NOVEMBER 30, 2022

Data breach class actions: SDNY finds standing based on sketchy injury-in-fact allegations

by James F. Bogan III

Takeaway: Ever since the U.S. Supreme Court ruled in *Clapper v. Amnesty Int'l USA* , 568 U.S. 398, 416 (2013), that plaintiffs "cannot manufacture standing merely by inflicting harm on themselves based on . . . hypothetical future harm," courts have endeavored to ascertain the line between "imminent" and "hypothetical" harm in data breach and other cases alleging intangible harm. We have written extensively about these issues, including a recent article about the district court's decision in *Webb v. Injured Workers Pharmacy, Inc.*, No. 22-10797-RGS, 2022 WL 10483751 (D. Mass. Oct. 17, 2022), where we believe the district court correctly dismissed the action for lack of standing. *See Data breach class actions: District of Massachusetts dismisses complaint for failure to allege injury-in-fact* (Oct. 28, 2022). Recently, the Southern District of New York found that standing existed in another data breach class action, *Rand v. Travelers Indemnity Co.*, No. 21 CV 10744 (VB), 2022 WL 15523722 (S.D.N.Y. Oct. 27, 2022), based on (in our view) dubious injury-in-fact allegations. Any questionable standing ruling puts the parties to the risk of litigating issues to their full conclusion, ultimately to discover on appeal that the district court never had jurisdiction to begin with.

The *Rand* decision involves websites offering instant automobile insurance premium quotes that are maintained by The Travelers Indemnity Company (Travelers) and other insurance carriers. They do this by drawing information from state department of motor vehicles (DMVs) or other entities that receive personal identifying information (PII) from DMVs. The websites enable insurance agents to input minimal information about a potential insured, such as a name, address, and date of birth, after which the website "auto-populates" with other PII – such as the individual's driver's license number – to generate an instant premium quote.

The New York State Department of Financial Services issued alerts to Travelers and other companies warning that cybercriminals were targeting these websites to steal drivers' license numbers. These alerts recommended security measures to prevent the "serious risk of theft and consumer harm" posed by these websites. *Rand,* 2022 WL 15523722, at *1.

Jennifer Rand was not an insured of Travelers and never herself applied for Travelers automobile insurance. But she received a notice from Travelers "that an unauthorized party may have accessed her name, address, date of birth, and driver's license number by improperly using the credentials of Travelers agents to access Travelers's agency portal." *Id.* Travelers then offered Ms. Rand complimentary credit monitoring and identity theft services for a period of one year.

After receiving this notice, Ms. Rand sprang into action by taking various steps and incurring various costs to address her risk of future harm, such as costs associated with credit freezes and costs to purchase additional credit monitoring and identity theft services.

She then filed a putative class action against Travelers based on the alleged improper disclosure of her

PII to cybercriminals, asserting statutory claims under the federal Driver's Privacy Protection Act and Section 349 of the New York State General Business Law, as well as common law claims for negligence and negligence per se.

Travelers moved to dismiss, including on the ground that Ms. Rand did not have standing because she did not suffer an Article III injury-in-fact. (Travelers also moved to dismiss Ms. Rand's claims for failure to state claim, which this article does not discuss. That motion was granted in part and denied in part.) In its standing analysis, the district court applied the Second Circuit's decision in *McMorris v. Carlos Lopez & Associates, LLC,* 995 F.3d 295 (2d Cir. 2021). As we explained in a prior article, *McMorris* developed a three-factor test to determine whether a data breach plaintiff has suffered an injury-in-fact. *See Data breach class actions: Second Circuit sets out parameters for Article III injury-in-fact* (May 28, 2021). Those three factors are "(1) whether the plaintiffs' data has been exposed as the result of a targeted attempt to obtain that data; (2) whether any portion of the dataset has already been misused, even if the plaintiffs themselves have not yet experienced identity theft or fraud; and (3) whether the type of data that has been exposed is sensitive such that there is a high risk of identity theft or fraud." *Rand*, 2022 WL 15523722, at *3 (quoting *McMorris*, 995 F.3d at 303).

