In a Wrong Place at a Wrong Time:

Data Breach Victims and Their Standing to Sue

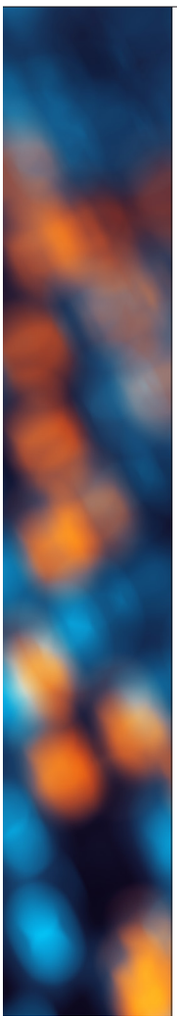
This article examines how data breaches harm, how courts grapple with them, and how the U.S. Supreme Court's decision in *Transunion v. Ramirez* may shape the determination of which harms qualify as "concrete" under Article III.

SUMMARY
Nearly everyone – other than hackers, that is – can agree that data breaches are not a good thing, especially when they involve individuals' personal information. But there is less agreement about the appropriate remedies for victims of data breaches.

Disagreement among federal courts as to the correct standard for determining remedies means that residents of some parts of the United States whose information is taken will fare better if they successfully bring suit after a breach than will residents of other areas. How courts interpret the harms that data breaches cause will affect how entities secure personal information of employees, customers, and patients and whether data-breach victims can hold them accountable for failing to secure information.

This article summarizes the history of data breaches and explains the different approaches of federal courts to data-breach cases. The author suggests that a recent U.S. Supreme Court case could have helped to resolve the circuit split but so far has not been used by federal courts to reach this result.

BY ALEX PHILLIPS



In 2018, hackers targeted a Wisconsin-based hospital system's patient files, stealing the data belonging to 1.4 million patients. It was the second breach the hospital system had suffered in two years. In both breaches, "phishing" attacks were used to pilfer patients' "protected health information" (PHI) and "personally identifiable information" (sometimes referred to as personal identifying information) (PII). The PHI and PII included patient names, Social Security numbers, and medical records.

Following the breach, two patients sued the hospital for failing to safeguard their PHI and PII, alleging the hospital's lax security systems led to the breaches. In support, the patients alleged the breach harmed them, in part, because they were at an "increased risk for future identity theft." The hospital moved to dismiss their complaint, arguing that harm did not meet the U.S. Constitution's standard for "concrete injury" under Article III.[1] But fortunately for the patients, they live in Wisconsin. Under Seventh Circuit precedent, an "increased risk for identity theft" qualifies as "concrete" under Article III. As a result, the U.S. District Court for the Western District of Wisconsin denied the hospital's motion, explaining that "the Seventh Circuit has repeatedly held that injuries like plaintiffs' injuries are sufficient to establish standing in data breach cases."[2]

Hundreds of miles away in Alabama, patients victimized in a similar attack were not so lucky. In 2019, hackers infiltrated an Alabama-based hospital system's files and stole the PHI and PII belonging to 391,472 patients, most of whom were children. Like the Wisconsin patients, the Alabama patients sued the hospital alleging they were at "an increased risk of their identities being stolen." And, as in Wisconsin, the hospital moved to dismiss on Article III grounds.

In its decision, the Alabama federal district court recognized the distress data breaches cause: "For many, the phrase 'data breach' provokes dread and invokes disquiet. Suddenly, a person's once private information roams untrammeled, and a degree of uncertainty as to its location and possessor now unexpectedly exists." But despite recognizing the "dread" and "disquiet" that data breaches cause, the district court found the patients' "increased risk" allegations were too speculative to support standing under Article III: "[Plaintiffs'] pleading speaks of possibilities and traffics in maybes."[3] As a result, the court dismissed the patients' claims for failing to establish standing.

Less than one year later, the U.S. Court of Appeals for the 11th Circuit adopted the same reasoning, finding that an "increased risk for identity theft," on its own, cannot support standing under Article III.[4]

While circuit splits are not novel, data breaches are a relatively recent phenomenon, and they require courts to rethink what qualifies as "harm." Indeed, how courts interpret the "harms" that data breaches cause will affect how entities secure PHI and PII and whether data-breach victims can hold them accountable for failing to secure information. This article examines the harms caused by data breaches, how courts grapple with breaches and resulting

suits, and how the U.S. Supreme Court's decision in *Transunion v. Ramirez* may shape determination of which harms qualify as "concrete" under Article III.

