# SENATE, No. 3062

# STATE OF NEW JERSEY

## 219th LEGISLATURE

INTRODUCED OCTOBER 22, 2020

**Sponsored by:**
**Senator ANTHONY M. BUCCO**
**District 25 (Morris and Somerset)**

**SYNOPSIS**

Creates affirmative defense for certain breaches of security.

**CURRENT VERSION OF TEXT**

As introduced.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(3) unauthorized access to and acquisition personal information, restricted information, or both 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, required by subsection a. of this section, shall be based on 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 information security and reduce vulnerabilities; and

(5) the resources available to the covered entity.

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

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

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

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

(b) NIST special publication 800-171;

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

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

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

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

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

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

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

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

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

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

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

c. (1) The cybersecurity program reasonably complies, as determined by the director, with both the current version of the Payment Card Industry (PCI) Data Security Standard and reasonably conforms to the current version of another applicable industry recognized cybersecurity framework listed in subsection a. of this section, subject to required revisions, if applicable.

(2) When a final revision to the PCI Data Security Standard is published, a covered entity whose cybersecurity program reasonably complies with that standard shall reasonably comply, as

determined by the director, with the revised standard not later than one year after the publication date stated in the revision.

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

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

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

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

7. This act shall take effect immediately.

STATEMENT

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

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

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

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

The bill requires that the scale and scope of a covered entity's cybersecurity program is to be based on 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 information security and reduce vulnerabilities; and

5) the resources available to the covered entity.

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

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