THOMPSON COBURN LLP

insights

TYPES NOT MAPPED YET November 15, 2021 | TTR not mapped yet | Elizabeth (Libby) A. Casale, Layla F. Husen, Luke Sosnicki

Second Circuit rules that risk of future identity theft not enough to support standing in data breach class action

The Second Circuit recently joined a growing number of federal courts to decide when a data breach of personally identifiable information ("PII") is actionable. According to the Second Circuit, plaintiffs do not have standing to bring a lawsuit when there is no allegation their PII was targeted or misused.

The Second Circuit's decision

To bring a lawsuit in federal court, a plaintiff must have standing. To have standing, the plaintiff must establish, among other things, an "injury in fact." This means an injury that is "concrete and particularized" as well as "actual or imminent." A "conjectural" or "hypothetical" injury is not enough. This distinction is important in data breach cases, where courts are increasingly asked to decide whether a future risk of identity theft is sufficient to maintain claims in federal court.

In *McMorris v. Carlos Lopez & Associates*, former employees brought a class action after an employer accidentally emailed 65 employees a spreadsheet containing social security numbers, home addresses, dates of birth, telephone numbers, educational degrees, and dates of hire for approximately 130 current and former employees.[1] The plaintiffs alleged they were "at imminent risk of suffering identity theft" and becoming victims of "unknown but certainly impending future crimes." However, the plaintiffs did not allege that the spreadsheet was shared with anyone outside the employer or otherwise taken or misused by third parties.

The parties settled the case after the employer filed a motion to dismiss. However, the district judge declined to approve the settlement agreement and dismissed the case for lack of standing. According to the judge, the plaintiffs failed to allege "a substantial risk of identity theft" or that such harm "was certainly impending."

On appeal, the Second Circuit recognized that a plaintiff could, theoretically, establish standing based on an "increased risk" of identity theft. But the plaintiffs in *McMorris* failed to do so. The court identified three factors courts should consider:

- Whether the data had been exposed as the result of a targeted attempt to obtain that data;
- Whether any portion of the dataset had already been misused; and
- Whether the type of data that had been exposed is sensitive such that there is a high risk of identity theft or fraud.

Because the PII in the spreadsheet was highly sensitive, the plaintiffs met the third factor. However, they didn't meet the other factors, because there were no facts suggesting an unauthorized third party took the PII or that the PII was otherwise misused. Unlike in a case involving a malicious cyberattack "carried out to obtain sensitive information for improper use," the court reasoned, the plaintiffs didn't allege that their data was "intentionally targeted or obtained." As such, any actions they took to purchase credit monitoring or identity theft protection services were not enough to establish injury.

The *McMorris* decision underscores a distinction between targeted data attacks by a threat actor and inadvertent data disclosures. In this particular case, the latter was not enough to establish a substantial risk of future harm.

THOMPSON COBURN LLP

The view from other courts

Prior to *McMorris*, other courts reached similar decisions. For example, the Third Circuit did not find standing even when an unknown hacker penetrated a firewall of a payroll processing firm–potentially gaining access to the PII of approximately 27,000 employees at approximately 1,900 companies–because there was no evidence of maliciousness or that the hacker read, copied, or understood the data.[2] On the other hand, other courts have refused to require allegations of malicious targeting or misuse.[3]

In the wake of the Supreme Court's Ramirez decision, it is unclear how courts will view "risk of future harm" allegations in data breach cases. In *Ramirez*, the Court rejected a "risk of future harm" argument made by plaintiffs whose credit reports were never provided to third parties. But the facts of that case involved the Fair Credit Reporting Act, which courts may distinguish in other cases.

Takeaway

Despite these evolving legal nuances, one takeaway seems clear: securing PII and mitigating the risk of threats posed by disclosure is increasingly important. The various cases suggest that it matters whether a third party targeted or misused the data. This underscores the need for robust implementation of cybersecurity best practices and cross-functional team involvement in navigating incident responses.

Thompson Coburn's Cybersecurity, Data Governance and Privacy team monitors developments like these as it counsels clients in the evolving landscape of cybersecurity and data privacy. Our cybersecurity attorneys have the experience needed to rapidly respond to threatened litigation, investigations, and class actions related to data security breaches.

Luke Sosnicki is a Los Angeles partner in Thompson Coburn's Business Litigation group who has written and spoken extensively about data privacy litigation and regulatory risks. Layla Husen and Libby Casale are associates in Thompson Coburn's Business Litigation group.

[1] *McMorris v. Carlos Lopez & Assoc.*, LLC, 995 F.3d 295, 298 (2d. Cir. 2021).

[2] *Reilly v. Ceridian Corp.*, 664 F.3d 38, 40, 42 (3d. Cir. 2011).

[3] *See e.g., Krottner v. Starbucks Corp.*, 628 F.3d 1139, 1143 (9th Cir. 2010) (the theft of a laptop containing unencrypted personal data was, alone, sufficient injury to confer standing).

authorsTest

elizabeth
Elizabeth (Libby) A. Casale

layla
Layla F. Husen

luke
Luke Sosnicki