PRECEDENTIAL

UNITED STATES COURT OF APPEALS
FOR THE THIRD CIRCUIT

_____

No. 21-1506

_____

JENNIFER CLEMENS,
Appellant

v.

EXECUPHARM INC.; PAREXEL INT'L CORP.

_____

On Appeal from the United States District Court
for the Eastern District of Pennsylvania
(Civil No. 2-20-cv-03383)
District Judge: Honorable Gerald J. Pappert

_____

Argued December 14, 2021

_____

Before: GREENAWAY, JR., KRAUSE, and PHIPPS, *Circuit Judges*.

(Filed: September 2, 2022)

Mark S. Goldman
Goldman Scarlato & Penny
161 Washington Street
8 Tower Bridge, Suite 1025
Conshohocken, PA 19428

J. Austin Moore [ARGUED]
Norman E. Siegel
Barrett J. Vahle
Caleb J. Wagner
Stueve Siegel Hanson
460 Nichols Road
Suite 200
Kansas City, MO 64112

Counsel for Appellant

Shifali Baliga
Kristine M. Brown
Donald M. Houser [ARGUED]
Alston & Bird
1201 West Peachtree Street
One Atlantic Center, Suite 4900
Atlanta, GA 30309

Mathieu Shapiro
Obermayer Rebmann Maxwell & Hippel
1500 Market Street
Centre Square West, 34th Floor
Philadelphia, PA 19102

Counsel for Appellees

OPINION OF THE COURT

GREENAWAY, JR., *Circuit Judge*.

In this appeal, Jennifer Clemens asks us to reverse the District Court's dismissal of her complaint seeking equitable and monetary relief in connection with a data breach that resulted in the publication of her sensitive personal information on the Dark Web. Clemens argues that her injury was sufficiently imminent to constitute an injury-in-fact for purposes of standing. We agree. Accordingly, we will vacate the judgment of the District Court and remand for consideration of the merits.

I. Background[1]

Clemens is a former employee of ExecuPharm, Inc. ("ExecuPharm" or "the Company"), a subsidiary of the global biopharmaceutical company Parexel International Corp. ("Parexel"). As a condition of her employment, Clemens was required to provide ExecuPharm with sensitive personal and financial information, including her address, social security

[1] Where, as here, the challenge to a District Court's subject matter jurisdiction was made on the face of the pleadings, we accept all "well-pleaded factual allegations as true and draw all reasonable inferences" in favor of the plaintiff. *In re Horizon Healthcare Servs. Inc. Data Breach Litig.*, 846 F.3d 625, 633 (3d Cir. 2017).

number, bank and financial account numbers, insurance and tax information, her passport, and information relating to her husband and child. In exchange, Clemens's employment agreement provided that ExecuPharm would "take appropriate measures to protect the confidentiality and security" of this information. J.A. 41 ¶ 58. Based on the complaint's allegations, ExecuPharm did not perform its obligation.

After Clemens had left ExecuPharm, a hacking group known as CLOP accessed ExecuPharm's servers through a phishing attack in March 2020, stealing sensitive information pertaining to current and former employees, including Clemens. Specifically, the stolen information contained social security numbers, dates of birth, full names, home addresses, taxpayer identification numbers, banking information, credit card numbers, driver's license numbers, sensitive tax forms, and passport numbers. In addition to exfiltrating the data, CLOP installed malware to encrypt the data stored on ExecuPharm's servers. Then, CLOP held the decryption tools for ransom, threatening to release the information if ExecuPharm did not pay the ransom**.** Either because ExecuPharm refused to pay or for nefarious reasons unknown, the hackers made good on their threat and posted the data on underground websites located on the Dark Web, which is "a portion of the Internet that is intentionally hidden from search engines and requires the use of an anonymizing browser to be accessed. It is most widely used as an underground black market where individuals sell illegal products like . . . sensitive stolen data that can be used to commit identity theft or fraud." J.A. 25 ¶ 15. Screenshots by an Israel-based intelligence firm confirm that CLOP made available for download at least one archive containing nearly 123,000 files and 162 gigabytes of

data pertaining to ExecuPharm and Parexel, including sensitive employee information.

Throughout March and April of 2020, ExecuPharm provided periodic updates to current and former employees to inform them of the breach and encourage them to take precautionary measures. ExecuPharm appreciated the risks, cautioning current and former employees that "[u]nauthorized access to [the compromised] information may potentially lead to the misuse of [their] personal data to impersonate [them] and/or to commit, or allow third parties to commit, fraudulent acts such as securing credit in [their] name." J.A. 30 ¶ 28.

To mitigate potential harm, Clemens took immediate action. She conducted a review of her financial records and credit reports for unauthorized activity; placed fraud alerts on her credit reports; transferred her account to a new bank; enrolled in ExecuPharm's complimentary one-year credit monitoring services; and purchased three-bureau credit monitoring services for herself and her family for $39.99 per month for additional protection. As a result of the breach, Clemens alleges that she has sustained a variety of injuries—primarily the *risk* of identity theft and fraud—in addition to the investment of time and money to mitigate potential harm.

