

FLORIDA'S CYBERSECURITY LIABILITY BILL FACES SURPRISE VETO

BY CHRIS BACH, LITIGATION ASSOCIATE, PHELPS DUNBAR LLP

Through this article, Chris Bach unpacks Governor DeSantis' veto of Florida's Cybersecurity Incident Liability Act, HB 473. The bill, aimed at granting immunity to companies post-data breaches, faced unexpected opposition due to concerns over broad protections and potential cybersecurity risks. Bach highlights the implications for data breach legislation in Florida, emphasizing the need for balanced measures to protect consumer interests while encouraging effective cybersecurity practices.

In a surprising turn of events, Governor DeSantis has vetoed Florida's Cybersecurity Incident Liability Act, HB 473. That bill would have provided immunity from civil liability in Florida to companies that suffered a data breach if they met certain conditions. The prevailing thought was that the Governor would sign the bill (or allow it to become law without his signature).

But in the early evening of June 26, 2024, Governor DeSantis formally vetoed the legislation. In doing so, he provided a letter that revealed his rationale. He noted that HB 473 would provide "broad liability protections for state and local governments and private companies." However, he took issue with the bill because those governments and companies only had to "substantially comply with minimum cybersecurity standards in the event of a data breach or other cybersecurity event."

“GOVERNOR DESANTIS ARGUED THAT HB 473 ‘MAY RESULT IN A CONSUMER HAVING INADEQUATE RECOURSE IF A BREACH OCCURS,’ EMPHASIZING THE NEED FOR STRONGER PROTECTIONS AMID RISING DATA BREACH LITIGATION”

Governor DeSantis explained that "the bill could result in Floridians' data being less secure as the bill provides across-the-board protections for only substantially complying with standards." He believed that this would "incentivize doing the minimum." Ultimately, Governor DeSantis argued that HB 473 "may result in a consumer having inadequate recourse if a breach occurs."

In concluding his letter, though, Governor DeSantis was willing to review "potential alternatives to the bill that provide

a level of liability protection while also ensuring critical data and operations against cyberattacks are protected as much as possible." He encouraged interested parties to coordinate with the Florida Cybersecurity Advisory Council, placing the onus on Florida legislators to rework the bill if they intend to pursue it further. With data breach litigation only continuing to increase across the country—notably, the state of Florida, which remains a hotbed for data breach litigation—most expect Florida legislators to pursue a narrower or more stringent bill that Governor DeSantis would approve.

If HB 473 had become law, it would have pushed the envelope on a growing trend among various states to enact greater protections for companies facing data breaches. Indeed, it would have provided immunity for substantially complying companies and a model for other states to follow. For now, that level of immunity appears to be out of reach within Florida. Governor DeSantis has removed that possibility with his veto. However, based on the Governor's concluding remarks in his letter, Florida companies should expect him to be receptive to a similar if less powerful, bill in the future. **CA**

