

[First Reprint]

SENATE, No. 1233

STATE OF NEW JERSEY
219th LEGISLATURE

INTRODUCED FEBRUARY 3, 2020

Sponsored by:

Senator THOMAS H. KEAN, JR.

District 21 (Morris, Somerset and Union)

Senator NELLIE POU

District 35 (Bergen and Passaic)

Co-Sponsored by:

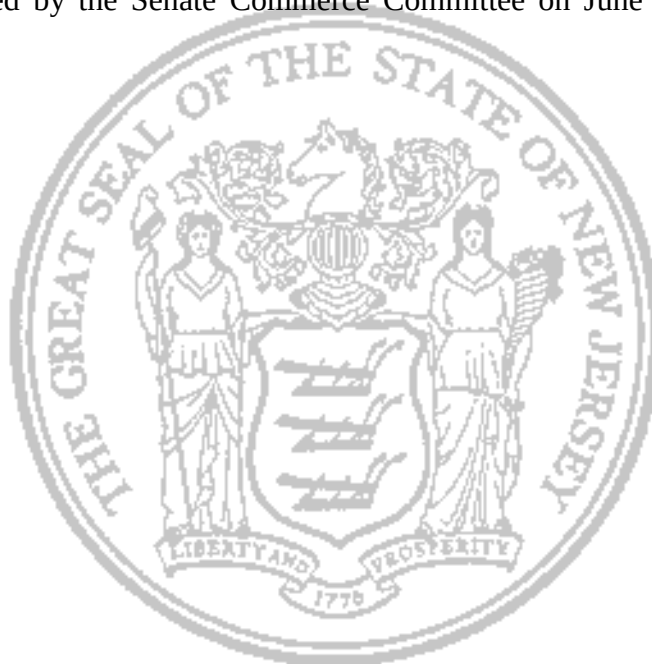
Senator Gill

SYNOPSIS

Requires certain persons and business entities to maintain comprehensive information security program.

CURRENT VERSION OF TEXT

As reported by the Senate Commerce Committee on June 16, 2021, with amendments.



(Sponsorship Updated As Of: 12/2/2021)

1 **AN ACT** concerning comprehensive information security programs
 2 and supplementing P.L.1960, c.39 (C.56:8-1 et seq.).

3
 4 **BE IT ENACTED** *by the Senate and General Assembly of the State*
 5 *of New Jersey:*

6
 7 1. As used in this act:

8 “Breach of security” means the unauthorized acquisition or
 9 unauthorized use of unencrypted data or encrypted electronic data and
 10 the confidential process or key that is capable of compromising the
 11 security, confidentiality, or integrity of personal information
 12 maintained by a person or agency, that creates a substantial risk of
 13 identity theft or fraud against a resident of the State. A good faith but
 14 unauthorized acquisition of personal information by a person or
 15 agency, or employee or agent thereof, for the lawful purposes of the
 16 person or agency, is not a breach of security unless the personal
 17 information is used in an unauthorized manner or subject to further
 18 unauthorized disclosure.

19 “Electronic” means relating to technology or having electrical,
 20 digital, magnetic, wireless, optical, electromagnetic or similar
 21 capabilities.

22 “Encrypted” means the transformation of data into a form in which
 23 meaning cannot be assigned without the use of a confidential process
 24 or key.

25 “Owns or licenses” means receives, stores, maintains, processes, or
 26 otherwise has access to personal information in connection with the
 27 provision of goods or services or in connection with employment.

28 “Person” means a natural person, corporation, association,
 29 partnership or other legal entity, other than an agency, department,
 30 board, commission, bureau, division or authority of the State or any
 31 political subdivision thereof. ¹“Person” includes, but is not limited to,
 32 a financial service firm, investment firm, and digital asset business as
 33 that term is defined in P.L. c. (C.) (pending before the
 34 Legislature as Senate Bill No. 3132 of 2020). “Person” shall not
 35 include an insured depository institution as defined pursuant to the
 36 "Federal Deposit Insurance Act," 12 U.S.C. s.1813, an insured credit
 37 union as defined pursuant to 12 U.S.C. s.1752, or a financial institution
 38 or an affiliate of a financial institution that is subject to Title V of the
 39 federal "Gramm-Leach-Bliley Act," 15 U.S.C. s.6801 et seq. and the
 40 rules and implementing regulations promulgated thereunder.¹

41 “Personal information” means a New Jersey resident's first name
 42 and last name or first initial and last name in combination with any one
 43 or more of the following data elements that relate to a resident: (1)
 44 Social Security number; (2) driver's license number or state-issued
 45 identification card number; or (3) financial account number, or credit
 46 or debit card number, with or without any required security code,

EXPLANATION – Matter enclosed in bold-faced brackets **[thus]** in the above bill is
 not enacted and is intended to be omitted in the law.

Matter underlined thus is new matter.

Matter enclosed in superscript numerals has been adopted as follows:

¹Senate SCM committee amendments adopted June 16, 2021.

1 access code, personal identification number or password, that would
2 permit access to a resident's financial account; provided, however, that
3 "personal information" shall not include information that is lawfully
4 obtained from publicly available information, or from federal, state or
5 local government records lawfully made available to the general
6 public.

7 "Record" means any material upon which written, drawn, spoken,
8 visual, or electromagnetic information or images are recorded or
9 preserved, regardless of physical form or characteristics.

10 "Service provider" means any person that receives, stores,
11 maintains, processes, or otherwise is permitted access to personal
12 information through its provision of services directly to a person that is
13 subject to this act.

