

ASSEMBLY, No. 3984

STATE OF NEW JERSEY
219th LEGISLATURE

INTRODUCED MAY 4, 2020

Sponsored by:

Assemblywoman BETTYLOU DECROCE

District 26 (Essex, Morris and Passaic)

SYNOPSIS

Creates affirmative defense for certain breaches of security.

CURRENT VERSION OF TEXT

As introduced.



1 AN ACT concerning affirmative defense for certain breaches of
2 security and supplementing Title 56 of the Revised Statutes.

3

4 **BE IT ENACTED** by the Senate and General Assembly of the State
5 of New Jersey:

6

7 1. As used in P.L. , c. (C.) (pending before the
8 Legislature as this bill):

9 "Breach of security" shall have the same meaning as provided in
10 section 10 of P.L.2005, c.226 (C.56:8-161). "Breach of security"
11 shall not include:

12 the good faith acquisition of personal information or restricted
13 information by the covered entity's employee or agent for the
14 purposes of the covered entity's, provided that the personal
15 information or restricted information is not used for an unlawful
16 purpose or subject to further unauthorized disclosure; and

17 acquisition of personal information or restricted information
18 pursuant to a search warrant, subpoena, or other court order, or
19 pursuant to a subpoena, order, or duty of a regulatory State agency

20 "Business" means any limited liability company, limited liability
21 partnership, corporation, sole proprietorship, association, public or
22 private institution of higher education, as defined in section 1 of
23 P.L.2012, c.75 (C.18A:3-29), or other group, however organized
24 and whether operating for profit or not-for-profit, including a
25 financial institution organized, chartered, or holding a license
26 authorizing operation under the laws of this State, any other state,
27 the United States, or any other country, or any financial institution
28 parent or subsidiary.

29 "Covered entity" means a business, or State or local government
30 unit that accesses, maintains, communicates, or processes personal
31 information or restricted information in or through one or more
32 systems, networks, or services located within or outside this State.

33 "Director" means the Director of the Division of Consumer
34 Affairs in the Department of Law and Public Safety.

35 "Local government unit" means a county, municipality, or other
36 political subdivision of the State, or any agency, authority, or other
37 entity thereof.

38 "Personal information" shall have the same meaning as provided
39 in section 10 of P.L.2005, c.226 (C.56:8-161).

40 "Restricted information" means any information about an
41 individual, other than personal information, that, alone or in
42 combination with other information, including personal
43 information, can be used to distinguish or trace the individual's
44 identity or that is linked or linkable to an individual, if the
45 information is not encrypted, redacted, or altered by any method or
46 technology in a manner that the information is unreadable, and the

1 breach of which is likely to result in a material risk of identity theft
2 or other fraud to person or property.

3

4 2. a. A covered entity seeking an affirmative defense pursuant
5 to P.L. , c. (C.) (pending before the Legislature as this bill)
6 shall have created, maintained, and complied with a written
7 cybersecurity program that contains administrative, technical, and
8 physical safeguards for the protection of personal information or
9 restricted information, or both, and that reasonably conforms to an
10 industry recognized cybersecurity framework, as determined by a
11 court of law in this State.

12 b. A covered entity's cybersecurity program, required by
13 subsection a. of this section, shall be designed to protect against the
14 following:

15 (1) breaches of the security and confidentiality of personal
16 information, restricted information, or both;

17 (2) any anticipated threats or hazards to the security or integrity
18 of personal information, restricted information, or both; and

19 (3) unauthorized access to and acquisition personal information,
20 restricted information, or both that is likely to result in a material
21 risk of identity theft or other fraud to the individual to whom the
22 information relates.

23 c. The scale and scope of a covered entity's cybersecurity
24 program, required by subsection a. of this section, shall be based on
25 all of the following factors:

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

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

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

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

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

32 d. A covered entity that satisfies subsections a., b., and c. of
33 this section is entitled to an affirmative defense to any cause of
34 action sounding in tort that is brought under the laws of this State or
35 in the courts of this State and that alleges that the failure to
36 implement reasonable information security controls resulted in a
37 breach of security concerning personal information or restricted
38 information or both.