Seeking redress, Clemens brought suit against ExecuPharm and Parexel in the United States District Court for the Eastern District of Pennsylvania. She sought to represent herself and a class of all others whose personal information was compromised, as well as a subclass of current and former ExecuPharm employees whose employment agreements promised that the Company would take appropriate measures to protect their personal data. She invoked the subject matter

jurisdiction of the District Court under the Class Action Fairness Act, 28 U.S.C. § 1332(d).

She asserted claims for negligence (Count I), negligence per se (Count II), and breach of implied contract (Count III) against both Defendants. She also asserted claims for breach of contract (Count IV), breach of fiduciary duty (Count V), and breach of confidence (Count VI) against ExecuPharm. Lastly, she sought a declaratory judgment that Defendants' existing data security measures fail to comply with their fiduciary duties of care and that instructs them to implement and maintain industry-standard measures.

ExecuPharm and Parexel filed a motion to dismiss the complaint under Federal Rule of Civil Procedure 12(b)(6). The District Court ordered the parties to submit supplemental briefing regarding Clemens's standing, and, after receiving that briefing, granted the motion to dismiss on February 25, 2021 based on lack of Article III standing. Specifically, the District Court stated that it sought to follow our "bright line" rule providing that allegations of an increased risk of identity theft resulting from a security breach are insufficient for standing. J.A. 9 (quoting *In re Rutter's Inc. Data Sec. Breach Litig.*, 511 F. Supp. 3d 514, 525 (M.D. Pa. 2021)). Applying our decision in *Reilly v. Ceridian Corp.*, 664 F.3d 38 (3d Cir. 2011), the District Court concluded that Clemens's risk of future harm was not imminent, but "speculative," because she had not yet experienced actual identity theft or fraud. J.A. 9-11. This conclusion also meant that any money Clemens spent to mitigate the speculative risk was likewise insufficient to confer standing. The District Court additionally held that, even if ExecuPharm breached the employment agreement, it would not have automatically given Clemens standing to assert her

breach of contract claim. Clemens timely appealed and seeks vacatur of the District Court's dismissal of her complaint.

II. Applicable Law[2]

A. Article III Standing Requirements

Article III standing requires a plaintiff to demonstrate: "(1) that he or she suffered an injury in fact that is concrete, particularized, and actual or imminent, (2) that the injury was caused by the defendant, and (3) that the injury would likely be redressed by the requested judicial relief."[3] *Thole v. U.S. Bank N.A.*, 140 S. Ct. 1615, 1618 (2020) (citing *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 560-61 (1992)). Only the first two prongs are disputed on appeal.

a. Injury-in-fact: Imminent

---

[2] The District Court had jurisdiction over the underlying putative class action pursuant to 28 U.S.C. § 1332(d). We have jurisdiction pursuant to 28 U.S.C. § 1291.

[3] Our concurring colleague suggests that because Clemens "brings causes of action 'of the sort traditionally amenable to, and resolved by, the judicial process,'" we need not apply the typical tri-partite standing analysis in this case. Concurring Opinion at 5 (quoting *Uzuegbunam v. Preczewski*, 141 S. Ct. 792, 798 (2021)). We disagree, and apply this tri-partite approach consistent with binding precedent. *See, e.g.*, *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 560-61 (1992) (citations omitted); *Thorne v. Pep Boys Manny Moe & Jack Inc.*, 980 F.3d 879, 885 (3d Cir. 2020) (quoting *Spokeo, Inc. v. Robins*, 578 U.S. 330, 338 (2016)).

With regard to the injury-in-fact prong, the injury must be "actual or imminent, not 'conjectural' or 'hypothetical.'" *Lujan*, 504 U.S. at 560 (citations omitted). That "actual or imminent" is disjunctive is critical: it indicates that a plaintiff need not wait until he or she has *actually* sustained the feared harm in order to seek judicial redress, but can file suit when the risk of harm becomes imminent. This is especially important in the data breach context, where the disclosure of the data may cause future harm as opposed to currently felt harm. In this way, depending on the nature of the data at issue, claims flowing from a data breach can differ from traditional tort claims like defamation or invasion of privacy. While a claim arising from a data breach may share some commonalities with such torts—*e.g.*, in that it may involve the publication of information to a third party or unauthorized access to private information—the latter claims involve actual injury. A claim for defamation, for instance, rests on the "reputational harm" that flows from the publication of a statement "that would subject [the victim] to hatred, contempt, or ridicule." *TransUnion LLC v. Ramirez*, 141 S. Ct. 2190, 2208-09 (2021) (quoting *Milkovich v. Lorain Journal Co.*, 497 U.S. 1, 13 (1990)). And a claim for invasion of privacy contemplates that the exposure "cause[s] mental suffering, shame or humiliation" to the victim. *Pro Golf Mfg., Inc. v. Tribune Rev. Newspaper Co.*, 809 A.2d 243, 248 (Pa. 2002). By contrast, the type of data involved in a data breach may be such that mere access and publication do not cause inherent harm to the victim. *Reilly*, 664 F.3d at 42. Even then, however, it can still poise the victim to endure the kind of future harm that qualifies as "imminent."

