

[First Reprint]
SENATE, No. 52

STATE OF NEW JERSEY
218th LEGISLATURE

PRE-FILED FOR INTRODUCTION IN THE 2018 SESSION

Sponsored by:

Senator TROY SINGLETON

District 7 (Burlington)

Senator NIA H. GILL

District 34 (Essex and Passaic)

Assemblyman RALPH R. CAPUTO

District 28 (Essex)

Assemblyman JAY WEBBER

District 26 (Essex, Morris and Passaic)

Assemblywoman CAROL A. MURPHY

District 7 (Burlington)

Co-Sponsored by:

Senator Lagana, Assemblywomen B.DeCroce, Handlin, Assemblyman Benson, Assemblywomen Pinkin, Quijano, Assemblyman Verrelli, Assemblywomen Vainieri Huttel, Downey, Assemblymen Houghtaling, Conaway, Assemblywoman Jasey and Assemblyman Moriarty

SYNOPSIS

Requires disclosure of breach of security of online account.

CURRENT VERSION OF TEXT

As reported by the Senate Commerce Committee on May 10, 2018, with amendments.



(Sponsorship Updated As Of: 2/26/2019)

1 AN ACT concerning disclosure of breaches of security and
2 amending P.L.2005, c.226.

3

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

6

7 1. Section 10 of P.L.2005, c.226 (C.56:8-161) is amended to
8 read as follows:

9 10. As used in sections 10 through 15 of **[this amendatory and**
10 **supplementary act]** P.L.2005, c.226 (C.56:8-161 through C.56:8-
11 166):

12 "Breach of security" means unauthorized access to electronic
13 files, media or data containing personal information that
14 compromises the security, confidentiality or integrity of personal
15 information when access to the personal information has not been
16 secured by encryption or by any other method or technology that
17 renders the personal information unreadable or unusable. Good
18 faith acquisition of personal information by an employee or agent of
19 the business for a legitimate business purpose is not a breach of
20 security, provided that the personal information is not used for a
21 purpose unrelated to the business or subject to further unauthorized
22 disclosure.

23 "Business" means a sole proprietorship, partnership, corporation,
24 association, or other entity, however organized and whether or not
25 organized to operate at a profit, including a financial institution
26 organized, chartered, or holding a license or authorization
27 certificate under the law of this State, any other state, the United
28 States, or of any other country, or the parent or the subsidiary of a
29 financial institution.

30 "Communicate" means to send a written or other tangible record
31 or to transmit a record by any means agreed upon by the persons
32 sending and receiving the record.

33 "Customer" means an individual who provides personal
34 information to a business.

35 "Individual" means a natural person.

36 "Internet" means the international computer network of both
37 federal and non-federal interoperable packet switched data
38 networks.

39 "Personal information" means an individual's first name or first
40 initial and last name linked with any one or more of the following
41 data elements: (1) Social Security number; (2) driver's license
42 number or State identification card number; **[or]** (3) account
43 number or credit or debit card number, in combination with any
44 required security code, access code, or password that would permit

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 May 10, 2018.

1 access to an individual's financial account; or (4) user name, email
2 address, or any other account holder identifying information, in
3 combination with any password or security question and answer
4 that would permit access to an online account. Dissociated data
5 that, if linked, would constitute personal information is personal
6 information if the means to link the dissociated data were accessed
7 in connection with access to the dissociated data.

8 For the purposes of sections 10 through 15 of **【this amendatory**
9 **and supplementary act】** P.L.2005, C.226 (C.56:8-161 through
10 C.56:8-166, personal information shall not include publicly
11 available information that is lawfully made available to the general
12 public from federal, state or local government records, or widely
13 distributed media.

14 "Private entity" means any individual, corporation, company,
15 partnership, firm, association, or other entity, other than a public
16 entity.

17 "Public entity" includes the State, and any county, municipality,
18 district, public authority, public agency, and any other political
19 subdivision or public body in the State. For the purposes of
20 sections 10 through 15 **【of this amendatory and supplementary act】**
21 P.L.2005, C.226 (C.56:8-161 through C.56:8-166, public entity
22 does not include the federal government.

23 "Publicly post" or "publicly display" means to intentionally
24 communicate or otherwise make available to the general public.

25 "Records" means any material, regardless of the physical form,
26 on which information is recorded or preserved by any means,
27 including written or spoken words, graphically depicted, printed, or
28 electromagnetically transmitted. Records does not include publicly
29 available directories containing information an individual has
30 voluntarily consented to have publicly disseminated or listed.