39

40 3. The Director of the Division of Consumer Affairs in the
41 Department of Law and Public Safety may review and deem that a
42 covered entity's cybersecurity program reasonably conforms to an
43 industry-recognized cybersecurity framework as required to be
44 entitled to an affirmative defense pursuant to section 2 of
45 P.L. , c. (C.) (pending before the Legislature as this bill) if
46 any of the following are satisfied:

1 a. (1) the cybersecurity program reasonably conforms, as
2 determined by the director, to the current version of any of the
3 following, or any combination of the following, subject to required
4 revisions, if applicable:

5 (a) the Framework for Improving Critical Infrastructure
6 Cybersecurity developed by the National Institute of Standards and
7 Technology (NIST);

8 (b) NIST special publication 800-171;

9 (c) NIST special publications 800-53 and 800-53a;

10 (d) the Federal Risk and Authorization Management Program
11 (FedRAMP) security assessment framework;

12 (e) the Center for Internet Security Critical Security Controls for
13 Effective Cyber Defense publication; or

14 (f) the International Organization for Standardization and
15 International Electrotechnical Commission 27000 family -
16 information security management systems.

17 (2) When a final revision to a framework listed in paragraph (1)
18 of this subsection is published, a covered entity whose
19 cybersecurity program reasonably conforms to that framework shall
20 reasonably conform, as determined by the director, to the revised
21 framework not later than one year after the publication date stated
22 in the revision.

23 b. (1) If the covered entity is regulated by the State, by the
24 federal government, or both, or is otherwise subject to the
25 cybersecurity requirements of any of the laws or regulations listed
26 below, and the cybersecurity program reasonably conforms, as
27 determined by the director, to the current version of any of the
28 following, subject to required revisions, if applicable:

29 (a) Part 164 Subpart C of Title 45 of the Code of Federal
30 Regulations, established pursuant to the "Health Insurance
31 Portability and Accountability Act of 1996," Pub.L.104-191;

32 (b) Title V of the "Gramm-Leach-Bliley Act of 1999,"
33 15 U.S.C. s.6801 et seq., as amended;

34 (c) the "Federal Information Security Modernization Act of
35 2014," Pub.L.113-283; or

36 (d) Part 162 of Title 45 of the Code of Federal Regulations,
37 established pursuant to the "Health Information Technology for
38 Economic and Clinical Health Act," Pub.L.111-5.

39 (2) When a framework listed in paragraph (1) of this subsection
40 is amended, a covered entity whose cybersecurity program
41 reasonably conforms to that framework shall reasonably conform,
42 as determined by the director, to the amended framework not later
43 than one year after the effective date of the amended framework.

44 c. (1) The cybersecurity program reasonably complies, as
45 determined by the director, with both the current version of the
46 Payment Card Industry (PCI) Data Security Standard and
47 reasonably conforms to the current version of another applicable

1 industry recognized cybersecurity framework listed in subsection a.
2 of this section, subject to required revisions, if applicable.

3 (2) When a final revision to the PCI Data Security Standard is
4 published, a covered entity whose cybersecurity program
5 reasonably complies with that standard shall reasonably comply, as
6 determined by the director, with the revised standard not later than
7 one year after the publication date stated in the revision.

8 d. If the director determines that a covered entity's
9 cybersecurity program reasonably conforms to a combination of
10 industry-recognized cybersecurity frameworks, or complies with a
11 standard, as in the case of the PCI Data Security Standard, pursuant
12 to subsection c. of this section, and two or more of those
13 frameworks are revised, the covered entity whose cybersecurity
14 program reasonably conforms to or complies with, as applicable,
15 those frameworks shall reasonably conform to or comply with, as
16 applicable, all of the revised frameworks not later than one year
17 after the latest publication date stated in the revisions.