Indeed, allegations of future injury "suffice if the threatened injury is 'certainly impending' or there is a

'substantial risk' that the harm will occur." *Susan B. Anthony List v. Driehaus*, 573 U.S. 149, 158 (2014) (quoting *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 414 n.5 (2013)). A substantial risk means a "'realistic danger of sustaining a direct injury.'" *Pennell v. City of San Jose*, 485 U.S. 1, 8 (1988) (quoting *Babbitt v. United Farm Workers Nat'l Union*, 442 U.S. 289, 298 (1979)). While plaintiffs are not required "to demonstrate that it is literally certain that the harms they identify will come about," a "possible future injury"—even one with an "objectively reasonable likelihood" of occurring—is not sufficient. *Clapper*, 568 U.S. at 409-10, 414 n.5 (emphasis omitted).

In *Reilly*, we considered whether an alleged risk of future identity theft or fraud stemming from a data breach in which an unknown hacker potentially accessed sensitive personal and financial information from a company's network was sufficiently imminent for purposes of standing. 664 F.3d 38 (3d Cir. 2011). We held that it was not. We observed that the injury alleged was a future injury as opposed to a present injury. *Id.* at 42. Consistent with *Susan B. Anthony List*, that an injury will occur in the future is not fatal to standing. 573 U.S. at 158. But where the future injury is also hypothetical, there can be no imminence and therefore no injury-in-fact.

Because the plaintiffs in *Reilly* alleged a future, hypothetical risk of identity theft or fraud, we concluded that they had not suffered an injury-in-fact. Specifically, the risk was "dependent on entirely speculative, future actions of an unknown third-party." 664 F.3d at 42. Further, we could not "describe how the [Appellants] will be injured . . . without beginning our explanation with the word 'if': *if* the hacker read, copied, and understood the hacked information, and *if* the

hacker attempts to use the information, and *if* he does so successfully." *Id.* at 43.

In holding that the *Reilly* plaintiffs lacked standing, we did not create a bright line rule precluding standing based on the alleged risk of identity theft or fraud. Such a rule would require plaintiffs to wait until they had sustained an actual injury to bring suit. This would directly contravene the Supreme Court's holding in *Susan B. Anthony List*, which authorizes suits based on a "'substantial risk' that the harm will occur." 573 U.S. at 158 Instead, *Reilly* requires consideration of whether an injury is present versus future, and imminent versus hypothetical.

Courts rely on a number of factors in determining whether an injury is imminent—meaning it poses a substantial risk of harm—versus hypothetical in the data breach context. These non-exhaustive factors can serve as useful guideposts, with no single factor being dispositive to our inquiry. Among them is whether the data breach was intentional. *See, e.g.*, *McMorris v. Carlos Lopez & Assocs.*, 995 F.3d 295, 301-03 (2d Cir. 2021) (holding that the intentional nature of an attack renders standing more likely); *Pisciotta v. Old Nat'l Bancorp*, 499 F.3d 629, 632 (7th Cir. 2007) (finding standing where a breach was "sophisticated, intentional and malicious"); *In re U.S. Off. of Pers. Mgmt. Data Sec. Breach Litig.*, 928 F.3d 42, 58-59 (D.C. Cir. 2019) (noting that "hackers targeted—and extracted data"); *In re Zappos.com, Inc.*, 888 F.3d 1020, 1029 n.13 (9th Cir. 2018) (emphasizing that hackers "specifically targeted" the data to distinguish from a case in which there was no substantial risk of identity theft).

Courts also consider whether the data was misused.[4] *See, e.g.*, *McMorris*, 995 F.3d at 301-02 (holding that misuse cuts towards standing); *Krottner v. Starbucks Corp.*, 628 F.3d 1139, 1142-43 (9th Cir. 2010) (finding standing where a laptop with personal unencrypted data was stolen and a plaintiff alleged that someone "attempted to open a bank account in his name"); *Remijas v. Neiman Marcus Grp.*, 794 F.3d 688, 692-94 (7th Cir. 2015) (finding standing where plaintiff alleged that personal data had "already been stolen" and that 9,200 people had "incurred fraudulent charges").

Of note, misuse is not necessarily required. The Seventh Circuit has found standing despite no allegations of misuse, holding that it was sufficient that a data breach "increas[ed] the risk of future harm that the plaintiff would have otherwise faced, absent the defendant's actions." *Pisciotta*, 499 F.3d at 634.