Data Breaches Through History

In 1834, two bankers hacked the French government's telegraph lines to steal information about the Parisian stock market. In what would be considered the world's first "data breach," accomplices sent the bankers coded messages about the market's movements, capitalizing on the telegraph's speed while their competitors corresponded by mail. The bankers profited from their hack for two years – until an accomplice turned them in.[5] Although successful, the hack and the "harm" it caused were small, given the limited technology in 1834.

Over the ensuing decades, the data environment evolved and so too did the threat that breaches pose. By the 1980s, people started digitizing data, storing it on appliance-sized hard drives that occupied entire rooms. Despite their size, the drives spared entities and individuals from having to save data on paper in even bigger filing cabinets and warehouses.

But with greater capacity came greater risk. In 1984, the New York Times reported on the first digital data breach, which exposed the credit histories of about 90 million U.S. residents.[6] Hackers accessed the reports after stealing a notepad that had the password written on it.[7] Although hackers only used the data to manipulate credit scores and open accounts, it is not hard to imagine that exposing 90 million credit histories could harm people.

By 2005, the need for big data had grown, and so too did the desire to steal it. In what would be the first modern data breach, hackers stole 1.4 million consumer account numbers from shoe retailer DSW, using the data to fraudulently charge consumers' accounts.[8] A few months later, hackers targeted CardPayment Solutions, dwarfing the DSW breach by exposing over 40 million account numbers.[9] Data breaches had become a regular part of life.

Today, data breaches happen nearly every day. Hackers target hospitals, banks, retailers, and governmental agencies and entities to steal PHI and PII. Although the attacks vary by type (ransomware, malware, and phishing), they all exploit an entity's security vulnerabilities. When the attacks succeed, the hackers hold the data ransom, sell it on the dark web, or both.

On the dark web, criminals repackage stolen PHI and PII with data from other breaches to create "fullz" packages. A fullz package is a "dossier on a person's identity, including their contact information, Social Security number, account log-in information, and account numbers."[10] Once complete, fullz packages typically sell for between $8 and $1,767, depending on the information involved.[11] Because PHI and PII can circulate on the dark web indefinitely, hackers might create a fullz package and capitalize on victims' stolen identities several years after a breach.

Harms Caused by Data Breaches

Given that misuse of data might occur or the threat of misuse might continue for a long time, sometimes data-breach victims sue the breached entity for failing to safeguard their data. In so doing, they generally allege the harms below:

• **Identity theft**: Identity theft happens when someone steals PII or PHI to commit fraud, such as opening financial accounts or stealing income tax returns. Plaintiffs allege this harm when they suffer identity theft following a data breach.

• **Increased risk for identity theft:** An "increased risk for identity theft" refers to identity theft that is "imminent" under the circumstances. Plaintiffs allege "imminency" by showing that hackers have tried to steal their identities, that other class plaintiffs suffered identity theft, or that the stolen data

Alex Phillips, U.W. 2017, is with Turke & Strauss LLP, Madison. His practice focuses on commercial litigation, class actions, and employment law. Access the digital article at www.wisbar.org/wl.

alexp@turkestrauss.com

was especially "sensitive," for example, information such as Social Security and financial account numbers.

• **Money spent mitigating risks**: After a breach, consumers often buy credit monitoring or other services to guard against identity theft. Plaintiffs claim these costs as damages in data-breach lawsuits.

• **Time spent mitigating risks**: Monitoring for identity theft following a data breach takes time, including in changing account numbers, checking bank statements, and freezing credit reports. Some courts recognize this as an "opportunity cost" that plaintiffs can recover as damages.

• **Diminished value of PII or PHI**: A person's PHI and PII have value that hackers exploit when selling it on the dark web. Plaintiffs allege that exposing their PII or PHI diminishes its value and they might demand the reduction in value as damages.

• **Emotional harm**: In ransomware hacks, cybercriminals sometimes target medical records because they know that the PHI might be considered sensitive by the entity and the victim. Exposing this information distresses victims, who might claim emotional-harm damages.

Whether these "harms" support Article III standing in data-breach cases often depends on where a plaintiff lives.

Article III Standing in Data-Breach Cases

In cases brought in federal courts, plaintiffs must establish their standing to sue under Article III of the U.S. Constitution. To do so, plaintiffs must show the following: "(i) that [they] suffered an injury in fact that is concrete, particularized, and actual or imminent; (ii) that the injury was likely caused by the defendant; and (iii) that the injury would likely be redressed by judicial relief."[12] In other words, a plaintiff must allege the harm, that the defendant caused it, and that the district court has the power to provide relief for the plaintiff.

