a cognizable injury because the causal chain was too "attenuated" and "dependent on entirely speculative, future actions of an unknown third-party" (the would-be fraudster).[17] That the hacker here was identifiable, had "criminal intent," undeniably accessed the data, and even published some of it were "distinctions without a difference."[18] For example, although Clemens's data was on the dark web, someone had to "actually download[] her information," "attempt to use" it, and "do so successfully" for harm to occur.[19] The district court then disposed of Clemens's other bases for standing: "[T]ime, money and effort" spent to avoid a speculative injury is not itself an injury, and it isn't clear that "a contractual breach *categorically* creates an Article III injury."[20] Clemens timely appealed.[21]

---

[10] *Id.* at *2 (emphasis omitted). ExecuPharm did not definitively state that Clemens's data had been breached, only that it "*may*" have. *Id.* On the motion to dismiss, both the district and appellate courts "credit[ed] that her information was accessed." *Id.*; *see also Clemens*, 48 F.4th at 156 ("[A] known hacker group . . . accessed Clemens's sensitive information."). But not all courts have given plaintiffs the benefit of the doubt. *See, e.g.*, *Reilly*, 664 F.3d at 42 ("Appellants' contentions rely on speculation that the hacker . . . read, copied, and understood their personal information . . . .").

[11] *Clemens*, 2021 WL 735728, at *2.

[12] *Id.* at *2–3.

[13] *Id.* at *2.

[14] *Id.* at *1, *3.

[15] *Id.* at *3 (citing Lujan v. Defs. of Wildlife, 504 U.S. 555, 560–61 (1992)).

[16] 664 F.3d 38 (3d Cir. 2011).

[17] *Id.* at 42.

[18] *Clemens*, 2021 WL 735728, at *4.

[19] *Id.* That Clemens hadn't suffered identity theft or fraud in the year since the breach only "underscored" the "speculative nature of any future harm." *Id.*

[20] *Id.* at *5 (quoting Plaintiff's Supplemental Brief Regarding Article III Standing at 10, *Clemens*, 48 F.4th 146 (No. 20-3383)).

[21] *Clemens*, 48 F.4th at 151.

The Third Circuit vacated and remanded.[22] Writing for the panel, Judge Greenaway[23] held that Clemens had standing to bring her claims,[24] with the bulk of the analysis centered on the "actual or imminent" prong of injury in fact.[25] He conceded that "mere access and publication" of data may not "cause inherent harm" — hence, no actual injury — but asserted that a data breach might "still poise the victim to endure" imminent future harms, like identity theft or fraud.[26] He clarified that *Reilly* "did not create a bright line rule precluding standing" based on future risks, as such a reading would "directly contravene" Supreme Court precedent that plaintiffs need not "wait until they . . . sustain[] an actual injury to bring suit."[27] Instead, synthesizing cross-circuit precedent, he held that it is enough for there to be a "substantial risk" of harm,[28] which exists if (1) the "breach was intentional," (2) "the data was misused," and (3) "the nature of the [breached] information . . . could subject a plaintiff to a risk of identity theft."[29]

Applying these factors, Judge Greenaway agreed with Clemens that the risk of harm here was imminent: (1) the ransomware group intentionally "launched a sophisticated phishing attack" at ExecuPharm; (2) it misused ExecuPharm's data by holding it for ransom; and (3) the data included both personal and financial information, a "particularly concerning" combination that "could be used to perpetrate both identity theft and fraud."[30] Moreover, whereas *Reilly* involved "an *unknown* hacker who *potentially* gained access to sensitive information,"[31] here, the hacker was a "sophisticated" and "notorious" operator who had "already published Clemens's data on the Dark Web."[32]

Judge Phipps concurred in the judgment.[33] He argued that the majority "unnecessar[ily]" applied the Article III standing test,[34] which only governs "claims seeking to vindicate constitutional or statutory

---

[22] *Id.* at 150.

[23] Judge Greenaway was joined by Judge Krause.

[24] *Clemens*, 48 F.4th at 159.