Further, courts consider whether the nature of the information accessed through the data breach could subject a plaintiff to a risk of identity theft. *See, e.g.*, *McMorris*, 995 F.3d at 302. For instance, disclosure of social security

---

[4] In accordance with *Spokeo, Inc. v. Robins*, which provides that "named plaintiffs who represent a class 'must allege and show that they personally have been injured,'" our inquiry should focus on the misuse of information particular to the *plaintiff*—not other members of the class. 578 U.S. 330, 338 n.6 (2016) (quoting *Simon v. E. Ky. Welfare Rts. Org.*, 426 U.S. 26, 40 n.20 (1976)); *but see McMorris v. Carlos Lopez & Assocs.*, 995 F.3d 295, 301-02 (2d Cir. 2021) (holding that any misuse of the data, even if the class representative has not yet been affected, cuts towards standing).

numbers, birth dates, and names is more likely to create a risk of identity theft or fraud. *Id.* (citing *Attias v. CareFirst, Inc.*, 865 F.3d 620, 628 (D.C. Cir. 2017)). By contrast, the disclosure of financial information alone, without corresponding personal information, is insufficient. *See, e.g.*, *In re SuperValu, Inc.*, 870 F.3d 763, 770-71 (8th Cir. 2017); *Tsao v. Captiva MVP Rest. Partners*, 986 F.3d 1332, 1343 (11th Cir. 2021). This is because financial information alone generally cannot be used to commit identity theft or fraud. *See In re SuperValu, Inc.*, 870 F.3d at 770-71.

b. Injury-in-fact: Concrete

The injury-in-fact prong of the standing analysis also requires that the alleged injury be "concrete," meaning "real, and not abstract." *Spokeo, Inc. v. Robins*, 578 U.S. 330, 340 (2016) (internal quotation marks omitted); *see Lujan*, 504 U.S. at 560

The Supreme Court recently clarified in *TransUnion LLC v. Ramirez* that "[c]entral to assessing concreteness is whether the asserted harm 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." 141 S. Ct. at 2200 (citing *Spokeo*, 578 U.S. at 340-41). The fact that an injury is intangible—that is, it does not represent a purely physical or monetary harm to the plaintiff—does not prevent it from nonetheless being concrete, as various intangible harms have been "traditionally recognized as providing a basis for lawsuits in American courts." *Id.* at 2204 (citing *Spokeo*, 578 U.S. at 340-41). For example, certain privacy harms, like the disclosure of private information and intrusion upon seclusion, though intangible, have long given rise to tort claims. *Id.*

The first step in assessing concreteness is to ask whether the asserted harm is adequately analogous to a harm traditionally recognized as giving rise to a lawsuit. In the data breach context, there are several potential parallels to harms traditionally recognized at common law, depending on the precise theory of injury the plaintiff puts forward. For example, if the theory of injury is an unauthorized exposure of personally identifying information that results in an increased risk of identity theft or fraud, that harm is closely related to that contemplated by privacy torts that are "well-ensconced in the fabric of American law." *In re Horizon Healthcare Servs. Inc. Data Breach Litig.*, 846 F.3d 625, 638-39 (3d Cir. 2017) (quoting David A. Elder, *Privacy Torts* § 1:1 (2016)).[5] Though such an injury is intangible, it is nonetheless concrete.

---

[5] At argument, ExecuPharm contended that any analogies to the traditional privacy torts fail because the stolen data here was not the sort of inherently private information that could have given rise to a successful privacy claim at common law. For example, the "private facts" contemplated in the tort of public disclosure of private facts would not include the transactional employee data that was exposed here.

Even if we were to accept the premise that this particular combination of stolen information could not form the basis for common law privacy tort liability—and we have no occasion to address that issue here—this mistakes the nature of the inquiry required for an assessment of Article III standing. In looking for a common law analog to an asserted theory of harm, "we do not require an exact duplicate." *TransUnion LLC v. Ramirez*, 141 S. Ct. 2190, 2209 (2021). Indeed, in *TransUnion* itself, the Supreme Court cites *Davis v. Fed. Election Comm'n*, in which the information disclosed was only

TransUnion also made clear, though, that the mere existence of a common law analog for the asserted harm does not necessarily end our inquiry. In a suit premised on the "mere risk of future harm"—that is, where the alleged injury-in-fact is "imminent" rather than "actual"—we must also consider the type of relief sought. *TransUnion LLC*, 141 S. Ct. at 2210-11. Where the plaintiff seeks injunctive relief, the allegation of a risk of future harm alone can qualify as concrete as long as it "is sufficiently imminent and substantial." *Id.* at 2210 (citing *Clapper*, 568 U.S. at 414 n.5). However, where the plaintiff seeks only damages, something more is required. Specifically, that plaintiff can satisfy concreteness where "the exposure to the risk of future harm itself causes a *separate* concrete harm." *Id.* at 2211.

---

the fact that the plaintiff had spent a certain amount of personal funds in his campaign, 554 U.S. 724, 733 (2008), as a case in which the asserted intangible harm was concrete because it was closely related to the "disclosure of private information." *TransUnion LLC*, 141 S. Ct. at 2204.

Likewise, we are content for now that the exposure of the type of information that was alleged here—information employees would normally choose to keep to themselves and would reasonably not want to make publicly available—and the resulting substantial risk of identity theft or fraud is a harm that bears at least a "close relationship" to harms traditionally recognized in privacy torts. *Id.* at 2208 (citing *Spokeo*, 578 U.S. at 341). Accordingly, the asserted injury supports Article III standing—and whether a plaintiff has successfully made out claims under a particular cause of action is a separate question.