The Second Circuit issued *McMorris*, however, before the Supreme Court's decision in *TransUnion LLC v. Ramirez*, 141 S. Ct 2190 (2021). As the district court noted, "*McMorris*, decided before *TransUnion*, suggested that a sufficiently imminent risk of identity theft, standing alone, could constitute injury-in-fact, 'even in a suit for damages.'" *Rand*, 2022 WL 15523722, at *4 n.2. But, as the district court observed, it appears that *TransUnion* "abrogated this holding in suits for damages by requiring both an imminent risk of future harm and a concrete injury related to the risk." *Id*. (citation omitted). The court nevertheless relied on *McMorris* as a guide to ascertain the "imminence" of future harm.

Ms. Rand argued that she suffered an injury-in-fact from (1) an alleged loss of privacy and (2) harm suffered from efforts to mitigate the risk of future harm. Regarding the loss of privacy, the district court noted that "an injury-in-fact must bear 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.'" *Id*. at *3 (quoting *TransUnion*, 141 S. Ct. at 2200). According to the district court, Ms. Rand's alleged loss of privacy was analogous to the common law tort of public disclosure of private information. "The privacy tort applies when 'one gives publicity to a matter concerning the private life of another,' so long as the 'matter publicized is of a kind that (a) would be highly offensive to a reasonable person, and (b) is not of legitimate concern to the public.'" *Id*. at *4 (quoting *Restatement (Second) of Torts* § 652(D)). But "it is not enough 'to communicate a fact concerning the plaintiff's private life to a single person or even to a small group of persons.'" *Id*. at *4 n. 3 (again quoting *Restatement (Second) of Torts* § 652(D)).

The court ruled that Ms. Rand's allegations satisfied the elements of the tort of public disclosure of private information, although its analysis raises several questions. First, the court appeared to assume without any discussion that the notice from Travelers that a third party "may have accessed" her information demonstrated that cybercriminals did in *fact* access Ms. Rand's PII. *Id*. at *4.

Second, the court appeared to conflate Travelers's *intended* disclosure of PII to Travelers agents accessing Travelers's agency portal, on the one hand, and Travelers's *unintended* disclosure of PII to cybercriminals posing as Travelers agents (using stolen credentials), on the other. *Id*.

Third, the court muddled through the tort's requirements that the disclosure be "highly offensive to a

reasonable person" and also be "sufficiently public." *Id*. It is difficult to see how Travelers – like Ms. Rand, a data breach victim – engaged in highly offensive conduct, and (as for the "sufficiently public" requirement) the court had no idea how extensive the alleged disclosure was. One cybercriminal? More?

The district court's analysis of the costs incurred by Ms. Rand to mitigate the risk of future identify theft was similarly problematic.

Addressing the three *McMorris* factors, the court recognized that Ms. Rand did not allege that her PII had been misused, and she did not allege that anyone attempted to misuse her data. But the court nevertheless found that consideration of the first and third *McMorris* factors "support[ed] a determination that [Ms. Rand's] risk of future identity theft is sufficiently imminent and substantial such that the costs incurred to mitigate that risk constitute an independent injury-in-fact." *Id*. at *5.

Regarding the first factor ("whether the plaintiffs' data has been exposed as the result of a targeted attempt to obtain that data"), the court again appeared to assume that Ms. Rand's data was in fact misappropriated by one or more cybercriminals in a targeted attack, despite Travelers only having provided notice her PII "may have" been accessed. Regarding the third factor ("whether the type of data that has been exposed is sensitive such that there is a high risk of identity theft or fraud"), the court accepted Ms. Rand's allegation that a driver's license number is sufficiently "sensitive," but it based its ruling in part on "the allegation that third parties had already improperly obtained *and misused* plaintiff's personal information to access the agency portal in the first instance" (*id*. at *5 (emphasis added)), despite recognizing earlier in its opinion that there was no allegation of misuse or attempted misuse of Ms. Rand's PII.

Moreover, the district court appeared to endorse Ms. Rand's purchase of *additional* credit monitoring and identity theft services with no indication that the complimentary services offered by Travelers were in any way deficient.

Ultimately, in what it acknowledge was a "close call," the court ruled that Ms. Rand alleged "an imminent risk of future identity theft," such that "the financial costs plaintiff allegedly incurred mitigating that risk constitute[d] an independent injury-in-fact." *Id*. at *5.