18

19 4. Where a covered entity asserts an affirmative defense
20 pursuant to P.L. , c. (C.) (pending before the Legislature as
21 this bill), the court shall consider the director's determination of
22 reasonable conformance, pursuant to section 3 of
23 P.L. , c. (C.) (pending before the Legislature as this bill), as
24 evidence in order to determine whether the covered entity is entitled
25 to the affirmative defense. A covered entity may raise the
26 affirmative defense in court without the director's determination of
27 reasonable conformance. Absent the director's determination of
28 reasonable conformance, the court may determine reasonable
29 conformance pursuant to the standards set forth in section 3 of
30 P.L. , c. (C.) (pending before the Legislature as this bill).

31

32 5. The provisions of P.L. , c. (C.) (pending before the
33 Legislature as this bill) shall not be construed to provide a private
34 right of action, including a class action, with respect to any practice
35 regulated under P.L. , c. (C.) (pending before the
36 Legislature as this bill).

37

38 6. The Director of the Division of Consumer Affairs in the
39 Department of Law and Public Safety shall adopt, pursuant to the
40 "Administrative Procedure Act," P.L.1968, c.410 (C.52:14B-1 et
41 seq.), within 90 days of the effective date of P.L. , c. (C.)
42 (pending before the Legislature as this bill), any rules and
43 regulations necessary to effectuate the purposes of P.L. ,
44 c. (C.) (pending before the Legislature as this bill), including
45 the number of days the director has to make a determination
46 pursuant to section 3 of P.L. , c. (C.) (pending before the
47 Legislature as this bill).

1 7. This act shall take effect immediately.

2

3

4

STATEMENT

5

6 This bill creates an affirmative defense for breaches of security
7 of personal and restricted information, as those terms are defined in
8 the bill. The bill requires that if a covered entity, as that term is
9 defined in the bill, seeks an affirmative defense to a breach of
10 security, it is to have created, maintained, and complied with a
11 written cybersecurity program that contains administrative,
12 technical, and physical safeguards for the protection of personal
13 information or restricted information, or both, and that reasonably
14 conforms to an industry recognized cybersecurity framework. A
15 covered entity's cybersecurity program is to be designed to protect
16 against the following:

17 1) breaches of the security and confidentiality of personal
18 information, restricted information, or both;

19 2) any anticipated threats or hazards to the security or integrity
20 of personal information, restricted information, or both; and

21 3) unauthorized access to and acquisition of personal
22 information, restricted information, or both that is likely to result in
23 a material risk of identity theft or other fraud to the individual to
24 whom the information relates.

25 The bill requires that the scale and scope of a covered entity's
26 cybersecurity program is to be based on all of the following factors:

27 1) the size and complexity of the covered entity;

28 2) the nature and scope of the activities of the covered entity;

29 3) the sensitivity of the information to be protected;

30 4) the cost and availability of tools to improve information
31 security and reduce vulnerabilities; and

32 5) the resources available to the covered entity.

33 The bill permits the Director of the Division of Consumer Affairs
34 in the Department of Law and Public Safety (director) to deem a
35 covered entity's cybersecurity program, required by the bill, to
36 reasonably conform to an industry recognized cybersecurity
37 framework if the covered entity's cybersecurity program reasonably
38 conforms to any of the cybersecurity frameworks or provisions of
39 law enumerated in the bill. A determination of reasonable
40 conformance by the director is to be considered by a court as
41 evidence in order to determine whether the covered entity is entitled
42 to an affirmative defense. A covered entity may raise the
43 affirmative defense in court without the director's determination of
44 reasonable conformance. Absent the director's determination of
45 reasonable conformance, the court may determine reasonable
46 conformance pursuant to the standards set forth in the bill.

A3984 B.DECROCE

7

- 1 The provisions of the bill are not to be construed to provide a
- 2 private right of action, including a class action, with respect to any
- 3 practice regulated under the bill.