Cooley

Second Circuit Rules Individuals Have Standing to Sue for 'Increased Risk' of Identity Theft

April 30, 2021

Earlier this week, the United States Court of Appeals for the Second Circuit held that where personal information is disclosed without authorization, impacted individuals may have standing to sue if they can show an "increased risk" of identity theft or fraud, even if this hasn't yet happened. The court, which had not before decided if plaintiffs could establish standing based on the risk of *future* identity theft or fraud resulting from the unauthorized disclosure of their data, articulated a non-exhaustive three-factor test: (1) whether the data was compromised as part of a targeted attack intended to obtain the plaintiff's data; (2) whether at least some part of the compromised data set was misused (even if the plaintiff's data was not); and (3) whether the type of data at issue is likely to cause a risk of perpetual identity theft or fraud.

The case, *McMorris v. Carlos Lopez & Assocs., LLC*, No. 19-4310, ____ F.3d ____, 2021 WL 1603808 (2d Cir. Apr. 26, 2021), involved an inadvertent mass email where one of the defendant's employees sent a spreadsheet containing 130 current and former employees' Social Security numbers, home addresses, dates of birth, telephone numbers, educational degrees and dates of hire to all of the company's 65 employees. Three employees whose information was circulated brought a putative class action against their employer alleging state-law negligence claims and consumer protection violations. The plaintiffs did not allege that the disclosure of their personal information had resulted in identity theft, fraud or misuse by any third party. They also did not claim that anyone outside the company had obtained their information. Instead, the plaintiffs claimed they faced an "imminent risk" of identity theft, which forced them to take mitigation steps, including purchasing identity theft protection services, canceling credit cards and spending time assessing if they should apply for new Social Security numbers (although they had not actually applied for the new Social Security numbers).

To have constitutional standing to bring a federal suit, a plaintiff must allege: (1) an actual injury that is concrete, particularized, and actual or imminent; (2) that the injury was caused by the defendant; and (3) that the injury is likely to be redressed by the requested relief. Defendants moved to dismiss the case for lack of standing and argued that a risk of future identity theft was too speculative to be a concrete, particularized, imminent injury. Before the motion could be decided, the parties reached an agreement to settle the case. However, the district court ordered further briefing on standing before it would hold a hearing to consider the fairness of the class action settlement, and ultimately dismissed the case for lack of standing instead of approving the settlement. Plaintiffs appealed, arguing they had standing based on an "imminent risk of suffering identity theft." They also argued that the mitigation measures they had taken equaled actual harm, supplying an independent basis for standing.

When analyzing the question of standing based on the risk of future identity theft or fraud from the disclosure of personal data, the Second Circuit surveyed the law in other federal circuits. It noted "no court of appeals has explicitly foreclosed plaintiffs from establishing standing based on a risk of future identity theft," but acknowledged courts had found lack of standing based on the facts of particular cases. *McMorris*, 2021 WL 1603808, at *3.[1]

The Second Circuit therefore characterized its decision as one that "join[s] . . . sister circuits that have specifically addressed the issue in holding that plaintiffs may establish standing based on an increased risk of identity theft or fraud following the unauthorized disclosure of their data." *Id.* at *3. The Second Circuit put forward a "non-exhaustive" list of factors that courts should consider when assessing standing in the context of unauthorized disclosure of data:

1. Whether the data was compromised as a result of a targeted attack intended to obtain plaintiffs' data;
2. Whether some portion of the compromised data set has already been misused, even if the plaintiffs' data was not; and
3. Whether the compromised data is of a type that is "likely to expose plaintiffs to a perpetual risk of identity theft or fraud" once exposed.

Applying these factors, the Second Circuit determined plaintiffs did not have standing to sue because they "failed to show that they are at a substantial risk of future identity theft or fraud." *Id.* at *5. (It is worth remembering that the trigger for the lawsuit was an accidental all-employee email that contained a spreadsheet with employee personally identifiable information.) The court quickly disposed of the first factor – targeted attack – because there was none. As for the second factor – evidence of misuse – the court noted that plaintiffs did not allege any facts suggesting their data was misused. Regarding the third factor – the likelihood of perpetual identity theft or fraud – the court recognized that Social Security numbers, coupled with names, addresses and dates of birth "might put Plaintiffs at a substantial risk of identity theft or fraud." *Id.* at *6. But, because plaintiffs did not allege "any other facts suggesting that the PII was intentionally taken by an unauthorized third party or otherwise misused," the sensitivity of the data, standing alone, was not sufficient to establish an injury in fact. For this reason, the court ultimately found plaintiffs lacked Article III standing.

On one hand, *McMorris* poses clear hurdles for data breach class actions in the Second Circuit because it will be difficult for plaintiffs to plead sufficient facts showing that the purpose of any given cyberattack was to target *their* data. (It would be easier to make this showing in financially motivated cyberattacks.) On the other hand, given the ubiquity of data breaches and inadvertent emails, it should not be particularly difficult for plaintiffs to allege that some portion of a compromised data set has already been misused. For example, a plaintiff whose personal data was compromised and who later receives an early fraud warning from their credit card issuer could plausibly allege misuse. And depending on the type of data at issue, *McMorris* may spur even more class actions because of the court's recognition that the sensitivity of the data exposed, by itself, may be enough to establish standing. Finally, the three-factor test gives courts plenty of leeway because no one factor is dispositive.

Notes

1. For example, in *In re SuperValu, Inc.,* 870 F.3d 763, 773 (8th Cir. 2017), the Eighth Circuit found certain plaintiffs lacked standing to sue because they failed to allege that their disclosed credit card information had been misused, but declined to hold that evidence of misuse following a data breach was necessary to establish standing. Similarly, in *Tsao v. Captiva MVP Rest. Partners, LLC,* 986 F.3d 1332, 1340 (11th Cir. 2021), the Eleventh Circuit held "evidence of actual misuse is not necessary for a plaintiff to establish standing following a data breach." However, in *Reilly v. Ceridian Corp.*, 664 F.3d 38, 45 (3d Cir. 2011), the Third Circuit held that "in data breach cases where no misuse is alleged . . . there has been no injury[.]"). The Second Circuit noted that the *Reilly* court did not "reject the 'increased-risk' theory altogether," and instead distinguished analogous cases on their facts. *McMorris*, 2021 WL 1603808, at *3 n2.

Key Contacts

Tiana Demas	tdemas@cooley.com +1 212 479 6560
Travis LeBlanc Washington, DC	tleblanc@cooley.com +1 202 728 7018

Bethany Lobo San Francisco	blobo@cooley.com +1 415 693 2187
Sarah M. Egoul New York	segoul@cooley.com +1 212 479 6451