In data-breach cases, defendants most often challenge a plaintiff's standing on the first prong — whether they suffered a "concrete injury." A concrete injury must be "real, and not abstract."[13] Such harms include physical damages and monetary losses — tangible harms that courts readily recognize as "real." But courts also recognize that some harms are *intangible* but no less real: "Various intangible harms can also be concrete [...] Those include, for example, reputational harms, disclosure of private information, and intrusion upon seclusion."[14] Either way, such harms must be "sufficiently imminent," in that they cannot be "too speculative."[15]

Federal courts differ in how they address data breaches and data-breach victims, whose injuries are often likely but not certain.

In answering this question, federal courts of appeal fall into two groups. In the first group, the Third, Sixth, Seventh, Ninth, and D.C. Circuits have set perhaps the most "realistic" threshold for establishing standing in data-breach cases, holding that plaintiffs need only allege a breach of sensitive information to support standing.

The Seventh Circuit articulates a standard that accommodates all or most of the harms plaintiffs allege in data-breach cases. For example, in *Lewert v. P.F. Chang's China Bistro Inc.*, the court explained that when criminals steal consumer data, consumers should not have to wait for criminals to "misuse" it before they can sue. Relying on an earlier holding, the Seventh Circuit explained: "The plaintiffs should not have to wait until hackers commit identity theft or credit-card fraud in order to give the class standing, because there is an 'objectively reasonable likelihood' that such injury will occur."[16] Applying this standard, the court found that data-breach victims could allege identity theft, an "increased risk of identity theft," and the costs and time to mitigate that risk to support standing.

In the second group, the Second, Fourth, Eighth, and Eleventh Circuits set the bar somewhat higher for data-breach plaintiffs. As the Fourth Circuit has explained, a breach alone will not support standing: "the mere theft of [data], without more, cannot confer Article III standing."[17] In some circuits, plaintiffs might need to allege "actual misuse" of their data, showing not only that the data was stolen but also that it was "misused" in some way. Still, those

courts acknowledge that plaintiffs' claims can survive without plaintiffs showing misuse if they allege hackers "targeted" their "sensitive data."[18] Plaintiffs who cannot make this showing might "render[] their contention of an enhanced risk of future identity theft too speculative." In other words, plaintiffs might have to wait until identity theft or other "misuse" occurs before suing in these circuits, an eventuality that can take years to arrive.

But whether this split persists depends on how the federal courts of appeal apply the U.S. Supreme Court's decision in *TransUnion v. Ramirez* to data-breach cases.

TransUnion LLC v. Ramirez and the Future

The split among the federal courts of appeal developed before the U.S. Supreme Court decided *TransUnion* in 2021. Going forward, the *TransUnion* precedent might shape how the federal appellate courts apply their standards to data-breach cases. Although *TransUnion* concerned Fair Credit Reporting Act (FCRA) violations, not data breaches, its holding clarified how the Court applies Article III standing to "future harms."

The *TransUnion* plaintiffs alleged that TransUnion included errors in their credit reports, sharing some of those reports with third parties and keeping the others internally. The Court held that the plaintiffs in the first group (those whose reports were shared with third parties) had standing because TransUnion disclosed their errant reports. But the Court held that the plaintiffs in the second group (those whose reports were kept internally by TransUnion) could not establish standing because no one saw their reports and thus these plaintiffs suffered no harm.

Although the plaintiffs in the second group argued that they were "at risk" for harm, the Court held that their risk was too speculative to support standing because they did not show "a serious likelihood of disclosure" and courts "cannot simply presume a material risk of concrete harm." In other words, the plaintiffs could not establish standing because they could not show it was "likely" that TransUnion would disclose their errant reports.

TransUnion raised more questions than it answered in the data-breach context. Although the Court might have narrowed the window for data-breach plaintiffs to argue standing, courts deciding standing questions continue to apply the same standards they used before *TransUnion* was issued.[19]

More to the point, the extent to which *TransUnion* applies to data-breach cases is unclear. First, *TransUnion* applied to undisclosed credit reports, not stolen PII or PHI, which is by its nature "disclosed." Second, *TransUnion* turned on the

"substantial likelihood" that TransUnion would share plaintiffs' errant reports, which appeared unlikely: "Nor did the plaintiffs demonstrate that there was a sufficient likelihood that TransUnion would otherwise intentionally or accidentally release their information to third parties."

