NOVEMBER 21, 2025

Data breach class actions: Fourth Circuit charts its own course in data breach standing ruling

by James F. Bogan III

Takeaway: For Article III standing purposes, an injury-in-fact must be "concrete." Tangible harms, such as physical injury and monetary loss, are obviously concrete injuries. But data breach litigation usually involves allegations of intangible harm, namely, the improper disclosure of information. In those cases, determining whether an intangible harm rises to the level of a "concrete" injury can be difficult, leading different courts to reach different decisions on similar fact patterns. In a recent data breach case, *Holmes v. Elephant Ins. Co.*, --- F.4th ----, No. 23-1782, 2025 WL 2907615 (4th Cir., Oct. 14, 2025), a Fourth Circuit panel charted its own course, recognizing that its decision was at odds with decisions by other courts of appeals.

Holmes involves data breach claims alleged against Elephant Insurance and affiliated companies ("Elephant") that sell car and home insurance, among other types of insurance policies. Elephant maintains a database of personal information such as driver's license numbers, which it obtains from DMV records. To facilitate the insurance application process, Elephant's on-line platform "auto-populates" driver's license numbers when other personal information is entered (such as name and date of birth).

In 2022, hackers breached Elephant's network, exposing the driver's license numbers of nearly 3 million individuals. After the breach, Elephant delivered notices of the data breach to all impacted individuals, offering (among other things) a year of free credit monitoring.

In a consolidated class action complaint filed in the Eastern District of Virginia, four putative class representatives asserted claims against Elephant, asserting four alleged injuries-in-fact arising from the data breach: "(1) the actual compromise of their personal information in the breach; (2) the risk of future misuse of their personal information by other malicious actors; (3) the risk of having their personal information taken again in the future in another hack of Elephant; and (4) the emotional distress and time spent monitoring their financial records to mitigate the likelihood of future harm." *Holmes*, 2025 WL 2907615, at *3.

Two of the plaintiffs alleged that their driver's license numbers were listed on the dark web; the other two plaintiffs merely alleged that their driver's license numbers had been obtained by the unnamed hackers.

The district court concluded that all four plaintiffs had failed to sustain an injury-in-fact and dismissed the consolidated class action complaint in its entirety.

On appeal, a Fourth Circuit panel reversed the district court in part, concluding that the class representatives who alleged that their data had made it onto the dark web had sufficiently alleged an Article III injury-in-fact supporting a claim for damages.

To put the arguments in procedural context, the panel observed that "a plaintiff must demonstrate standing separately for each form of relief sought." *Id*. at *2 (quoting *Friends of the Earth, Inc. v. Laidlaw Env. Servs. (TOC), Inc.*, 528 U.S. 167, 185 (2000)). "So a plaintiff could, for example, have standing to seek damages from the defendant but lack standing to seek an injunction." *Id*.

The panel applied the *TransUnion* "harm-analogue test." *See TransUnion LLC v. Ramirez*, 594 U.S. 413 (2021). Quoting *TransUnion*, the panel observed that, for an intangible injury such as data disclosure to qualify as a "concrete" injury under Article III, the harm must bear "a close relationship to harms traditionally recognized as providing a basis for lawsuits in American courts." *Id*. at *3. The most analogous harm was the harm addressed by the common law tort of public disclosure of private information, which requires that a defendant "(1) disclose (2) to the public (3) true but private information that would be highly offensive to a reasonable person and (4) is otherwise of no legitimate concern to the public." *Id*. at *5.

In evaluating this common law tort, the panel emphasized that the tort was not concerned with disclosures to small groups of people; rather, the harm required a *public* disclosure: "Overall, the public disclosure of private information is aimed at the harm that occurs when sensitive personal information is released *into the open*." *Id*. at *6 (emphasis added).

Publication on the dark web qualified as a sufficiently *open* disclosure, said the panel, while the acquisition of the information by the unnamed (and uncounted) hackers did not – plaintiffs did "not allege that the unnamed hackers [were] so numerous as to constitute the public on their own." *Id*. at *7.

At two points along the way in its application of the "harm-analogue test," the Fourth Circuit panel disagreed with rulings by other circuit courts. First, in rejecting Elephant's argument that a driver's license number was not the type of "sensitive information" qualifying for protection under the common law tort, the panel disagreed with the ruling in *Baysal v. Midvale Indemnity Co.*, 78 F.4th 976, 977 (7th Cir. 2023), in which the Seventh Circuit concluded that "[a] license number is not viewed as embarrassing . . . or private . . . but as neutral." *Id*. at *8 (quoting *Baysal*, 78 F.4th at 979). But *Baysal* acknowledged that a social security number qualified as "sensitive information." The Fourth Circuit panel "[saw] things differently," concluding that a driver's license number was similar in nature to a social security number, even though a driver's license number may be *less* private than a social security number. *Id*. at *9.

Second, in rejecting the plaintiffs' argument that publication on the dark web meant that future misuse of information was sufficiently "imminent" (i.e., sufficient to support a grant of injunctive relief), the panel disagreed with decisions by the First, Second, Seventh, and D.C. Circuits. *Id*. at *13. The panel concluded that while a dark web disclosure might present "a reasonable probability of future harm," such disclosure

did not present the "imminent harm" required for a grant of injunctive relief under the Supreme Court's decision in *Clapper v. Amnesty Int'l USA* , 568 U.S. 398 (2013). The panel concluded: "The plaintiffs may have alleged enough to show that the risk of future misuse is an imminent injury before other courts. But they have not done so before this one." *Id*.

Finally, the panel easily rejected the other two alleged harms alleged by the plaintiffs. Having failed to demonstrate an imminent injury sufficient to support the grant of injunctive relief, the plaintiffs' allegations did not establish that another data breach would occur at Elephant; and without a separate imminent injury, they could not recover damages for time addressing the risk or the emotional distress they felt as a result of it. *Id*. at *13-*16.