[25] Judge Greenaway also held that Clemens's injury was concrete, citing both the close analogue to "harms long recognized at common law like the 'disclosure of private information,'" *id.* at 157 (quoting TransUnion LLC v. Ramirez, 141 S. Ct. 2190, 2204 (2021)), and her attendant concrete harms like emotional distress, *id.* at 158. He found the other two standing prongs, traceability and redressability, to be satisfied as well. *Id.*

[26] *Id.* at 152; *see also id.* at 155.

[27] *Id.* at 153 (citing Susan B. Anthony List v. Driehaus, 573 U.S. 149, 158 (2014)). *Reilly* held that plaintiffs "have not suffered any injury" "[u]nless and until" the hacker makes "unauthorized transactions in [their] names." Reilly v. Ceridian Corp., 664 F.3d 38, 42 (3d Cir. 2011).

[28] *Clemens*, 48 F.4th at 152 (quoting *Susan B. Anthony List*, 573 U.S. at 158).

[29] *Id.* at 153–54. The court cautioned that these factors were neither individually dispositive nor exhaustive, *id.* at 153, and, in particular, that "misuse is not necessarily required," *id.* at 154.

[30] *Id.* at 157.

[31] *Id.* at 156 (citing *Reilly*, 664 F.3d at 42–43).

[32] *Id.* at 157.

[33] *Id.* at 159 (Phipps, J., concurring in the judgment).

[34] *Id.* at 161.

rights"[35] and "operates as a supplement to, not a substitute for" standing predicated on "traditionally recognized cause[s] of action."[36] In his view, the fact that Clemens's claims, which sounded in contract and tort, were "of the sort traditionally amenable to, and resolved by, the judicial process" was sufficient in and of itself to confer standing.[37]

Clemens's discretion-laden test for imminent injuries perpetuates the unfortunate trend in data breach cases of standing hinging on minute and subjective differences in the facts. The Third Circuit should have taken a different approach and held that while Clemens suffered no *imminent* injury under the reasoning of *Reilly*, she did suffer an *actual* injury by virtue of having her data stolen and subsequently needing to take costly precautions against identity theft. Such a reorientation would eschew guesswork about probabilities in favor of a more objective evaluation of the sensitivity of the breached data, yielding more consistent judgments in favor of meritorious plaintiffs while penalizing companies for lax security practices. An actual-injury analysis would thus strike a better balance between the many considerations at play in data breach litigation: recompense for plaintiffs, fairness for defendants, administrability for courts, and protections for society.

Having characterized Clemens's injury as "the risk of identity theft or fraud,"[38] the *Clemens* court was obliged to ask, for standing purposes, whether this risk was imminent. The problem is that imminence is unworkable in the context of data breaches. Of the three factors the court considered — intent of the hacker, evidence of actual misuse, and sensitivity of the data[39] — only the third is sensible: the kind of data that was compromised is both objectively determinable and determinative of the potential harm.[40] By contrast, the second factor, actual misuse,[41] is fraught because it is hard to trace identity theft back to a specific

---

[35] *Id.* at 159–60.

[36] *Id.* at 161 (emphases omitted).

[37] *Id.* (quoting Uzuegbunam v. Preczewski, 141 S. Ct. 792, 798 (2021)).

[38] *Id.* at 156 (majority opinion).

[39] *Id.* at 153–54. The Second Circuit adopted the same three-part test in *McMorris v. Carlos Lopez & Associates, LLC*, 995 F.3d 295, 301–02 (2d Cir. 2021). And many other courts have considered the hacker's intent, *see, e.g.*, *In re* Marriott Int'l, Inc., Customer Data Sec. Breach Litig., 440 F. Supp. 3d 447, 460 (D. Md. 2020); *In re* Adobe Sys., Inc. Priv. Litig., 66 F. Supp. 3d 1197, 1215 (N.D. Cal. 2014); *In re* Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig., 45 F. Supp. 3d 14, 25 (D.D.C. 2014), actual misuse, *see, e.g.*, Beck v. McDonald, 848 F.3d 262, 274 (4th Cir. 2017); Storm v. Paytime, Inc., 90 F. Supp. 3d 359, 366 (M.D. Pa. 2015); *Adobe*, 66 F. Supp. 3d at 1216, and the nature of the data, *see, e.g.*, *In re* U.S. Off. of Pers. Mgmt. Data Sec. Breach Litig., 928 F.3d 42, 56 (D.C. Cir. 2019); Lewert v. P.F. Chang's China Bistro, Inc., 819 F.3d 963, 967 (7th Cir. 2016); *Adobe*, 66 F. Supp. 3d at 1215–16.

