Senate Bill 493

By: Senators Thompson of the 14th, Beach of the 21st, Harbison of the 15th, Cowsert of the 46th and Harbin of the 16th

AS PASSED SENATE

A BILL TO BE ENTITLED

AN ACT

To amend Chapter 1 of Title 10 of the Official Code of Georgia Annotated, relating to selling and other trade practices, so as to provide for legislative findings; to provide standards for cybersecurity programs to protect businesses from liability; to provide for affirmative defenses for data breaches of private information; to provide for related matters; to provide for an effective date; to repeal conflicting laws; and for other purposes.

BE IT ENACTED BY THE GENERAL ASSEMBLY OF GEORGIA:

SECTION 1.

Chapter 1 of Title 10 of the Official Code of Georgia Annotated, relating to selling and other trade practices, is amended by adding a new article to read as follows:

"ARTICLE 35

10-1-920.

The General Assembly finds that:

(1) The purpose of this article is to establish a legal safe harbor which may be pled as an affirmative defense to a cause of action sounding in tort that alleges or relates to the failure to implement reasonable cybersecurity controls, resulting in a data breach of private information. This article shall apply to all covered entities that implement a cybersecurity program that substantially complies with the requirements of this article or that implement a cybersecurity program through the use of an appropriately credentialed independent security professional; and

(2) This article is intended to incentivize and encourage businesses to achieve a higher level of cybersecurity through voluntary action. This article does not, and is not intended to, create a minimum cybersecurity standard that must be achieved, nor shall it be read to impose liability upon businesses that do not obtain or maintain practices in compliance with this article.

10-1-921.

As used in this article, the term:

(1) 'Covered entity' means a business that accesses, maintains, communicates, or processes personal information in or through one or more systems, networks, or services located in or outside of this state.

(2) 'Data breach' means unauthorized access to and acquisition of computerized data that compromises the security or confidentiality of personal information owned by or licensed to a covered entity and that causes, is reasonably believed to have caused, or is reasonably believed to have the potential to cause a material risk of identity theft or other fraud to person or property. Such term shall not include either of the following:

(A) Good faith acquisition of personal information by the covered entity's employee or agent for the purposes of the covered entity, provided that the personal information is not used for an unlawful purpose or subject to further unauthorized disclosure; or

(B) Acquisition of personal information pursuant to a search warrant, subpoena, or other court order, or pursuant to a subpoena, order, or duty of a regulatory state agency.

(3) 'Personal information' means an individual's first name or first initial and last name in combination with any one or more of the following data elements when either the name or the data elements are not encrypted or redacted:

(A) Social security number;

(B) Driver's license number or state identification card number;

(C) Account number, credit card number, or debit card number, if circumstances exist wherein such a number could be used without additional identifying information, access codes, or passwords;

(D) Account passwords or personal identification numbers or other access codes;

(E) Student information including grades, disciplinary history, and standardized test scores;

(F) Information related to medical treatment, diagnosis, or history; or

(G) Any of the items contained in subparagraphs (A) through (F) of this paragraph when not in connection with the individual's first name or first initial and last name, if the information compromised would be sufficient to perform or attempt to perform identity theft or other fraud against the individual whose information was compromised.

Such term shall not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

10-1-922.

(a) A covered entity intending to assert an affirmative defense to a data breach of personal information under this article shall create, maintain, and comply with a written

cybersecurity program that contains administrative, technical, and physical safeguards for the protection of personal information and that reasonably conforms to an industry recognized cybersecurity framework as described in Code Section 10-1-923.

(b) A covered entity's cybersecurity program shall be designed to do all of the following:

(1) Protect the security and confidentiality of personal information;

(2) Protect against any anticipated threats or hazards to the security or integrity of personal information; and

(3) Protect against unauthorized access to and acquisition of personal information that is likely to result in a material risk of identity theft or other fraud to the individual to whom the information relates.

(c) The scale and scope of a covered entity's cybersecurity program is reasonable if it takes into consideration all of the following factors:

(1) The size and complexity of the covered entity;

(2) The nature and scope of the activities of the covered entity;

(3) The sensitivity of the information to be protected;

(4) The cost and availability of tools to improve cybersecurity and reduce vulnerabilities; and

(5) The resources available to the covered entity.

10-1-923.

(a) A covered entity shall be deemed to be in compliance with this article if it implements a cybersecurity program that includes:

(1) Reasonable administrative safeguards in which the covered entity:

(A) Designates one or more employees to coordinate the cybersecurity program;

(B) Identifies reasonably foreseeable internal and external risks;

(C) Assesses the sufficiency of safeguards in place to control the identified risks;

(D) Trains and manages employees in the cybersecurity program practices and procedures;

(E) Selects service providers capable of maintaining appropriate safeguards and requires those safeguards by contract; and

(F) Adjusts the cybersecurity program in light of business changes or new circumstances;

(2) Reasonable technical safeguards in which the covered entity:

(A) Assesses risks in network and software design;

(B) Assesses risks in information processing, transmission, and storage;

(C) Detects, prevents, and responds to attacks or system failures; and

(D) Regularly tests and monitors the effectiveness of key controls, systems, and procedures; and

(3) Reasonable physical safeguards in which the covered entity:

(A) Assesses risks of information storage and disposal;

(B) Detects, prevents, and responds to intrusions;

(C) Protects against unauthorized access to or use of private information during or after the collection, transportation, and destruction or disposal of the information; and

(D) Disposes of private information within a reasonable amount of time after it is no longer needed for business purposes by erasing electronic media so that the information cannot be read or reconstructed.

(e) It shall be an affirmative defense to liability for a data breach of personal information if the covered entity can establish:

(1) Substantial compliance with the provisions of this article; or

(2) That it has, within 12 months prior to the data breach, undergone a data security assessment by an independent security assessment firm using appropriately credentialed security professionals and received a certification of adherence to a widely recognized information security standard issued by an authoritative cybersecurity standards body."

SECTION 2.

This Act shall become effective on July 1, 2020.

SECTION 3.

All laws and parts of laws in conflict with this Act are repealed.