31 (cf: P.L.2005, c.226, s.10)

32

33 ¹2. Section 12 of P.L.2005, c.226 (C.56:8-163) is amended to
34 read as follows:

35 12. a. Any business that conducts business in New Jersey, or
36 any public entity that compiles or maintains computerized records
37 that include personal information, shall disclose any breach of
38 security of those computerized records following discovery or
39 notification of the breach to any customer who is a resident of New
40 Jersey whose personal information was, or is reasonably believed to
41 have been, accessed by an unauthorized person. The disclosure to a
42 customer shall be made in the most expedient time possible and
43 without unreasonable delay, consistent with the legitimate needs of
44 law enforcement, as provided in subsection c. of this section, or any
45 measures necessary to determine the scope of the breach and restore
46 the reasonable integrity of the data system. Disclosure of a breach
47 of security to a customer shall not be required under this section if
48 the business or public entity establishes that misuse of the

1 information is not reasonably possible. Any determination shall be
2 documented in writing and retained for five years.

3 b. Any business or public entity that compiles or maintains
4 computerized records that include personal information on behalf of
5 another business or public entity shall notify that business or public
6 entity, who shall notify its New Jersey customers, as provided in
7 subsection a. of this section, of any breach of security of the
8 computerized records immediately following discovery, if the
9 personal information was, or is reasonably believed to have been,
10 accessed by an unauthorized person.

11 c. (1) Any business or public entity required under this
12 section to disclose a breach of security of a customer's personal
13 information shall, in advance of the disclosure to the customer,
14 report the breach of security and any information pertaining to the
15 breach to the Division of State Police in the Department of Law and
16 Public Safety for investigation or handling, which may include
17 dissemination or referral to other appropriate law enforcement
18 entities.

19 (2) The notification required by this section shall be delayed if a
20 law enforcement agency determines that the notification will
21 impede a criminal or civil investigation and that agency has made a
22 request that the notification be delayed. The notification required
23 by this section shall be made after the law enforcement agency
24 determines that its disclosure will not compromise the investigation
25 and notifies that business or public entity.

26 d. For purposes of this section, notice may be provided by one
27 of the following methods:

28 (1) Written notice;

29 (2) Electronic notice, if the notice provided is consistent with
30 the provisions regarding electronic records and signatures set forth
31 in section 101 of the federal "Electronic Signatures in Global and
32 National Commerce Act" (15 U.S.C. s.7001); or

33 (3) Substitute notice, if the business or public entity
34 demonstrates that the cost of providing notice would exceed
35 \$250,000, or that the affected class of subject persons to be notified
36 exceeds 500,000, or the business or public entity does not have
37 sufficient contact information. Substitute notice shall consist of all
38 of the following:

39 (a) E-mail notice when the business or public entity has an e-
40 mail address;

41 (b) Conspicuous posting of the notice on the Internet web site
42 page of the business or public entity, if the business or public entity
43 maintains one; and

44 (c) Notification to major Statewide media.

45 e. Notwithstanding subsection d. of this section, a business or
46 public entity that maintains its own notification procedures as part
47 of an information security policy for the treatment of personal
48 information, and is otherwise consistent with the requirements of

1 this section, shall be deemed to be in compliance with the
2 notification requirements of this section if the business or public
3 entity notifies subject customers in accordance with its policies in
4 the event of a breach of security of the system.

5 f. In addition to any other disclosure or notification required
6 under this section, in the event that a business or public entity
7 discovers circumstances requiring notification pursuant to this
8 section of more than 1,000 persons at one time, the business or
9 public entity shall also notify, without unreasonable delay, all
10 consumer reporting agencies that compile or maintain files on
11 consumers on a nationwide basis, as defined by subsection (p) of
12 section 603 of the federal "Fair Credit Reporting Act" (15 U.S.C.
13 s.1681a), of the timing, distribution and content of the notices.

14 g. (1) Notwithstanding subsection d. of this section, in the
15 case of a breach of security involving a user name or password, in
16 combination with any password or security question and answer
17 that would permit access to an online account, and no other
18 personal information as defined in section 10 of P.L.2005, c.226
19 (C.56:8-161), the business or public entity may provide the
20 notification in electronic or other form that directs the customer
21 whose personal information has been breached to promptly change
22 any password and security question or answer, as applicable, or to
23 take other appropriate steps to protect the online account with the
24 business or public entity and all other online accounts for which the
25 customer uses the same user name or email address and password or
26 security question or answer.

27 (2) Any business or public entity that furnishes an email account
28 shall not provide notification to the email account that is subject to
29 a security breach. The business or public entity shall provide notice
30 by another method described in this section or by clear and
31 conspicuous notice delivered to the customer online when the
32 customer is connected to the online account from an Internet
33 Protocol address or online location from which the business or
34 public entity knows the customer customarily accesses the account.¹
35 (cf: P.L.2005, c.226, s.12)

36

37 ¹**[2.] 3.** This act shall take effect on the first day of the fourth
38 month next following enactment.