[40] *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 30 (2007).

[41] The *Clemens* court unusually located actual misuse in the hackers holding ExecuPharm's data hostage and ultimately publishing it. *Clemens*, 48 F.4th at 157. This typically speaks more to the intent-of-the-hacker prong, discussed next, while actual misuse refers to direct exploitation of the data itself, causing loss to victims. *See, e.g.*, *Marriott*, 440 F. Supp. 3d at 459.

breach;[42] not to mention, it cuts against the court's own assertion that "a plaintiff need not wait until . . . she has actually sustained the feared harm" to sue.[43] And the first factor, hacker intent, is harder still to pin down. Even if it could be determined that a hacker were motivated by, say, espionage, that hardly rules out opportunistic fraud.[44] Nor does sophistication, which seemed to influence the court's analysis,[45] necessarily correlate with imminence: criminal outfits like the one that hacked ExecuPharm depend on companies ponying up for the *safe* return of their data, so misuse would undercut the hackers' own business.[46] On top of it all, standing is usually challenged on a motion to dismiss,[47] at which stage much of what plaintiffs know about the breach comes from the breached company itself — yet governing state law typically does not require disclosure of details like the hacker's identity,[48] and companies are increasingly reluctant to offer up such information,[49] making it exceptionally difficult for plaintiffs to plead the requisite facts.

Unsurprisingly, these multifactor tests have proven something of a lottery. Courts have divined opposite meanings from the same facts.[50] They have held differently in nearly identical scenarios[51] — even with respect to the same scenario.[52] And they have struggled to reconcile the

---

[42] U.S. GOV'T ACCOUNTABILITY OFF., *supra* note 40, at 28.

[43] *Clemens*, 48 F.4th at 152 (emphasis omitted).

[44] *See U.S. Off. of Pers. Mgmt.*, 928 F.3d at 57. The 2015 breach of Ashley Madison, a website that facilitates extramarital affairs, offers another example. Though the hackers appeared to be morally driven in demanding that the website be shut down, they also publicly posted the data, which was used by others to extort victims. *See* Kim Zetter, *Hackers Finally Post Stolen Ashley Madison Data*, WIRED (Aug. 18, 2015, 5:55 PM), https://www.wired.com/2015/08/happened-hackers-posted-stolen-ashley-madison-data [https://perma.cc/VEA2-6W22].

[45] *See Clemens*, 48 F.4th at 157.

[46] Steinberg, *supra* note 8 ("As smaller groups or lone wolves . . . get into the ransomware game, we will see more focus on short-term gain . . . ." (quoting Daniel Clayton, a cybersecurity expert)).

[47] *Clemens* and many key precedents arose on motions to dismiss. *See Clemens*, 48 F.4th at 151; Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 691 (7th Cir. 2015); Reilly v. Ceridian Corp., 664 F.3d 38, 40 (3d Cir. 2011); Krottner v. Starbucks Corp., 628 F.3d 1139, 1141 (9th Cir. 2010).

[48] Take California's data breach notification law, a model for forty-seven other states. KAMALA D. HARRIS, CAL. DEP'T OF JUST., CALIFORNIA DATA BREACH REPORT 2 (2014). Notifications must give "the types of personal information" breached and a "description of the . . . incident," but need not identify the entity behind the breach. *See* CAL. CIV. CODE § 1798.82(d)(2) (West 2022).

[49] *See* IDENTITY THEFT RES. CTR., DATA BREACH ANNUAL REPORT 15 (2022).