The Supreme Court did not reach the question of what separate harms might qualify as concrete to support a substantial-risk theory of future harm in an action for damages, but it did indicate that "a plaintiff's knowledge that he or she is exposed to a risk of future . . . harm could cause its own current emotional or psychological harm," which could be sufficiently analogous to the tort of intentional infliction of emotional distress. *Id.* at 2211 n.7.

Following *TransUnion*'s guidance, we hold that in the data breach context, where the asserted theory of injury is a substantial risk of identity theft or fraud, a plaintiff suing for damages can satisfy concreteness as long as he alleges that the exposure to that substantial risk caused additional, currently felt concrete harms. For example, if the plaintiff's knowledge of the substantial risk of identity theft causes him to presently experience emotional distress or spend money on mitigation measures like credit monitoring services, the plaintiff has alleged a concrete injury.

III. Analysis

We exercise de novo review over the District Court's dismissal of a complaint for lack of subject matter jurisdiction. *Horizon Healthcare*, 846 F.3d at 632.

Clemens's complaint asserts contract, tort, and secondary contract claims—each based on the same underlying facts. "[A] plaintiff must demonstrate standing for each claim he seeks to press." *DaimlerChrysler Corp. v. Cuno*, 547 U.S. 332, 352 (2006). Accepting the well-pleaded factual allegations in Clemens's complaint as true, we hold that Clemens has standing to assert her contract, tort, and secondary

contract claims. Her alleged injuries are sufficiently imminent and concrete to qualify as injuries-in-fact.

A. Contract Claims

The District Court erred in dismissing Clemens's contract claims, which are raised in Counts III (breach of implied contract) and IV (breach of contract). These claims arise from her employment agreement with ExecuPharm. When Clemens provided ExecuPharm with her sensitive personal information upon hire, ExecuPharm expressly contracted to "take appropriate measures to protect the confidentiality and security" of this information in Clemens's employment agreement**.** J.A. 40-41 ¶¶ 57-58. Clemens alleged that ExecuPharm breached this express provision when it failed to adequately protect her information, allowing CLOP to steal sensitive employee information, hold it for ransom, and publish it on the Dark Web. Moreover, Clemens has alleged an injury stemming from the breach—the risk of identity theft or fraud—that is sufficiently imminent and concrete.[6]

As employment agreements have become routine, information security provisions like the one in the instant case have assumed a new prominence. Likewise, the failure to uphold these provisions—particularly in the digital age—can yield uniquely drastic consequences. Namely, victims of a data breach must live with the perpetual, well-founded fear and risk

[6] Because Clemens has alleged an injury separate and apart from the breach of contract itself, we have no occasion to reach her additional argument that the breach of contract alone is a sufficiently imminent and concrete injury that confers standing for her to raise her contract claims.

that hackers will misuse their data. The only way to allay those concerns is to invest time and money into precautionary measures that *could* mitigate the potential misuse, like changing one's banking information. But there is no guarantee that mitigative measures will be effective—especially given that some information, such as our names and social security numbers, generally stay with us for life.

In *Reilly*, we had occasion to discuss the contours of the injury-in-fact requirement in the data breach context. This time, the alleged injury-in-fact is far more imminent. Whereas *Reilly* involved an *unknown* hacker who *potentially* gained access to sensitive information, 664 F.3d at 42-43; here, a known hacker group named CLOP accessed Clemens's sensitive information. CLOP is a sophisticated ransomware group that is notorious for encrypting companies' internal data and placing in every digital folder a text file called "ClopReadMe.txt" that contains a message demanding ransom. J.A. 24-25 ¶ 14. These attacks are particularly threatening given that, according to a data specialist, there are "no known decryption tools for CLOP ransomware." J.A. 35 ¶ 40.

In this instance, CLOP launched its signature attack against ExecuPharm: it encrypted ExecuPharm's information and held it for ransom. Further, while the injury to the plaintiffs in *Reilly* depended upon a string of hypotheticals being borne out, 664 F.3d at 43, CLOP has already published Clemens's data on the Dark Web, a platform that facilitates criminal activity worldwide. Clemens has alleged that the Dark Web is "most widely used as an underground black market where individuals sell illegal products like drugs, weapons, counterfeit money, and sensitive stolen data that can be used to commit identity theft or fraud." J.A. 25 ¶ 15.

Because we can reasonably assume that many of those who visit the Dark Web, and especially those who seek out and access CLOP's posts, do so with nefarious intent, it follows that Clemens faces a substantial risk of identity theft or fraud by virtue of her personal information being made available on underground websites. This set of facts clearly presents a more imminent injury than the ones we deemed to establish only a hypothetical injury in *Reilly*.

