Insights, News & Events

ONE EMPLOYEE'S ACCIDENTAL EMAIL LEADS TO A SIGNIFICANT DATA BREACH RULING IN FEDERAL APPEALS COURT

Insights
May 25, 2021

A federal appeals court recently addressed whether employees had standing to bring a lawsuit when their personally identifiable information (PII) was inadvertently circulated to other employees at the company, with no indication of misuse or external disclosure. In *McMorris v. Carlos Lopez & Associates, LLC*, the 2nd Circuit Court of Appeals (hearing cases from New York, Connecticut, and Vermont) determined that the particular plaintiffs at issue did not have standing and that their mere fear of identity theft was insufficient for them to sustain a claim for relief. Importantly, however, the court set forth a three-part framework for how standing could be established in a similar situation. While the ruling and its framework provide guidance on how standing could hypothetically be established, the ultimate takeaway is that standing in these types of situations will be determined based on an analysis of the particular circumstances in each case, with consideration given to issues such as the nature of the exposure, whether the exposed data was misused, and the nature of the data itself.

Case Background

This case stems from simple human error. Carlos Lopez & Associates, LLC (CLA) provides mental and behavioral health services to veterans, service members, and their families. In June 2018, a CLA employee accidentally emailed a spreadsheet to 65 CLA employees that included PII – including Social Security numbers, dates of birth, home

Related People

Jeffrey M. Csercsevits
Partner
610.230.2159

Service Focus

Litigation and Trials

Privacy and Cyber

Related Offices

New York

addresses, and telephone numbers – for 130 current and former CLA employees.

Three of the individuals whose information had been disclosed filed a class-action complaint in the Southern District of New York, alleging negligence and consumer protection violations. The plaintiffs did not allege that they had been victims of fraud or identity theft, but that they were at imminent risk of identity theft and at risk of becoming victims to future crimes. The plaintiffs did not allege that the PII in the spreadsheet was ever shared outside of CLA or taken or misused by any third parties. Nevertheless, they cancelled their credit cards and invested in credit monitoring and identity theft protection services.

In order to establish standing under Article III of the Constitution, plaintiffs must show, among other things, that they suffered an injury in fact that is concrete, particularized, and actual or imminent. The lower court found that the *McMorris* plaintiffs failed to satisfy this requisite and dismissed the case for lack of subject matter jurisdiction. On appeal, the 2nd Circuit Court of Appeals recently affirmed this decision.

The 2nd Circuit's Decision

As a case of first impression, the Second Circuit held on April 26 that it is possible for a plaintiff to establish standing based on an increased risk of identity theft or fraud following an unauthorized disclosure. In taking this position, the 2nd Circuit joined the other circuit courts who have addressed the issue and denied the suggested existence of a split among the circuit courts on the issue.

After confirming that it was possible to establish standing, the 2nd Circuit held that courts should consider the following non-exhaustive factors to determine whether a plaintiff has sufficiently alleged an Article III injury in fact when confronted with an allegation that a plaintiff is at an increased risk of identity theft or fraud based on an unauthorized data disclosure:

1. Whether the plaintiff's data was exposed due to a targeted attempt to obtain that data;

2. Whether any portion of the data had been misused, even if the plaintiff had not specifically experienced identity theft or fraud; and

3. Whether the data that had been exposed is sensitive such that there is a heightened risk of identity theft or fraud.

In sum, these factors are designed to assess the likelihood of future harm that may occur as a result of the disclosure.

Applying these factors in *McMorris*, the 2nd Circuit found that the first two factors supported dismissal because (1) the case involved an inadvertent disclosure of PII and there was no indication that the data was intentionally targeted and (2) the plaintiffs never alleged that the data was misused. On the final factor, the court noted that the data at issue included the type of PII that could have placed the plaintiffs at a substantial risk of identity theft or fraud. However, the court concluded that this alone could not establish standing because there was no indication that the PII was intentionally taken by an unauthorized party or misused.

In addition to the "increased risk" analysis, the 2nd Circuit also considered whether the costs associated with the plaintiffs' proactive steps to protect themselves through credit monitoring and identity theft protection could alone constitute an injury in fact. The court determined that these expenses were based on a speculative threat and could not create an injury because the plaintiffs failed to show that they were at a substantial risk of future identity theft or fraud. Essentially, the plaintiffs could not manufacture standing by inflicting harm upon themselves based on hypothetical concerns.

Key Takeaways for Employers

The case provides employees, and other individuals whose data has been disclosed, with specific guidance on how to tailor their arguments to increase their likelihood of establishing standing based on a fear of identity theft. Through its "increased risk" analysis, the court enables a potential plaintiff to assess the *McMorris* plaintiffs' shortcomings and create arguments to circumvent those shortcomings.

However, the case can also be used by employers defending against similar claims as it (1) provides guidance on challenging standing and specific considerations to target; (2) confirms that individuals cannot manufacture standing simply by taking proactive measures; and (3) seems to indicate that inadvertent disclosures may be less likely to justify standing.

Practical Guidance: What Should You Do?

This case was the result of simple employee error that has resulted in CLA fighting a protracted litigation and likely incurring significant associated costs. Moreover, given the publicity of this lawsuit, CLA may suffer reputational harm and lost business as patients may learn of the incident and question whether their confidential information is being properly safeguarded at CLA.

In sum, a simple mistake like this can have significant consequences on a business – yet these types of mistakes occur with alarming frequency. In a September 2020 report on data breaches caused by outbound emails over the preceding 12 months, Arlington Research found that 80% of the studied organizations experienced a data breach due to an employee attaching the wrong file to an email and 80% had experienced a breach due to the wrong recipient being included on an email.

Moreover, given the current remote work environment, employee email usage has increased, which only increases the likelihood of an inadvertent disclosure occurring. Therefore, employers should be mindful of the frequency and significance of these errors, and take necessary steps to properly train their employees on safeguarding confidential data, especially that which is being exchanged electronically.

This case also serves as a general reminder for employers to take proactive steps to minimize the likelihood of other types of data incidents occurring. This includes inadvertent disclosures of a different nature (*e.g.*, employees falling victim to malicious phishing emails) and criminal actors' "targeted attempts to obtain" an employers' confidential data. You should establish an incident response plan so that your company will be prepared if an incident occurs.

If you have any questions regarding data breach litigation, implementing policies to minimize the likelihood and impact of a data breach, developing incident response plans, or navigating the developing state privacy laws, please consult with the author of this Insight or a member of Fisher Phillips' Privacy and Cyber Practice Group.