

HB5243



102ND GENERAL ASSEMBLY

State of Illinois

2021 and 2022

HB5243

Introduced 1/31/2022, by Rep. Keith R. Wheeler

SYNOPSIS AS INTRODUCED:

New Act

Creates the Cybersecurity Compliance Act. Creates an affirmative defense for every covered entity that creates, maintains, and complies with a written cybersecurity program that contains administrative, technical, and physical safeguards for the protection of either personal information or both personal information and restricted information and that reasonably conforms to an industry-recognized cybersecurity framework. Prescribes requirements for the cybersecurity program.

LRB102 22790 SPS 31939 b

A BILL FOR

1 AN ACT concerning business.

2 **Be it enacted by the People of the State of Illinois,**
3 **represented in the General Assembly:**

4 Section 1. Short title. This Act may be cited as the
5 Cybersecurity Compliance Act.

6 Section 5. Definitions. As used in this Act:

7 "Business" means any limited liability company, limited
8 liability partnership, corporation, sole proprietorship,
9 association, State institution of higher education, private
10 college, or other group, however organized and whether
11 operating for profit or not-for-profit, or the parent or
12 subsidiary of any of the foregoing. "Business" includes a
13 financial institution organized, chartered, or holding a
14 license authorizing operation under the laws of this State,
15 any other state, the United States, or any other country.

16 "Covered entity" means a business that accesses,
17 maintains, communicates, or processes personal information or
18 restricted information in or through one or more systems,
19 networks, or services located in or outside of this State.

20 "Data breach" means unauthorized access to and acquisition
21 of computerized data that compromises the security or
22 confidentiality of personal information or restricted
23 information owned by or licensed to a covered entity and that

1 causes, reasonably is believed to have caused, or reasonably
2 is believed will cause a material risk of identity theft or
3 other fraud to person or property. "Data breach" does not
4 include:

5 (1) the good faith acquisition of personal information
6 or restricted information by the covered entity's employee
7 or agent for the purposes of the covered entity so long as
8 the personal information or restricted information is not
9 used for an unlawful purpose or subject to further
10 unauthorized disclosure; or

11 (2) the acquisition of personal information or
12 restricted information pursuant to a search warrant,
13 subpoena, or other court order, or pursuant to a subpoena,
14 order, or duty of a regulatory State agency.

15 "Personal information" has the same meaning as provided in
16 the Personal Information Protection Act.

17 "Restricted information" means any information about an
18 individual, other than personal information, that, alone or in
19 combination with other information, including personal
20 information, can be used to distinguish or trace the
21 individual's identity or that is linked or linkable to an
22 individual, if the information is not encrypted, redacted, or
23 altered by any method or technology in such a manner that the
24 information is unreadable, and the breach of which is likely
25 to result in a material risk of identity theft or other fraud
26 to a person or property.

1 Section 10. Safe harbor requirements.

2 (a) A covered entity seeking an affirmative defense under
3 this Act shall:

4 (1) create, maintain, and comply with a written
5 cybersecurity program that contains administrative,
6 technical, and physical safeguards for the protection of
7 personal information and that reasonably conforms to an
8 industry-recognized cybersecurity framework, as described
9 in Section 15; or

10 (2) create, maintain, and comply with a written
11 cybersecurity program that contains administrative,
12 technical, and physical safeguards for the protection of
13 both personal information and restricted information and
14 that reasonably conforms to an industry-recognized
15 cybersecurity framework, as described in Section 15.

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

18 (1) protect the security and confidentiality of
19 information;

20 (2) protect against any anticipated threats or hazards
21 to the security or integrity of information; and

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

1 (c) The scale and scope of a covered entity's
2 cybersecurity program under subsection (a), as applicable, is
3 appropriate if it is based on all of the following factors:

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

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

7 (3) the sensitivity of the information to be
8 protected;

9 (4) the cost and availability of tools to improve
10 information security and reduce vulnerabilities; and

11 (5) the resources available to the covered entity.

12 (d) A covered entity under this Section is entitled to an
13 affirmative defense as follows:

14 (1) A covered entity that satisfies paragraph (1) of
15 subsection (a) and subsections (b) and (c) is entitled to
16 an affirmative defense to any cause of action sounding in
17 tort that is brought under the laws of this State or in the
18 courts of this State and that alleges that the failure to
19 implement reasonable information security controls
20 resulted in a data breach concerning personal information.