Adopting and applying the factors that our Sister Circuits consider in determining imminence in the data breach context confirms this point. CLOP *intentionally* gained access to and *misused* the data: it launched a sophisticated phishing attack to install malware, encrypted the data, held it for ransom, and published it. *See McMorris*, 995 F.3d at 301-03; *Remijas*, 794 F.2d at 693-94; *Attias*, 865 F.3d at 628-29. The data was also the type of data that could be used to perpetrate identity theft or fraud. Not only did it contain financial information—which, on its own, could subject the breach victims to credit card fraud—but it also contained social security numbers, dates of birth, full names, home addresses, taxpayer identification numbers, banking information, credit card numbers, driver's license numbers, sensitive tax forms, and passport numbers. This combination of financial and personal information is particularly concerning as it could be used to perpetrate both identity theft and fraud. *See McMorris*, 995 F.3d at 302; *cf. In re SuperValu, Inc.*, 870 F.3d at 770-71 (noting that financial information, without accompanying personally identifying information, is unlikely to give rise to identity theft).

Together, these factors show that Clemens has alleged a "'substantial risk' that the harm will occur" sufficient to establish an "imminent" injury. *Anthony List*, 573 U.S. at 158

(quoting *Clapper*, 568 U.S. at 414 n.5).[7] Further, that injury is concrete, because the harm involved is sufficiently analogous to harms long recognized at common law like the "disclosure of private information." *TransUnion LLC*, 141 S. Ct. at 2204. And although the substantial risk of identity theft is a risk of future harm and this is a suit for damages, which may under other circumstances pose a problem for concreteness, *id.* at 2210-11, Clemens has alleged several additional concrete harms that she has already experienced as a result of that risk (that is, her emotional distress and related therapy costs and the time and money involved in mitigating the fallout of the data breach). Thus, her injury is also "concrete."

In addition to proving injury-in-fact, standing also requires Clemens to prove traceability and "that the injury would likely be redressed by the requested judicial relief." *Thole*, 140 S. Ct. at 1618. Traceability means that the injury was caused by the challenged action of the defendant as opposed to an independent action of a third party. *Lujan*, 504 U.S. at 560. We have yet to articulate a single standard for establishing this "causal relationship." *See Khodara Env't, Inc. v. Blakely*, 376 F.3d 187, 195 (3d Cir. 2004). Instead, we have held that but-for causation is sufficient to satisfy traceability. *See, e.g.*, *Edmonson v. Lincoln Nat'l Life Ins. Co.*, 725 F.3d 406, 418 (3d Cir. 2013). So, too, is concurrent

[7] At Oral Argument, ExecuPharm agreed that, in the abstract, facts satisfying the imminence inquiry yet falling short of actual harm could confer standing in a data breach case. However, it was unable to articulate such a scenario. If the facts in this case—which fall short of actual harm—do not meet the test for imminence, we would be hard pressed to conjure up a set of facts that would.

causation. *See, e.g.*, *Const. Party of Pa. v. Aichele*, 757 F.3d 347, 366 (3d Cir. 2014).

Here, Clemens has alleged facts that establish traceability, at least at the pleading stage. Specifically, she has identified her injuries as "a direct and proximate result of Defendants' breach" of contract: ExecuPharm's failure to safeguard her information enabled CLOP to publish it on the Dark Web as part of the stolen dataset of ExecuPharm and Parexel employee information. J.A. 65 ¶ 141, J.A. 66 ¶ 146. Likewise, Clemens satisfied redressability. As we observed in *Reilly*, the injuries caused by a data breach are "easily and precisely compensable with a monetary award," 664 F.3d at 45-46, and Clemens is seeking those damages to compensate for her losses here. This traceability and redressability analysis applies with equal force to the tort and secondary contract claims as well.

We will vacate the District Court's dismissal regarding these claims and remand for a consideration of the merits of these claims.

B. Tort Claims

In addition, the District Court erred in dismissing Clemens's tort claims, which are raised in Counts I (negligence) and II (negligence per se). The tort claims have the same factual genesis as the contract claims: namely, that ExecuPharm breached its duty to adequately safeguard sensitive employee information, which allowed CLOP to steal and misuse the data, and subjected Clemens to a substantial risk of identity theft or fraud.

In an increasingly digitalized world, an employer's duty to protect its employees' sensitive information has significantly broadened. Information security is no longer a matter of keeping a small universe of sensitive, hard-copy paperwork under lock and key. Now, employers maintain massive datasets on digital networks. In order to protect the data, they must implement appropriate security measures and ensure that those measures continue to comply with ever-changing industry standards.

Failure to satisfy this duty could leave employer networks vulnerable to data breach, subjecting data breach victims to a unique kind of harm: the perpetual risk of identity theft or fraud, necessitating the investment of time and money to hopefully mitigate that risk. With rare exception, where multiple pieces of personally identifying information about a given consumer are stolen and then publicized, one can draw a reasonable inference that the victims of the data breach face an imminent risk of identity theft or fraud. When that information is made available for download on the Dark Web—a platform that exists primarily to facilitate illegal activity—the risk that a criminal will access it and use it for a nefarious purpose is particularly acute.

As discussed *supra* in Section III Part A, Clemens's alleged risk of identity theft or fraud is sufficiently imminent. Compared to *Reilly*, the risk is not hypothetical: a known hacking group intentionally stole the information, misused it, ultimately published it on the Dark Web, and the sensitive information is the type that could be used to perpetrate identity theft or fraud. Consistent with *Anthony List*, Clemens cannot be required to wait until she has experienced actual identity theft or fraud before she can sue; the "substantial risk" that she has established is enough. 573 U.S. at 158. Her asserted injury

is also concrete, as intangible harms like the disclosure of private information qualify as concrete. *See TransUnion LLC*, 141 S. Ct. at 2204.

