ARCHER
ATTORNEYS AT LAW

January 2023 ***Client Advisory***

A Different Sort of Cyber Monday Deal: A Federal Appellate Court Clarifies the Standard for Liability to Businesses Flowing from a Data Breach

In its recent decision in Clemens v. ExecuPharm, the United States Court of Appeals for the Third Circuit clarified, and arguably expanded, the standards that determine when and if employees can file suit in federal court against employers that experience a data breach. In so ruling, the Court held that employees have "standing" to pursue claims for damages against their employer based on the risk of identity theft or fraud arising from a data breach. The decision thus presents important guidance for employees and employers alike, and further reinforces the need for employers to consider appropriate measures to protect personal and financial information which they choose to collect.

The facts in Clemens depict a very common scenario in today's business world. Jennifer Clemens, the plaintiff in the case, provided sensitive information to her employer, ExecuPharm (the defendant), as a condition of her employment. The information included her social security, banking, and financial account numbers, insurance and tax information, passport information, and certain information relating to her family.

After Clemens's employment ended, ExecuPharm was the victim of a ransomware attack by the hacking group CLOP. As is common, CLOP demanded a ransom (e.g. a payment) in exchange for the hacked data. When ExecuPharm declined to pay, CLOP posted Clemens's and other employees' information on the Dark Web -- a hidden part of the internet where such stolen information is regularly bought and sold. ExecuPharm notified its current and former employees of the breach and advised them to take precautionary measures. Clemens did so by, among other things, purchasing a credit monitoring service and transferring her accounts to a new bank.

Clemens then sued ExecuPharm for damages in the United States District Court for the Eastern District of Pennsylvania. She alleged that she sustained injuries, including the risk of identity theft and fraud, as well as emotional distress.

The trial court dismissed Clemens's complaint, reasoning that the Third Circuit's prior decision in Reilly v. Ceridian Corp., 664 F.3d 38 (3d Cir. 2011), mandated a finding that allegations of a mere increased risk of identity theft due to a data breach are insufficient to establish "standing" to sue. Therefore, because Clemens did not allege that her information had been used to complete fraudulent transactions in her name, her allegations were only "speculative" and her mitigation expenses alone were not enough to proceed with the claim.

However, on appeal, the Third Circuit reversed. In so ruling, the Court stated that its decision in Reilly was not intended to establish a bright line rule precluding a finding of standing based on the risk of future harm in all data breach cases. Instead, it reasoned that, to determine whether allegations of such a risk present sufficient injury to permit a plaintiff to proceed with a suit, courts should consider factors that include: whether the data breach was intentional; whether the data was misused; and whether the nature of the information accessed—such as sensitive personal and financial information—could subject the plaintiff to a risk of identity theft. Moreover, the Court held that a substantial risk of identity theft or fraud resulting from a data breach could be considered a sufficient injury for standing purposes so long as the plaintiff alleges that such a risk caused additional, currently felt harm.

Having thus clarified its standard, the Third Circuit found that Clemens's suit could continue because she claimed that her information was intentionally taken by a notorious hacking group (CLOP) in a ransomware attack; it was "misused" in that it was posted for sale on the Dark Web; and that the information was sensitive, such that it could easily be used for identity theft.

Although the tests for standing that the Court discussed in Clemens are somewhat indefinite, the decision would appear to further open the door to damages claims by federal plaintiffs who have not yet suffered any actual fraud or theft as a result of a data breach. And, while Clemens addressed employers that handle sensitive employee information, the Court's reasoning could potentially be applied more generally to data breaches in other contexts where sensitive personal or financial information is exposed.

Establishing "standing" is but the first step in a lawsuit, however, and it does not necessarily mean a plaintiff will ultimately be successful on the merits. Nevertheless, Clemens makes it clear that businesses are exposed to the sorts of damages claims that Clemens presented. Thus, Clemens stands as an important reminder that businesses must take appropriate measures to protect personal information and other sensitive data against unauthorized access and theft, and partner with experienced counsel, technical advisors, and insurance brokers to address these issues before they occur.

If you have questions about the measures that businesses should take to protect against the risks of d ata breaches or about
data breach and data privacy litigation, please contact:

Authors
Daniel DeFiglio: 856-616-2611 or ddefiglio@archerlaw.com
Christopher Terlingo: 856-673-7150 or cterlingo@archerlaw.com