21 (2) A covered entity that satisfies paragraph (2) of
22 subsection (a) and subsections (b) and (c) is entitled to
23 an affirmative defense to any cause of action sounding in
24 tort that is brought under the laws of this State or in the
25 courts of this State and that alleges that the failure to
26 implement reasonable information security controls

1 resulted in a data breach concerning personal information
2 or restricted information.

3 Section 15. Reasonable conformance.

4 (a) A covered entity's cybersecurity program reasonably
5 conforms to an industry-recognized cybersecurity framework for
6 purposes of this Act if the requirements of subsection (b),
7 (c), or (d) are satisfied.

8 (b) (1) The cybersecurity program reasonably conforms to an
9 industry-recognized cybersecurity framework for purposes of
10 this Act if the cybersecurity program reasonably conforms to
11 the current version of any of the following or any combination
12 of the following, subject to paragraph (2) and subsection (e):

13 (A) The "framework for improving critical
14 infrastructure cyber security" developed by the National
15 Institute of Standards and Technology (NIST);

16 (B) NIST special publication 800-171;

17 (C) NIST special publications 800-53 and 800-53a;

18 (D) The Federal Risk And Authorization Management
19 Program (FedRAMP) Security Assessment Framework;

20 (E) The Center for Internet Security Critical Security
21 Controls for Effective Cyber Defense; or

22 (F) The International Organization for
23 Standardization/International Electrotechnical Commission
24 27000 Family - Information Security Management Systems.

25 (2) When a final revision to a framework listed in

1 paragraph (1) is published, a covered entity whose
2 cybersecurity program reasonably conforms to that framework
3 shall reasonably conform to the revised framework not later
4 than one year after the publication date stated in the
5 revision.

6 (c)(1) The covered entity's cybersecurity program
7 reasonably conforms to an industry-recognized cybersecurity
8 framework for purposes of this Act if the covered entity is
9 regulated by the State, by the federal government, or both, or
10 is otherwise subject to the requirements of any of the laws or
11 regulations listed below, and the cybersecurity program
12 reasonably conforms to the entirety of the current version of
13 any of the following, subject to paragraph (2):

14 (A) The security requirements of the Health Insurance
15 Portability and Accountability Act of 1996, as set forth
16 in 45 CFR Part 164, Subpart C;

17 (B) Title V of the Gramm-Leach-Bliley Act of 1999,
18 Public Law 106-102, as amended;

19 (C) The Federal Information Security Modernization Act
20 of 2014, Public Law 113-283;

21 (D) The Health Information Technology for Economic and
22 Clinical Health Act, as set forth in 45 CFR Part 162.

23 (2) When a framework listed in paragraph (1) is amended, a
24 covered entity whose cybersecurity program reasonably conforms
25 to that framework shall reasonably conform to the amended
26 framework not later than one year after the effective date of

1 the amended framework.

2 (d) (1) The cybersecurity program reasonably conforms to an
3 industry-recognized cybersecurity framework for purposes of
4 this Act if the cybersecurity program reasonably complies with
5 both the current version of the payment card industry (PCI)
6 data security standard and conforms to the current version of
7 another applicable industry-recognized cybersecurity
8 framework listed in subsection (b), subject to paragraph (2)
9 of subsection (b) and subsection (e).

10 (2) When a final revision to the PCI data security
11 standard is published, a covered entity whose cybersecurity
12 program reasonably complies with that standard shall
13 reasonably comply with the revised standard not later than one
14 year after the publication date stated in the revision.

15 (e) If a covered entity's cybersecurity program reasonably
16 conforms to a combination of industry-recognized cybersecurity
17 frameworks, or complies with a standard, as in the case of the
18 PCI data security standard, as described in subsection (b) or
19 (d), and 2 or more of those frameworks are revised, the covered
20 entity whose cybersecurity program reasonably conforms to or
21 complies with, as applicable, those frameworks shall
22 reasonably conform to or comply with, as applicable, all of
23 the revised frameworks not later than one year after the
24 latest publication date stated in the revisions.

25 Section 20. No private right of action. This Act shall not

1 be construed to provide a private right of action, including a
2 class action, with respect to any act or practice regulated
3 under it.

4 Section 97. Severability. The provisions of this Act are
5 severable under Section 1.31 of the Statute on Statutes.