[50] In litigation over Nationwide's 2012 data breach, the district court saw Nationwide's provision of credit monitoring and identity-theft protection services to victims as a reason why the risk of injury was not "certainly impending," Galaria v. Nationwide Mut. Ins. Co., 998 F. Supp. 2d 646, 654–55 (S.D. Ohio 2014), *rev'd*, 663 F. App'x 384 (6th Cir. 2016), while the circuit court considered the fact that Nationwide offered the services at all to signal "the severity of the risk," *Galaria*, 663 F. App'x at 388; *accord Remijas*, 794 F.3d at 694 (finding such offerings "telling").

[51] Do plaintiffs have standing to sue over a stolen laptop with sensitive data? *Compare Krottner*, 628 F.3d at 1143 (yes), *with* Beck v. McDonald, 848 F.3d 262, 274 (4th Cir. 2017) (no). What about credit card information taken from a restaurant's point-of-sale system? *Compare* Lewert v. P.F. Chang's China Bistro, Inc., 819 F.3d 963, 965, 969 (7th Cir. 2016) (yes), *with* Tsao v. Captiva MVP Rest. Partners, LLC, 986 F.3d 1332, 1335, 1343 (11th Cir. 2021) (no).

[52] *Compare* Moyer v. Michaels Stores, Inc., No. 14 C 561, 2014 WL 3511500, at *6 (N.D. Ill. July 14, 2014), *with* Whalen v. Michaels Stores, Inc., 689 F. App'x 89, 90–91 (2d Cir. 2017).

case law.[53] The upshot: a plaintiff's odds turn largely on the venue (perhaps even the judge they draw) and the smallest factual variations.[54]

Reframing data breaches as actual injuries avoids these complications. The *Clemens* court was quick to assume that a data breach is not per se injurious because it does not resemble traditional tort harms[55] — but injury in fact is ultimately "a normative concept, not a descriptive one,"[56] and there are compelling policy reasons to adopt this reframing. First, deterrence. As the *Clemens* court observed, the fallout from data breaches may be impossible to remediate,[57] so companies must "implement appropriate security measures" ahead of time.[58] While the confused state of current jurisprudence does not reliably punish companies for complacency, certain and timely liability, which an actual-injury framework is more likely to produce, would strongly incentivize action. And, while reorienting Clemens's claims around actual injury would limit the available damages — she could not then recover for identity theft, which was imminent at best — in a class action like the one she brought, even small awards add up to meaningful sums.[59]

Second, loss limitation. Compensating victims for "necess[ary]"[60] precautions like credit monitoring is a cost-effective way to mitigate potential losses.[61] It is no answer to wait for losses to materialize before allowing suits to proceed: given the frequency of breaches nowadays, corporate defendants may well argue that such victims still lack standing because in the meantime, *other* companies holding the same victims' data have also been breached, so the loss is not fairly traceable to them.[62]

Third, basic notions of fairness. Consumers have no real say in whether to give up their data or how it is stored, placing them at the mercy of the companies they interact with. Clemens, for instance, was obligated to provide sensitive information "[a]s a condition of her

---

[53] *See Beck*, 848 F.3d at 273–74 (describing the deep circuit split).

[54] *See generally* F. Andrew Hessick, *Probabilistic Standing*, 106 NW. U. L. REV. 55, 75 (2012) (noting that courts, lacking "adequate information," are often forced to evaluate probabilities on a "gestalt feeling of the likelihood of a harm occurring," an approach that is "vulnerable to biases").

[55] *See Clemens*, 48 F.4th at 152.

[56] Courtney M. Cox, *Risky Standing: Deciding on Injury*, 8 NE. U. L.J. 75, 94 (2016); *see also* Cass R. Sunstein, *What's Standing After* Lujan*? Of Citizen Suits, "Injuries," and Article III*, 91 MICH. L. REV. 163, 188–89 (1992) (describing injury in fact as "normatively laden," *id.* at 189).

[57] *Clemens*, 48 F.4th at 156.

