

# SENATE, No. 2692

## STATE OF NEW JERSEY 218th LEGISLATURE

INTRODUCED JUNE 11, 2018

**Sponsored by:**

**Senator THOMAS H. KEAN, JR.**

**District 21 (Morris, Somerset and Union)**

**SYNOPSIS**

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

**CURRENT VERSION OF TEXT**

As introduced.



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  
10 and the confidential process or key that is capable of compromising  
11 the 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  
14 but 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  
23 which meaning cannot be assigned without the use of a confidential  
24 process or key.

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

29 “Person” means a natural person, corporation, association,  
30 partnership or other legal entity, other than an agency, department,  
31 board, commission, bureau, division or authority of the State or any  
32 political subdivision thereof.

33 “Personal information” means a New Jersey resident's first name  
34 and last name or first initial and last name in combination with any  
35 one or more of the following data elements that relate to a resident:  
36 (1) Social Security number; (2) driver's license number or state-  
37 issued identification card number; or (3) financial account number,  
38 or credit or debit card number, with or without any required security  
39 code, access code, personal identification number or password, that  
40 would permit access to a resident's financial account; provided,  
41 however, that “personal information” shall not include information  
42 that is lawfully obtained from publicly available information, or  
43 from federal, state or local government records lawfully made  
44 available to the general public.

45 “Record” means any material upon which written, drawn,  
46 spoken, visual, or electromagnetic information or images are  
47 recorded or preserved, regardless of physical form or  
48 characteristics.

1       “Service provider” means any person that receives, stores,  
2 maintains, processes, or otherwise is permitted access to personal  
3 information through its provision of services directly to a person  
4 that is subject to this act.

5  
6       2. a. Every person that owns or licenses personal information  
7 about a resident of the State shall develop, implement, and maintain  
8 a comprehensive information security program that is written in one  
9 or more readily accessible parts and contains administrative,  
10 technical, and physical safeguards that are appropriate to:

11       (1) the size, scope and type of business of the person obligated  
12 to safeguard the personal information under the comprehensive  
13 information security program;

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

15       (3) the amount of stored data; and

16       (4) the need for security and confidentiality of both consumer  
17 and employee information.

18       The safeguards contained in the program shall be consistent with  
19 the safeguards for protection of personal information and  
20 information of a similar character set forth in any State or federal  
21 regulations by which the person who owns or licenses the  
22 information may be regulated.

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

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

27       (2) identifying and assessing reasonably foreseeable internal and  
28 external risks to the security, confidentiality, and integrity of any  
29 electronic, paper or other records containing personal information,  
30 and evaluating and improving, where necessary, the effectiveness of  
31 the current safeguards for limiting the risks, including but not  
32 limited to:

33       (a) ongoing employee training, including ongoing training for  
34 temporary and contract employees;

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

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

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

40       (4) imposing disciplinary measures for violations of the  
41 comprehensive information security program rules;

42       (5) preventing terminated employees from accessing records  
43 containing personal information;

44       (6) oversight of service providers by:

45       (a) taking reasonable steps to select and retain third-party  
46 service providers that are capable of maintaining appropriate  
47 security measures to protect personal information consistent with  
48 this act and any applicable federal regulations; and

1 (b) requiring third-party service providers by contract to  
2 implement and maintain appropriate security measures for personal  
3 information;

4 (7) reasonable restrictions upon physical access to records  
5 containing personal information, and storage of records and data in  
6 locked facilities, storage areas or containers;

7 (8) regular monitoring to ensure that the comprehensive  
8 information security program is operating in a manner reasonably  
9 calculated to prevent unauthorized access to or unauthorized use of  
10 personal information, and upgrading information safeguards as  
11 necessary to limit risks;

12 (9) reviewing the scope of the security measures at least  
13 annually or whenever there is a material change in business  
14 practices that may reasonably implicate the security or integrity of  
15 records containing personal information; and

16 (10) documenting responsive actions taken in connection with  
17 any incident involving a breach of security, and mandatory post-  
18 incident review of events and actions taken, if any, to make changes  
19 in business practices relating to protection of personal information.  
20

21 3. Every person that owns or licenses personal information  
22 about a resident of this State and electronically stores or transmits  
23 the information shall include in its comprehensive information  
24 security program the establishment and maintenance of a security  
25 system covering its computers, including any wireless system, that,  
26 at a minimum, and to the extent technically feasible, shall have the  
27 following elements:

28 a. secure user authentication protocols including:

29 (1) control of user IDs and other identifiers;

30 (2) a reasonably secure method of assigning and selecting  
31 passwords, or use of unique identifier technologies, such as  
32 biometrics or token devices;

33 (3) control of data security passwords to ensure that passwords  
34 are kept in a location or format that does not compromise the  
35 security of the data they protect;

36 (4) restricting access to active users and active user accounts  
37 only; and

38 (5) blocking access to user identification after multiple  
39 unsuccessful attempts to gain access or the limitation placed on  
40 access for the particular system;

41 b. secure access control measures that:

42 (1) restrict access to records and files containing personal  
43 information to those who need that information to perform their job  
44 duties; and

45 (2) assign unique identifications and passwords, which are not  
46 vendor supplied default passwords, to each person with computer  
47 access, that are reasonably designed to maintain the integrity of the  
48 security of the access controls;

- 1       c. encryption of all transmitted records and files containing  
2 personal information that will travel across public networks, and  
3 encryption of all data containing personal information to be  
4 transmitted wirelessly;
- 5       d. reasonable monitoring of systems for unauthorized use of or  
6 access to personal information;
- 7       e. encryption of all personal information stored on laptops or  
8 other portable devices;
- 9       f. with respect to files containing personal information on a  
10 system that is connected to the Internet, reasonably up-to-date  
11 firewall protection and operating system security patches, which are  
12 reasonably designed to maintain the integrity of the personal  
13 information;
- 14       g. reasonably up-to-date versions of system security agent  
15 software which shall include malware protection and reasonably up-  
16 to-date patches and virus definitions, or a version of that software  
17 that can still be supported with up-to-date patches and virus  
18 definitions, and is set to receive the most current security updates  
19 on a regular basis; and
- 20       h. education and training of employees on the proper use of the  
21 computer security system and the importance of personal  
22 information security.

23  
24       4. It shall be an unlawful practice and a violation of P.L.1960,  
25 c.39 (C.56:8-1 et seq.) to willfully, knowingly or recklessly violate  
26 the provisions of this act.

27  
28       5. This act shall take effect on the 120th day next following  
29 enactment.

30

31

32

## STATEMENT

33

34       This bill requires any person, corporation, association,  
35 partnership or other legal entity that owns or licenses personal  
36 information about a resident of this State to develop, implement,  
37 and maintain a comprehensive information security program that is  
38 written in one or more readily accessible parts and contains  
39 administrative, technical, and physical safeguards that are necessary  
40 to protect the personal information.

41       The bill provides that it would be an unlawful practice under the  
42 consumer fraud act, P.L.1960, c.39 (C.56:8-1 et seq.), to willfully,  
43 knowingly or recklessly violate the provisions of the bill. An  
44 unlawful practice is punishable by a monetary penalty of not more  
45 than \$10,000 for a first offense and not more than \$20,000 for any  
46 subsequent offense. Additionally, a violation can result in cease  
47 and desist orders issued by the Attorney General, the assessment of  
48 punitive damages, and the awarding of treble damages and costs to  
49 those injured as a result of the violation.