The Florida Justice Reform Institute Opposes CS/HB 969's Creation of a New Private Cause of Action for Data Breaches

2021 Committee Substitute for House Bill 969 proposes comprehensive consumer data privacy protections, including the creation of new obligations for covered businesses and the significant expansion of consumers' rights concerning their personal information, such as a right to notice about a business's data collection and selling practices. While the bill is well-intentioned, the Florida Justice Reform Institute opposes the creation of a broad private cause of action for a consumer whose information is subject to a data breach as proposed in section 501.173(12), Florida Statutes.

The Private Cause of Action Lacks a Causation Requirement. Under proposed subsection (12), a consumer impacted by a business's data breach may sue the business for up to $750 per incident or actual damages, whichever is greater. Notably, the act does not contain an express causation requirement. Until now, the biggest obstacle plaintiffs faced in data breach litigation was proving actual harm—e.g., money losses. But under the legislation as drafted, any consumer whose information "is subject to" a data breach likely has a cause of action for statutory damages. Without a causation requirement, this relatively easy-to-satisfy statutory violation will prove lucrative for class action plaintiffs' attorneys who will see every data breach as the opportunity to recover hundreds of thousands or even millions of dollars in statutory damages.

While proponents of the law might argue that a plaintiff will still be required to show that the breach is a "result of the business' violation of the duty to implement and maintain reasonable security procedures and practices," such an argument ignores the reality of litigation. The question whether a business complied with the duty to maintain and implement reasonable security procedures and practices will inevitably be a factual question that will require extensive discovery and litigating, and is unlikely to be resolved prior to a costly and lengthy trial. Thus, even if the plaintiff is ultimately unable to prove that the data breach was the result of the business's failure to implement and maintain appropriate security practices within the meaning of the law, the business will still have spent hundreds of thousands of dollars defending the lawsuit in the meantime.

Private Information Is Too Broadly Defined for the Cause of Action. The definition of personal information under CS/HB 969 also makes for an extraordinarily broad cause of action, creating liability for even relatively innocuous data breaches.

Personal information is traditionally defined to mean sensitive, personally identifying information like Social Security numbers, credit card numbers, and medical information. Under CS/HB 969, however, in addition to those more traditional categories of personal information, the term "personal information" is defined to mean, just as examples:

- "information that identifies, relates to, or describes a particular consumer or household, or is reasonably capable of being directly or indirectly associated or linked with, a particular consumer or household" (*see* proposed § 501.173(1)(m), Fla. Stat.);

- "professional or employment-related information" (*see* proposed § 501.173(1)(m)1.j., Fla. Stat.); and

- "inferences drawn from any of the information identified in this paragraph to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes" (*see* proposed § 501.173(1)(m)1.j., Fla. Stat.).

Based on that broad "personal information" definition, a business's inadvertent disclosure that an individual is employed as an assistant or likes the color blue, or that an individual's household prefers watching true crime television shows, would allow that individual to sue the business that suffered the data breach. Such relatively harmless disclosures should not be the basis for expansive business liability.

The Proposed Cause of Action Is Inconsistent with Florida's Data Breach Notification Law. The definition of what constitutes a data breach, triggering the private cause of action proposed in CS/HB 969, is also broad and inconsistent with the definition of a data breach under Florida's data breach notification law.

Florida's data breach notification law requires businesses to implement reasonable data security measures and requires covered businesses experiencing a data breach within the meaning of the law to notify consumers and the Department of Legal Affairs. *See* § 501.171, Florida Statutes. Under CS/HB 969's private cause of action, "any unauthorized access and exfiltration, theft, or disclosure" of personal information is a data breach authorizing a consumer to bring suit. In contrast, Florida's breach notification law limits the definition of a breach to "unauthorized access of data in electronic form containing personal information." § 501.171(1)(a), Fla. Stat. The definition of "personal information" for purposes of the data breach notification law is also much narrower than the definition set forth in CS/HB 969. *See* § 501.171(1)(g), Fla. Stat.

The differences in these definitions mean this: it is possible that under CS/HB 969, a business might be sued based on a data breach for which it would not have been required to give notice under the data breach notification law. This may create a disincentive for businesses to notify the Department of Legal Affairs and consumers that a breach has occurred because bringing attention to the issue means the business would be risking significant statutory liability under CS/HB 969's private cause of action. Such a disincentive would in turn only make it more difficult for consumers to learn about and resolve data breaches involving their personal information.

Remove the Private Cause of Action from CS/HB 969. In short, there is little need to create a private cause of action to ensure businesses follow reasonable and secure consumer data privacy practices, and the cause of action proposed will benefit plaintiffs' lawyers more than it will benefit consumers. CS/HB 969 already creates an appropriate enforcement mechanism by which the Legislature can ensure businesses comply. Under subsection (13) of the proposed law,

210 S. MONROE ST. ● TALLAHASSEE, FL 32301-1824 ● 850.222.0170 ● FAX: 850.222.1098

the Department of Legal Affairs will be given broad authority to enforce the new protections, including through the imposition of civil penalties of $2,500 per unintentional violation and $7,500 per intentional violation, with penalties tripling if the consumer victim is 16 or younger. This is in addition to the authorization given to the Attorney General to seek up to $500,000 in civil penalties against businesses violating the data breach notification law. *See* § 501.171(9), Fla. Stat. The Florida Justice Reform Institute urges that subsection (12) of CS/HB 969 be removed from the bill.

210 S. Monroe St. ● Tallahassee, FL 32301-1824 ● 850.222.0170 ● FAX: 850.222.1098