[58] *Id.* at 158.

[59] For instance, the ExecuPharm breach appeared to affect five thousand employees. *See* Class Action Complaint ¶ 29, Clemens v. ExecuPharm, Inc., No. 20-3383, 2021 WL 735728 (E.D. Pa. Feb. 25, 2021). Compensating a class of five thousand for a year's worth of credit-monitoring services — purchased by Clemens for $40 a month, *id.* ¶ 71 — would run over $2,000,000.

[60] *Clemens*, 48 F.4th at 158.

[61] By contrast, if the injury is financial loss, taking precautions can perversely destroy standing. *See, e.g.*, Whalen v. Michaels Stores, Inc., 689 F. App'x 89, 90 (2d Cir. 2017) (denying standing because plaintiff canceled her credit card and thus faced no threat of fraud).

[62] ExecuPharm tried this very argument. *See* Brief for Appellees-Defendants ExecuPharm Inc. & Parexel International Corp. at 32, *Clemens*, 48 F.4th 146 (No. 21-1506), 2021 WL 2526001.

employment."[63] In other contexts, courts have responded to an imbalance of bargaining power by fashioning protective default rules — for instance, scrutinizing adhesion contracts under the judge-made doctrine of unconscionability.[64] They should do the same with data breaches.

Moreover, this characterization of data breaches as actual injuries is reconcilable with Supreme Court precedent. As an initial matter, while recent decisions like *TransUnion LLC v. Ramirez*[65] may clamp down on injury in fact by requiring concrete harms in cases involving statutory claims,[66] they do not obviously bear on common law cases like *Clemens*. Underlying *TransUnion* were concerns about separation of powers[67] and, in particular, congressional creation of "novel and expansive causes of action,"[68] neither of which is relevant when one private party is suing another on common law contract and tort theories.[69] And, at other times, the Court has liberally construed injury in fact to reflect, at its core, the "invasion of a legally protected interest."[70] Justice Thomas has further explained that standing is grounded in the "traditional, fundamental limitations . . . of common-law courts,"[71] which historically "possessed broad power to adjudicate suits involving the alleged violation of private rights, even when plaintiffs alleged . . . nothing more."[72]

Thus, the Third Circuit could have held that ExecuPharm's actions created a plausible risk of financial loss, invading Clemens's legal interests (whether or not loss materialized) and imposing an actual injury. Scholars and judges have suggested that individuals hold an interest "in not having to pay to insure against risk,"[73] that "loss of a chance of . . . avoiding an adverse consequence should be compensable,"[74] and that

---

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

64 *See* 8 WILLISTON ON CONTRACTS § 18:13 (4th ed.) (Westlaw) (last visited Apr. 2, 2023).

65 141 S. Ct. 2190 (2021).

66 *See id.* at 2214 ("No concrete harm, no standing."); *id.* at 2219 (Thomas, J., dissenting) ("[T]he majority holds that the mere violation of a personal legal right is *not* — and never can be — an injury sufficient to establish standing.").

67 *Id.* at 2203, 2207 (majority opinion).

68 *See id.* at 2206 n.1.

69 One might even question whether the tripartite standing test, often explained as a way to preserve separation of powers, *see id.* at 2203, should apply at all to common law actions that have long been deemed "well suited for judicial resolution," *Clemens*, 48 F.4th at 160 (Phipps, J., concurring in the judgment). *But see* Lujan v. Defs. of Wildlife, 504 U.S. 555, 560 (1992) ("[T]he irreducible constitutional minimum of standing contains three elements.").

70 Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1548 (2016) (quoting *Lujan*, 504 U.S. at 560).

71 *Id.* at 1550–51 (Thomas, J., concurring) (quoting Honig v. Doe, 484 U.S. 305, 340 (1988) (Scalia, J., dissenting)).

72 *Id.* at 1551; *cf.* Uzuegbunam v. Preczewski, 141 S. Ct. 792, 800 (2021) (noting that at common law, "a plaintiff who proved a legal violation could always obtain some form of damages").

