Florida Passes Cybersecurity Data Breach Immunity Law: 3 Things Businesses Need to Know – and 3 Things to Do

Insights
4.11.24

Florida lawmakers recently passed a law that provides businesses with a defense to claims arising from "cybersecurity incidents" that lead to data breaches – so long as they meet a few critical obligations. The bill is expected to be signed by Governor DeSantis in the coming weeks and take effect immediately. What are the three things Florida businesses need to know about this new law, and what are the three things you should do to gain the protection that it offers?

3 Things Businesses Need to Do To Gain Data Breach Protection

HB 473, which passed the legislature on March 5, says a company is "not liable in connection with a cybersecurity incident" if it generally meets the following three obligations:

- First, the company must "substantially comply" with the Florida Information Protection Act (FIPA). This law requires businesses to provide notice to Florida's Department of Legal Affairs whenever there is a breach of security that affects 500 or more individuals in Florida. FIPA has other technical requirements, as well, that businesses need to follow.
- Second, the company must adopt a cybersecurity program that "substantially aligns" with the current version of any standards, guidelines or regulations enumerated in the statute. These include:
    - The National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity or NIST special publications 800-171 or 800-53 and 800-53a;
    - The Federal Risk and Authorization Management Program security assessment framework;
    - The Center for Internet Security (CIS) Critical Security Controls;
    - The International Organization for Standardization/International Electrotechnical Commission 27000- series (ISO/IEC 27000) family of standards; or
    - Other similar industry frameworks or standards.

    Alternatively, a cybersecurity program can also be in compliance if it substantially aligns with applicable laws, such as the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act, or other similar federal or state laws.

- Third, a company must, within one year, update its cybersecurity program to "substantially align" with any changes to the applicable industry standard/framework or law.

3 Things You Should Know About The Law

1. Florida's New Law Expands on a Trend Established by Other States

This bill falls in line with other states that have passed similar laws to create protection from data breach lawsuits by requiring companies to increase their data security protocols and efforts. Notably, Florida's law is arguably more extensive than legislation passed in other states in that it does not condition immunity based on actual cybersecurity compliance.

2. Qualifications for Immunity are Broad

HB 473 does not establish a minimum cybersecurity standard that companies must achieve. Under the new law, a company is arguably entitled to immunity if it meets its burden to show that it adopted a cybersecurity program that "substantially complies" with consumer reporting notice requirements and updates its cybersecurity program to "substantially align" with industry standards.

Notably, the law takes a flexible approach to cybersecurity. It states that various business-specific factors should be considered, including the size, complexity, and nature of the business and its activities, and the sensitivity of the personal information to be protected.

3. The Scope of Immunity Will Need to Be Determined by Florida Courts

The law places the burden on businesses to show that they have achieved "substantial compliance" in order to receive protection under the law. But it does not specify which laws would be rendered toothless with such protection. As a result, we expect that the scope of immunity will be litigated and ultimately decided by Florida state courts.

Given the broad language of the law, we expect it can be used as an affirmative defense for claims under Florida common law and statutes. However, claims for breach of contract and those filed under federal law pursuant to industry specific federal rules and regulations would likely fall outside the scope of the bill.

3 Things Your Business Should Do

- You should take a **proactive approach** and assess what personal or sensitive data you hold to begin. You can then evaluate your cybersecurity measures to identify and address vulnerabilities.
- You should also work with your **data privacy counsel** to ensure that your organization will be able to comply with the law.
- Because the law is likely inadequate to create immunity for alleged violations of other states' laws, including data breach notification laws in other jurisdictions, you shouldn't think of the law

laws, including data breach notification laws in other jurisdictions, you shouldn't think of the law as complete magic shield. You should **review applicable contracts with vendors and other third parties** to ensure that you have adequately assessed any potential risk as it relates to cybersecurity incidents.

Conclusion

For further information, contact your Fisher Phillips attorney, the authors of this Insight, or any attorney on the firm's Consumer Privacy Team, the Privacy and Cyber Practice Group, or in one of our Florida offices. We will continue to monitor consumer privacy law developments and will provide updates as warranted, so make sure that you are subscribed to Fisher Phillips' Insight System to get the most up-to-date information directly to your inbox.

Related People

Ilanit Fischler
Partner
954.847.4723
Email

Brett P. Owens

Partner
813.769.7512
Email

Service Focus

Privacy and Cyber

Related Offices

Fort Lauderdale

Orlando

Tampa