Published on *The National Law Review* https://natlawreview.com

Circuit Split No More: 2nd Circuit Clarifies Article III Standing in Data Breach Cases

Article By:

Cybersecurity & Privacy Practice Group

While more states push forward on new privacy legislation statutorily granting consumers the right to litigate control of their personal information, federal courts continue to ponder how data breach injury fits traditional standing requirements. Previous to McMorris v. Carlos Lopez, McMorris v. Carlos Lopez & Assocs., LLC, many have argued there was a circuit split regarding whether an increased risk of identity theft resulting from a data breach is sufficient to establish Article III standing. However, in *McMorris*, the Second Circuit denied any confusion among its sister courts. Rather, the Second Circuit interestingly held that all courts have technically allowed for the possibility that an increased risk of identity theft could establish standing, but no plaintiff has yet hit the mark. Despite implying that standing could hypothetically exist in certain cases, however, the Second Circuit nonetheless found that McMorris fell short.

Devonne McMorris was an employee at a veteran's health services clinic, Carlos Lopez & Associates LLP (CLA). In 2018, a CLA employee mistakenly sent an email to other CLA employees containing a spreadsheet with sensitive personally identifiable information (PII), including, but not limited to, Social Security numbers, home addresses, and dates of birth of McMorris and over 100 other CLA employees. McMorris and other class-action plaintiffs filed suit claiming that this purported breach caused them to cancel credit cards, purchase credit monitoring and identity theft protection services, and assess whether to apply for new Social Security numbers. The class-action plaintiffs reached a settlement with CLA, but when sent to the district court for approval, the United States District Court for the Southern District of New York rejected the parties' agreement for lack of Article III standing. Only McMorris appealed to the Second Circuit.

The Holding

After reviewing recent decisions delivered by other circuits regarding standing and an increased risk for identity theft, the Second Circuit denied the existence of a circuit split, stating "[i]n actuality, no court of appeals has explicitly foreclosed plaintiffs from establishing standing based on a risk of future identity theft – even those courts that have declined to find standing on the facts of a particular case."

In deciding the present case, as a case of first impression, the Second Circuit unequivocally held that an increased risk of identity theft *could* be enough to establish standing, but only under the right circumstances. The Second Circuit set forth a non-exhaustive list of factors to consider:

1. Whether the plaintiff's data has been exposed as the result of a targeted attempt to obtain that data (which would make future harm more likely);

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 of such a sensitive nature that the risk of identity theft or fraud is heightened.

Despite the foregoing encouragement to would-be plaintiffs, the Second Circuit then struck a blow, holding that self-created damages, in the form of proactive steps to acquire protection from future harm post-data breach, such as purchasing credit monitoring, does *not* establish an injury in fact. Because there was no evidence of further dissemination of the PII and McMorris' data was not exposed as a result of a targeted hacking attempt, thereby making future harm hypothetical, McMorris lacked Article III standing. Although the data was sensitive, the court stated "[t]he sensitive nature of McMorris's internally disclosed PII, by itself, does not demonstrate that she is at substantial risk of future identity theft or fraud."

McMorris has large implications for both companies and victims of data breaches because the Second Circuit made sweeping proclamations about the national state of the law of standing for data breach victims. Although the refusal to recognize credit monitoring as indicia of future harm may make it difficult for would-be plaintiffs to prove heightened risk and establish standing, the Second Circuit has nonetheless created a hypothetical roadmap for doing so in an area of the law that has been analogized to the Wild West. Notably, the roadmap enumerated by the court seems to encompass the "risk of harm" analysis used by several states, namely, that if data is accessed or acquired by an unauthorized party, it is still not a data breach if there is no risk of harm to the data subject. With this in mind, companies should review their policies and procedures regarding the prevention of and reaction to data breaches. With appropriate prevention and monitoring tools, the chance of a successful "targeted attempt to obtain data," which could result in lawsuits, is decreased. Moreover, procedures, such as encryption of sensitive data, lower the likelihood that stolen data has "a high risk for identity theft or fraud."

National Law Review, Volume XI, Number 124