Because Clemens has sufficiently asserted her standing to bring her tort claims, we will vacate the District Court's dismissal and remand for a consideration of the merits of those claims.

C. Secondary Contract Claims

Finally, the District Court erred in dismissing Clemens's secondary contract claims which are raised in Counts V (breach of fiduciary duty) and VI (breach of confidence). The breach of the duties underlying these claims and the resulting harm are based on the same facts as the contract and tort claims. As with the prior claims, the District Court identified the failure to allege an imminent injury as fatal to standing.

Because we have rejected the contention that a risk of identity theft or fraud cannot qualify as sufficiently imminent, and hold that Clemens has alleged an injury-in-fact, we likewise will vacate the District Court's decision and remand for a determination of the merits of these claims.

IV. Conclusion

Clemens has standing to assert her contract, tort, and secondary contract claims. For all claims, she has alleged a future injury—the risk of identity theft or fraud—that is sufficiently imminent. The breach was conducted by a known hacking group CLOP, which intentionally stole the information, held it for ransom, and published it to the Dark

Web, thereby making it accessible to criminals worldwide. The nature of the information—a combination of personal and financial data—is the type that can be used to perpetrate identity theft or fraud. Given that intangible harms like the publication of personal information can qualify as concrete, and because plaintiffs cannot be forced to wait until they have sustained the threatened harm before they can sue, the risk of identity theft or fraud constitutes an injury-in-fact. Accordingly, we will vacate the judgment of the District Court on all counts and remand for consideration of the merits.

Clemens v. ExecuPharm Inc., No. 21-1506
PHIPPS, *Circuit Judge*, concurring in the judgment

The Majority Opinion labors through the modern tripartite test for Article III standing and concludes that Jennifer Clemens has standing to assert common-law claims for negligence, breach of contract, breach of confidence, and breach of fiduciary duty. The modern test for Article III standing, however, typically governs claims seeking to vindicate constitutional or statutory rights.[1] It has always been the rule that a litigant has standing in federal court to pursue a cause of action that was recognized as well suited for judicial resolution at the time of the Constitution's ratification:

> When a suit is made of "the stuff of the traditional actions at common law tried by the courts at Westminster in 1789" and is brought within the bounds of federal jurisdiction, the responsibility for deciding that suit rests with Article III judges in Article III courts.

---

[1] *See, e.g.*, *Spokeo, Inc. v. Robins*, 578 U.S. 330, 338–39 (2016); *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 409 (2013); *Summers v. Earth Island Inst.*, 555 U.S. 488, 493 (2009); *Friends of the Earth, Inc. v. Laidlaw Env't Servs. (TOC), Inc.*, 528 U.S. 167, 180–81 (2000); *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 560–61 (1992); *Allen v. Wright*, 468 U.S. 737, 751 (1984); *Valley Forge Christian Coll. v. Ams. United for Separation of Church & State, Inc.*, 454 U.S. 464, 472 (1982); *see also* 20 Charles Alan Wright & Mary Kay Kane, *Federal Practice and Procedure: Federal Practice Deskbook* § 14 (2d ed. Apr. 2022 update) ("The law of standing is almost exclusively concerned with public-law questions involving determinations of constitutionality and review of administrative or other governmental action.").

Stern v. Marshall, 564 U.S. 462, 484 (2011) (citation omitted) (quoting *N. Pipeline Constr. Co. v. Marathon Pipe Line Co.*, 458 U.S. 50, 90 (1982) (Rehnquist, J., concurring in judgment)); *see also Ariz. Christian Sch. Tuition Org. v. Winn*, 563 U.S. 125, 132 (2011) ("[Article III] restricts the federal judicial power 'to the traditional role of the Anglo-American courts.'" (quoting *Summers v. Earth Island Inst.*, 555 U.S. 488, 492 (2009))); *Commodity Futures Trading Comm'n v. Schor*, 478 U.S. 833, 854 (1986) ("[P]rivate, common law rights were historically the types of matters subject to resolution by Article III courts."); *N. Pipeline Constr. Co.*, 458 U.S. at 86 n.39 (plurality opinion) (stating that, "in the Framers' view, the tasks of [Article III] courts, for which independence was an important safeguard, included . . . matters of common law"); *Tenn. Elec. Power Co. v. Tenn. Valley Auth.*, 306 U.S. 118, 137 (1939) (holding that litigants have standing when "the right invaded is a legal right," such as "one of property, one arising out of contract, [or] one protected against tortious invasion"); *Murray's Lessee v. Hoboken Land & Improvement Co.*, 59 U.S. 272, 284 (1855) (explaining that "any matter which, from its nature, is the subject of a suit at the common law, or in equity" is within "judicial cognizance").[2]

The modern test builds on that principle by using traditionally recognized causes of action as a foundation for its comparative analysis. The premise of the test is that litigants