The same is not true in data breaches, in which stealing and misusing consumer data is the point. As the Seventh Circuit put it: "Why else would hackers break into a store's database and steal consumers, private information? Presumably, the purpose of the hack is, sooner or later, to make fraudulent charges or assume those consumers' identities."[20] As a result, it seems the circuit split might continue despite *TransUnion*.

Conclusion

As data breaches continue to occur, the harm they cause consumers will increase. Regulatory authorities cannot keep pace with this growth,[21] meaning the burden often falls to consumers to seek relief in court. When they do, whether they recover will depend on how seriously they were harmed by a breach and the approach of the federal court in which they can bring suit — a circumstance unlikely to change until the Supreme Court applies Article III to data-breach cases. **WL**

ENDNOTES

[1]*Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560-61 (holding that to have Article III standing to sue in federal court, a plaintiff must show they suffered a "concrete" injury in fact).

[2]*Fox v. Iowa Health Sys.*, 399 F. Supp. 3d 780, 790 (W.D. Wis. 2019).

[3]*Blahous v. Sarrell Reg'l Dental Ctr. for Pub. Health Inc.*, No. 2:19-CV-798-RAH-SMD, 2020 WL 4016246, at *6 (M.D. Ala. July 16, 2020).

[4]*Tsao v. Captiva MVP Rest. Partners LLC*, 986 F.3d 1332, 1344 (11th Cir. 2021).

[5]Schneier on Security, *1834: The First Cyberattack* (May 31, 2018), www.schneier.com/blog/archives/2018/05/1834_the_first_.html; U.S. Secs. & Exch. Comm'n, *Remarks on Cybersecurity and Securities Laws at the Northwestern University Pritzker School of Law* (Jan. 24, 2022), www.sec.gov/news/speech/gensler-cybersecurity-and-securities-laws-20220124.

[6]Stuart Diamond, *Credit File Password Is Stolen*, N.Y. Times (June 22, 1984), www.nytimes.com/1984/06/22/business/credit-file-password-is-stolen.html (behind paywall for some readers).

[7]David Kalat, *Nervous System: The First Major Data Breach: 1984*, BRG (Dec. 8, 2020), www.thinkbrg.com/insights/publications/kalat-first-major-data-breach/.

[8]Fed. Trade Comm'n, *DSW Inc. Settles FTC Charges* (Dec. 1, 2005), www.ftc.gov/news-events/news/press-releases/2005/12/dsw-inc-settles-ftc-charges.

[9]Eric Dash, *Lost Credit Data Improperly Kept, Company Admits*, N.Y. Times (June 20, 2005), www.nytimes.com/2005/06/20/technology/lost-credit-data-improperly-kept-company-admits.html (behind paywall for some readers).

[10]SEON, *What Are Fullz?* https://seon.io/resources/dictionary/fullz/ (last visited Dec. 2, 2022).

[11]Securities, *A Look Into the Pricing of Stolen Identities for Sale on Dark Web* (Jan. 22, 2021), www.securitymagazine.com/articles/94405-a-look-into-the-pricing-of-stolen-identities-for-sale-on-dark-web (unlimited access available only for registered users).

[12]*Defenders of Wildlife*, 504 U.S. at 560-61.

[13]*Spokeo Inc. v. Robins*, 578 U.S. 330, 340 (2016) (internal quotation marks omitted).

[14]*TransUnion LLC v. Ramirez*, 141 S. Ct. 2190, 2204 (2021).

[15]*Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 409 (2013) (quoting *Defenders of Wildlife*, 504 U.S. at 565 n.2).

[16]*Lewert v. P.F. Chang's China Bistro Inc.,* 819 F.3d 963, 966 (7th Cir. 2016).

[17]*Beck v. McDonald*, 848 F.3d 262, 275 (4th Cir. 2017).

[18]*McMorris v. Carlos Lopez & Assocs. LLC,* 995 F.3d 295, 303 (2d Cir. 2021).

[19]Molly McGinnis Stine & Tara Trifon, *Business as Usual – so Far – for Data Breach Cases After TransUnion LLC v. Ramirez*, JD Supra (Oct. 6, 2021), www.jdsupra.com/legalnews/business-as-usual-so-far-for-data-1312599/.

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

[21]Ben Leonard, *Hackers Have Laid Siege to U.S. Health Care and a Tiny HHS Office Is Buckling under the Pressure*, Politico (Aug. 28, 2022), www.politico.com/news/2022/08/28/hackers-have-laid-siege-to-u-s-health-care-and-a-tiny-hhs-agency-is-buckling-under-the-pressure-00053941. **WL**