WINSTON & STRAWN LLP

BLOG

Tennessee Law Restricts Data Breach Class Action Suits; Will Other States Follow?

JUNE 6, 2024

KEY TAKEAWAY

A law was recently passed in Tennessee that will shield private entities from class action lawsuits stemming from a cybersecurity event unless the event was caused by willful, wanton, or gross negligence. Similar laws have already been passed in Florida and West Virginia, possibly signaling a growing sentiment among states to make it more difficult for plaintiffs to sue companies for data exposure.

On May 22, 2024, Tennessee joined Florida and West Virginia in enacting legislation that provides a legal safe harbor for companies that have experienced a cyberattack. The law is designed to shield private entities from class action lawsuits stemming from a cybersecurity event unless the event was caused by willful, wanton, or gross negligence.

Broadly speaking, the legislation will make it more difficult for plaintiffs to sue Tennessee companies for data exposure. This is unwelcome news for class action plaintiffs' law firms in Tennessee, as they can no longer premise a lawsuit suit against companies that were cyberattacked on mere allegations that the companies were negligent in protecting consumer data. The bar to allege an actionable claim is now considerably higher.

Proponents of the law argue that it prevents frivolous litigation. They argue further that, in many cases, these cyberattacks cannot be stopped. And in such cases, it is unfair to allow potential plaintiffs to file class action lawsuits stemming from the cyberattacks, adding insult to injury. This law purports to allow companies who have been attacked to get back on their feet without having to simultaneously deal with meritless class action litigation.

Critics of the law argue that Tennessee already has one of the most lenient policies in the country, favoring companies. They argue that Tennessee had the correct standard in place before, when plaintiffs had to prove that a company did not exercise "reasonable care" in preventing consumer data from being compromised. Now, the law forces victims to prove that a company's cybersecurity practices were insufficient to prevent the attack, which opponents decry as too difficult of a burden. They also argue that this standard is out of step with federal recommendations from the Cybersecurity and Infrastructure Security Agency to strengthen cybersecurity protections for critical infrastructure sectors, such as health care.

Both Florida and West Virginia have already passed similar laws that protect businesses which have experienced data breaches. With Tennessee joining in, it will be interesting to see whether other states follow suit in passing laws that provide a similar legal safe harbor. Additionally, companies with existing strong ties to these states—such as in-state server farms or data storage centers—might also consider whether they have a defensible basis for using forum selection and/or choice of law clauses to secure appropriate application of the legislation against claims by out-of-state complainants.

Heather Donato, Law Clerk, co-authored this blog.

2 Min Read

Author

Heather M. Donato

Related Topics

Cyber Security | Data Breach

Related Capabilities

Class Actions & Group Litigation | Privacy & Data Security

This entry has been created for information and planning purposes. It is not intended to be, nor should it be substituted for, legal advice, which turns on specific facts.