73 Cox, *supra* note 56, at 100. Though courts usually recognize this interest only where "the risk posed is intolerable," *id.* at 112, *Clemens* found data breaches to clear this bar, forcing victims to live with severe, potentially irremediable risks, *see Clemens*, 48 F.4th at 156.

74 Joseph H. King, Jr., *Causation, Valuation, and Chance in Personal Injury Torts Involving Preexisting Conditions and Future Consequences*, 90 YALE L.J. 1353, 1354 (1981); *cf., e.g.*, Petriello v. Kalman, 576 A.2d 474, 483 (Conn. 1990) (characterizing plaintiff's increased risk of medical harm as a "present risk, rather than a future event for which she claims damages").

"risk of harm [is] itself a harm."[75] Here, *Clemens* posited a "well-founded fear" of hackers misusing victims' data,[76] and even courts that have denied standing have admitted that victims would "fear the worst" and "watch their credit reports until something untoward occurs."[77] Those impositions can themselves be injuries.

Importantly, this actual-injury approach has its limits. Plaintiffs on a motion to dismiss would have to plead that the breached data is of the sort that can be used for financial crime — names, addresses, account numbers[78] — unless defendants can produce mitigating evidence.[79] More benign breaches (say, of email addresses) would not inflict a plausible risk of loss and thus would not constitute injuries.[80] This responds to a concern about opening the floodgates of litigation,[81] as well as to the notion that it would be unfair or even counterproductive to hold companies liable for simple carelessness.[82] Companies can avoid liability by taking precautions like encryption that protect victims even in case of breach. Plus, damages would be limited as plaintiffs could recover only for costs that directly stem from the breach, like credit monitoring or time spent on remediation, not losses that are yet to occur.

In *Clemens*, the Third Circuit rightly recognized that in our "increasingly digitalized world," it is critical for companies that choose to "maintain massive datasets . . . [to] implement appropriate security measures."[83] But, having identified a compelling interest of victims in avoiding the "uniquely drastic" harms of data breaches,[84] it should have opted for the direct application of actual injury instead of the linguistic gymnastics of imminence in applying the Article III standing test. Future courts should take care to avoid the same pitfalls and instead articulate a more practicable set of conditions under which victims of data breaches may hold companies to account.

---

[75] Claire Finkelstein, *Is Risk a Harm?*, 151 U. PA. L. REV. 963, 977 (2003).

[76] *Clemens*, 48 F.4th at 156.

[77] *In re* Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig., 45 F. Supp. 3d 14, 26 (D.D.C. 2014).

[78] At least one circuit has taken this approach. *See* Attias v. CareFirst, Inc., 865 F.3d 620, 623, 629 (D.C. Cir. 2017) ("[A] substantial risk of harm exists . . . simply by virtue of the hack and the nature of the data . . . taken." *Id.* at 629.).

[79] *See, e.g.*, Polanco v. Omnicell, Inc., 988 F. Supp. 2d 451, 469 (D.N.J. 2013) (denying standing where company confirmed plaintiff's data was not breached); *Sci. Applications*, 45 F. Supp. 3d at 25 (denying standing in part because data was encrypted, in an uncommon file format, and on difficult-to-access physical media).

[80] *See* Antman v. Uber Techs., Inc., No. 15-cv-01175, 2018 WL 2151231, at *9 (N.D. Cal. May 10, 2018) ("Without a hack of information such as social security numbers, account numbers, or credit card numbers, there is no . . . credible risk of identity theft that risks real, immediate injury."). Some argue that "any risk of harm, even a tiny one, should suffice for Article III standing." Hessick, *supra* note 54, at 69. Even if that is right, courts can take the middle road on prudential grounds, recognizing data breach as an injury only to the extent necessary to deter lax data security.

[81] The flood of litigation might be illusory in any event. *See* Hessick, *supra* note 54, at 89–91.

[82] For an articulation of these arguments, see Cox, *supra* note 56, at 81, 122–23.

[83] *Clemens*, 48 F.4th at 158.

[84] *Id.* at 156.