14

15 2. a. Every person that owns or licenses personal information
16 about a resident of the State shall develop, implement, and maintain
17 a comprehensive information security program that is written in one
18 or more readily accessible parts and contains administrative,
19 technical, and physical safeguards that are appropriate to:

20 (1) the size, scope and type of business of the person obligated
21 to safeguard the personal information under the comprehensive
22 information security program;

23 (2) the amount of resources available to that person;

24 (3) the amount of stored data; and

25 (4) the need for security and confidentiality of both consumer
26 and employee information.

27 The safeguards contained in the program shall be consistent with
28 the safeguards for protection of personal information and
29 information of a similar character set forth in any State or federal
30 regulations by which the person who owns or licenses the
31 information may be regulated.

32 b. Every comprehensive information security program shall
33 include, but shall not be limited to:

34 (1) designating one or more employees to maintain the
35 comprehensive information security program;

36 (2) identifying and assessing reasonably foreseeable internal and
37 external risks to the security, confidentiality, and integrity of any
38 electronic, paper or other records containing personal information,
39 and evaluating and improving, where necessary, the effectiveness of
40 the current safeguards for limiting the risks, including but not
41 limited to:

42 (a) ongoing employee training, including ongoing training for
43 temporary and contract employees;

44 (b) employee compliance with policies and procedures; and

45 (c) means for detecting and preventing security system failures;

46 (3) developing security policies for employees relating to the
47 storage, access and transportation of records containing personal
48 information outside of business premises;

- 1 (4) imposing disciplinary measures for violations of the
- 2 comprehensive information security program rules;
- 3 (5) preventing terminated employees from accessing records
- 4 containing personal information;
- 5 (6) oversight of service providers by:
- 6 (a) taking reasonable steps to select and retain third-party
- 7 service providers that are capable of maintaining appropriate
- 8 security measures to protect personal information consistent with
- 9 this act and any applicable federal regulations; and
- 10 (b) requiring third-party service providers by contract to
- 11 implement and maintain appropriate security measures for personal
- 12 information;
- 13 (7) reasonable restrictions upon physical access to records
- 14 containing personal information, and storage of records and data in
- 15 locked facilities, storage areas or containers;
- 16 (8) regular monitoring to ensure that the comprehensive
- 17 information security program is operating in a manner reasonably
- 18 calculated to prevent unauthorized access to or unauthorized use of
- 19 personal information, and upgrading information safeguards as
- 20 necessary to limit risks;
- 21 (9) reviewing the scope of the security measures at least
- 22 annually or whenever there is a material change in business
- 23 practices that may reasonably implicate the security or integrity of
- 24 records containing personal information; and
- 25 (10) documenting responsive actions taken in connection with
- 26 any incident involving a breach of security, and mandatory post-
- 27 incident review of events and actions taken, if any, to make changes
- 28 in business practices relating to protection of personal information.
- 29
- 30 3. Every person that owns or licenses personal information
- 31 about a resident of this State and electronically stores or transmits
- 32 the information shall include in its comprehensive information
- 33 security program the establishment and maintenance of a security
- 34 system covering its computers, including any wireless system, that,
- 35 at a minimum, and to the extent technically feasible, shall have the
- 36 following elements:
- 37 a. secure user authentication protocols including:
- 38 (1) control of user IDs and other identifiers;
- 39 (2) a reasonably secure method of assigning and selecting
- 40 passwords, or use of unique identifier technologies, such as
- 41 biometrics or token devices;
- 42 (3) control of data security passwords to ensure that passwords
- 43 are kept in a location or format that does not compromise the
- 44 security of the data they protect;
- 45 (4) restricting access to active users and active user accounts
- 46 only; and

- 1 (5) blocking access to user identification after multiple
- 2 unsuccessful attempts to gain access or the limitation placed on
- 3 access for the particular system;
- 4 b. secure access control measures that:
- 5 (1) restrict access to records and files containing personal
- 6 information to those who need that information to perform their job
- 7 duties; and
- 8 (2) assign unique identifications and passwords, which are not
- 9 vendor supplied default passwords, to each person with computer
- 10 access, that are reasonably designed to maintain the integrity of the
- 11 security of the access controls;
- 12 c. encryption of all transmitted records and files containing
- 13 personal information that will travel across public networks, and
- 14 encryption of all data containing personal information to be
- 15 transmitted wirelessly;
- 16 d. reasonable monitoring of systems for unauthorized use of or
- 17 access to personal information;
- 18 e. encryption of all personal information stored on laptops or
- 19 other portable devices;
- 20 f. with respect to files containing personal information on a
- 21 system that is connected to the Internet, reasonably up-to-date
- 22 firewall protection and operating system security patches, which are
- 23 reasonably designed to maintain the integrity of the personal
- 24 information;
- 25 g. reasonably up-to-date versions of system security agent
- 26 software which shall include malware protection and reasonably up-
- 27 to-date patches and virus definitions, or a version of that software
- 28 that can still be supported with up-to-date patches and virus
- 29 definitions, and is set to receive the most current security updates
- 30 on a regular basis; and
- 31 h. education and training of employees on the proper use of the
- 32 computer security system and the importance of personal
- 33 information security.
- 34
- 35 4. It shall be an unlawful practice and a violation of P.L.1960,
- 36 c.39 (C.56:8-1 et seq.) to willfully, knowingly or recklessly violate
- 37 the provisions of this act.
- 38
- 39 5. This act shall take effect on the 120th day next following
- 40 enactment.