

Senate Bill 493

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

A BILL TO BE ENTITLED
AN ACT

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

6 BE IT ENACTED BY THE GENERAL ASSEMBLY OF GEORGIA:

7 **SECTION 1.**

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

10 "ARTICLE 35

11 10-1-920.

12 The General Assembly finds that:

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

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

25 10-1-921.

26 As used in this article, the term:

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

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

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

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

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

43 (A) Social security number;

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

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

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

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

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

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

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

58 10-1-922.

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

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

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

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

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

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

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

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

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

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

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

78 (5) The resources available to the covered entity.

79 10-1-923.

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

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

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

84 (B) Identifies reasonably foreseeable internal and external risks;

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

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

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

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

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

93 (A) Assesses risks in network and software design;

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

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

- 96 (D) Regularly tests and monitors the effectiveness of key controls, systems, and
97 procedures; and
- 98 (3) Reasonable physical safeguards in which the covered entity:
- 99 (A) Assesses risks of information storage and disposal;
100 (B) Detects, prevents, and responds to intrusions;
101 (C) Protects against unauthorized access to or use of private information during or after
102 the collection, transportation, and destruction or disposal of the information; and
103 (D) Disposes of private information within a reasonable amount of time after it is no
104 longer needed for business purposes by erasing electronic media so that the information
105 cannot be read or reconstructed.
- 106 (e) It shall be an affirmative defense to liability for a data breach of personal information
107 if the covered entity can establish:
- 108 (1) Substantial compliance with the provisions of this article; or
109 (2) That it has, within 12 months prior to the data breach, undergone a data security
110 assessment by an independent security assessment firm using appropriately credentialed
111 security professionals and received a certification of adherence to a widely recognized
112 information security standard issued by an authoritative cybersecurity standards body."

113 **SECTION 2.**

114 This Act shall become effective on July 1, 2020.

115 **SECTION 3.**

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