FJRI Supports HB 635 and a Sensible Safe Harbor from Class Actions Premised on Cybersecurity Incidents

Cybersecurity is a growing concern for consumers and businesses alike. To encourage businesses to take action and secure their data, the Florida Justice Reform Institute supports HB 635 which will provide a much-needed safe harbor from class action liability for businesses that implement sensible, industry-recognized cybersecurity measures.

Every cyberattack or data breach can be devastating, to both the breached business—which has to remediate the damage done by the attack, in addition to facing steep regulatory sanctions—and the individuals whose private information is exposed by the attack. With the actual perpetrators of these attacks unlikely to be found, data breaches have spurred numerous lawsuits involving a variety of legal theories for holding the businesses that are also victims of the breach liable. Claims often include common-law claims like negligence, but plaintiffs' attorneys are increasingly resorting to statutory claims as well, including under the Florida Deceptive and Unfair Trade Practices Act ("FDUTPA"). *See, e.g.*, *Burrows v. Purchasing Power, LLC*, No. 1:12-CV-22800-UU, 2012 WL 9391827, at *6 (S.D. Fla. Oct. 18, 2012).

Hospitals and other healthcare entities are a common target for data breaches and consequently data breach litigation. In 2023, Tampa General Hospital was hit with a class action lawsuit for a data breach affecting an estimated 1.2 million patients; the purported class asserted claims for common-law negligence, breach of contract, invasion of privacy, breach of fiduciary duty, unjust enrichment, and violation of FDUTPA against the hospital, although the action was ultimately dismissed. *See, e.g.*, *Doe v. Fla. Health Scis. Ctr., Inc. d/b/a Tampa Gen. Hosp.*, No. 23-CA-014169 (Fla. 13th Cir. Ct. 2023).[1] In other instances, law firms are bringing individual lawsuits on behalf of hundreds or even thousands of clients claiming damages from a data breach, as evidenced by numerous lawsuits filed against HCA Healthcare in 2023. *See, e.g.*, David Minsky, *HCA Healthcare Sued in Fla. Over Data Breach Of 11M Patients*, Law360 (Sept. 11, 2023).[2] Often, the plaintiffs or class members have not suffered damage as a result of the data breach—their claims are premised on the ***threat*** of harm posed by the exposure of their personal information. *See, e.g.*, *Doe*, Case No. 23-CA-014169, Compl. ¶ 45 (plaintiff "will continue to be at present, imminent, and continued increased risk of identity theft and fraud for years to come"); *see also id.* ¶¶ 50-52 (describing risks associated with identity theft).

Unfortunately, the true culprits are rarely held accountable. Instead, the businesses that are also victims of the breach perceived to have deep pockets are financially punished both in litigation and in fines. While on one view, litigation attacking businesses for not doing enough in the area

[1] The Second DCA affirmed the trial court's dismissal of the action. *See Doe v. Fla. Gen. Health Scis. Ctr.*, Case No. 2D2024-1678 (Sept. 12, 2025).

[2] HCA ultimately agreed to settle the actions. *See* Steve Alder, *HCA Healthcare Multi-million Dollar Data Breach Settlement Approved*, The HIPAA Journal (July 31, 2025), https://www.hipaajournal.com/hca-healthcare-data-breach-settlement/.

of cybersecurity might highlight the importance of safety measures and spur action, they can actually have the opposite effect. Confronting this problem, many states have implemented safe harbors to incentivize businesses to guard against such breaches in the first place. These states include Connecticut,[3] Iowa,[4] Ohio,[5] Oregon,[6] and Utah.[7]

Florida should join these states in taking the proactive approach of affirmatively offering compliant businesses a safe harbor from class action liability so long as they implement and maintain industry-standard cybersecurity measures. Under HB 635, a business would not be liable in connection with a cybersecurity incident if it substantially complies with the state's data breach notification law, section 501.171, Florida Statutes (if applicable), and if it has implemented a cybersecurity program that substantially aligns with the current version of several industry standards outlined in the proposed statute, has a disaster recovery plan for cybersecurity incidents, and has multi-factor authentication. A business's compliance with the statute may be demonstrated by providing documentation or other evidence of an assessment, conducted internally or by a third party, reflecting that the business's cybersecurity program meets these requirements. Any business using the safe harbor would also be required to update their standards upon any revisions to the frameworks or standards used within one year after the revisions are published. The defendant in any action involving a cybersecurity incident would bear the burden of proving substantial compliance with the safe harbor. The bill also confirms that these provisions do not create a private cause of action, and the failure of a business to use the safe harbor is not evidence of negligence or fault under any theory of liability. This new law would apply to any putative class action filed before, on, or after the effective date of the act (which would take effect upon becoming law).

Responsible businesses should be entitled to a presumption against class action liability so long as they implement and maintain prescribed cybersecurity measures. For all these reasons, the Florida Justice Reform Institute supports HB 635.

---

[3] Conn. Gen. Stat. § 42-901 (providing safe harbor from punitive damages to businesses implementing cybersecurity measures).

[4] Iowa Code § 554G.2. (covered entity with specified cybersecurity program has an affirmative defense to any cause of action sounding in tort that alleges failure to implement reasonable protocols resulting in a data breach).

[5] Ohio Rev. Code § 1354.02 (covered entity with specified cybersecurity program has an affirmative defense to any cause of action sounding in tort that alleges failure to implement reasonable protocols resulting in a data breach).

[6] Or. Rev. Stat. § 646A.604(11)(b) (covered entity or vendor may affirmatively defend against an allegation that entity or vendor did not develop, implement, or maintain reasonable safeguards for data security by showing that entity or vendor developed, implemented, and maintained reasonable security measures).

[7] Utah Code § 78B-4-702 (providing affirmative defenses for entities and persons creating certain cybersecurity programs).