[2] *See also* Erwin Chemerinsky, *Federal Jurisdiction* 74 (8th ed. 2020) ("Injury to rights recognized at common law – property, contracts, and torts – are sufficient for standing purposes."); Cass R. Sunstein, *Standing and the Privatization of Public Law*, 88 Colum. L. Rev. 1432, 1439 (1988) (explaining that "the existence of an interest protected at common law [has been] sufficient to confer standing").

have standing for claims traditionally recognized as well suited for judicial resolution. *See TransUnion LLC v. Ramirez*, 141 S. Ct. 2190, 2204 (2021) (explaining that the concreteness component of the injury-in-fact element requires that a statutory cause of action bear a "close relationship" to a "historical or common-law analogue").[3] Thus, the modern test for Article III standing operates as a *supplement to*, not a *substitute for*, the rule that a litigant has Article III standing to bring a traditionally recognized cause of action in federal court.[4]

---

[3] *See also Hollingsworth v. Perry*, 570 U.S. 693, 700 (2013) ("As used in the Constitution, ['case' and 'controversy'] do not include every sort of dispute, but only those 'historically viewed as capable of resolution through the judicial process.'" (quoting *Flast v. Cohen*, 392 U.S. 83, 95 (1968))); *DaimlerChrysler Corp. v. Cuno*, 547 U.S. 332, 342 (2006) ("[W]e must find that the question is presented in a 'case' or 'controversy' that is, in James Madison's words, 'of a Judiciary Nature.'" (quoting 2 *Records of the Federal Convention of 1787* 430 (Max Farrand ed., 1966))); *Schlesinger v. Reservists Comm. to Stop the War*, 418 U.S. 208, 220–21 (1974) (explaining that federal courts can resolve only disputes that take "a form traditionally capable of judicial resolution").

[4] *See* F. Andrew Hessick, *Standing, Injury in Fact, and Private Rights*, 93 Cornell L. Rev. 275, 277 (2008) ("The purpose of the factual injury requirement is to ensure that plaintiffs are asserting their own private rights. The requirement therefore is superfluous in cases alleging the violation of a private right."); 20 Charles Alan Wright & Mary Kay Kane, *Federal Practice and Procedure: Federal Practice Deskbook* § 14 (2d ed. Apr. 2022 update) ("The person suing for breach of contract or for a tort must be found to be the real party in interest, but in practice those suits are brought only by a person harmed by the supposed wrong, and standing to sue is self-evident. It is

The claims that Clemens pursues here – for negligence, breach of contract, breach of confidence, and breach of fiduciary duty – are traditional causes of action that were recognized as well suited for judicial resolution at the time of the Constitution's adoption.[5] She therefore has standing. Yet by applying the modern test for Article III standing when it is unnecessary to do so, the Majority Opinion gives the mistaken impression that the modern test replaces the original understanding of what constitutes a case or controversy subject to resolution in federal court.[6]

---

only when the question is of a public nature that the interested bystander is likely to attempt suit.").

[5] *See* Robert J. Kaczorowski, *The Common-Law Background of Nineteenth-Century Tort Law*, 51 Ohio St. L.J. 1127, 1129 (1990) (explaining that some negligence claims were "in the common law for centuries," while others "primarily emerged in the last quarter of the seventeenth century"); Harold J. Berman & Charles J. Reid, Jr., *The Transformation of English Legal Science: From Hale to Blackstone*, 45 Emory L.J. 437, 460–61 (1996) (stating that "the common-law courts in the late seventeenth and early eighteenth centuries expanded the forms of action to cover . . . obligations arising from breach of contract"); Neil M. Richards & Daniel J. Solove, *Privacy's Other Path: Recovering the Law of Confidentiality*, 96 Geo. L.J. 123, 136 (2007) (describing how "[l]egal remedies for divulging . . . confidential information began to emerge as early as the eighteenth century," when "English courts of equity . . . fashion[ed] an action for breach of confidence"); Leonard I. Rotman, *Fiduciary Law's "Holy Grail": Reconciling Theory and Practice in Fiduciary Jurisprudence*, 91 B.U. L. Rev. 921, 922 (2011) ("Fiduciary law has been a part of the common law tradition since its crystallization in the landmark case of *Keech v. Sandford* in 1726.").

[6] In footnote three, the Majority Opinion asserts that its approach is consistent with binding precedent, but despite the

I cannot join that analysis, and I respectfully concur in the judgment only. It suffices for her Article III standing that Clemens brings causes of action "of the sort traditionally amenable to, and resolved by, the judicial process." *Uzuegbunam v. Preczewski*, 141 S. Ct. 792, 798 (2021) (quoting *Vt. Agency of Nat. Res. v. United States ex rel. Stevens*, 529 U.S. 765, 774 (2000)); *see also Stern*, 564 U.S. at 494 (stating that "the most prototypical exercise of judicial power" is a court's adjudication of "a common law cause of action"). Nothing more is needed.

---

abundance of precedent on Article III standing, the Majority Opinion identifies no Supreme Court case applying the modern test to a traditionally recognized cause of action.