

P.L. 2019, CHAPTER 95, *approved May 10, 2019*
Senate, No. 52 (*First Reprint*)

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

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 data elements: (1) Social Security number; (2) driver's license
2 number or State identification card number; **【or】** (3) account
3 number or credit or debit card number, in combination with any
4 required security code, access code, or password that would permit
5 access to an individual's financial account; or (4) user name, email
6 address, or any other account holder identifying information, in
7 combination with any password or security question and answer
8 that would permit access to an online account. Dissociated data
9 that, if linked, would constitute personal information is personal
10 information if the means to link the dissociated data were accessed
11 in connection with access to the dissociated data.

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

18 "Private entity" means any individual, corporation, company,
19 partnership, firm, association, or other entity, other than a public
20 entity.

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

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

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

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

36

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

39 12. a. Any business that conducts business in New Jersey, or
40 any public entity that compiles or maintains computerized records
41 that include personal information, shall disclose any breach of
42 security of those computerized records following discovery or
43 notification of the breach to any customer who is a resident of New
44 Jersey whose personal information was, or is reasonably believed to
45 have been, accessed by an unauthorized person. The disclosure to a
46 customer shall be made in the most expedient time possible and
47 without unreasonable delay, consistent with the legitimate needs of

1 law enforcement, as provided in subsection c. of this section, or any
2 measures necessary to determine the scope of the breach and restore
3 the reasonable integrity of the data system. Disclosure of a breach
4 of security to a customer shall not be required under this section if
5 the business or public entity establishes that misuse of the
6 information is not reasonably possible. Any determination shall be
7 documented in writing and retained for five years.

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

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

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

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

33 (1) Written notice;

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

38 (3) Substitute notice, if the business or public entity
39 demonstrates that the cost of providing notice would exceed
40 \$250,000, or that the affected class of subject persons to be notified
41 exceeds 500,000, or the business or public entity does not have
42 sufficient contact information. Substitute notice shall consist of all
43 of the following:

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

46 (b) Conspicuous posting of the notice on the Internet web site
47 page of the business or public entity, if the business or public entity
48 maintains one; and

1 (c) Notification to major Statewide media.

2 e. Notwithstanding subsection d. of this section, a business or
3 public entity that maintains its own notification procedures as part
4 of an information security policy for the treatment of personal
5 information, and is otherwise consistent with the requirements of
6 this section, shall be deemed to be in compliance with the
7 notification requirements of this section if the business or public
8 entity notifies subject customers in accordance with its policies in
9 the event of a breach of security of the system.

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

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

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

41

42 ¹[2.] 3.¹ This act shall take effect on the first day of the fourth
43 month next following enactment.

44

45

46

47

48

Requires disclosure of breach of security of online account.