

ASSEMBLY, No. 3590

STATE OF NEW JERSEY 219th LEGISLATURE

INTRODUCED FEBRUARY 25, 2020

Sponsored by:

Assemblyman STERLEY S. STANLEY

District 18 (Middlesex)

Assemblywoman BRITNEE N. TIMBERLAKE

District 34 (Essex and Passaic)

SYNOPSIS

Revises requirements for disclosure of a breach of security of certain computerized records containing personal information.

CURRENT VERSION OF TEXT

As introduced.



(Sponsorship Updated As Of: 1/27/2021)

1 AN ACT concerning the security of personal information 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 12 of P.L.2005, c.226 (C.56:8-163) is amended to
8 read as follows:

9 12. a. Any business that conducts business in New Jersey, or
10 any public entity that compiles or maintains computerized records
11 that include personal information, shall disclose any breach of
12 security of those computerized records following discovery or
13 notification of the breach to any customer who is a resident of New
14 Jersey whose personal information was, or is reasonably believed to
15 have been, accessed by an unauthorized person. The disclosure to a
16 customer shall be made in the most expedient time possible and
17 without unreasonable delay, not to exceed five business days,
18 except as is consistent with the legitimate needs of law
19 enforcement, as provided in subsection c. of this section, or any
20 measures necessary to determine the scope of the breach and restore
21 the reasonable integrity of the data system. Disclosure of a breach
22 of security to a customer shall not be required under this section if,
23 after an appropriate investigation by the business or public entity
24 and consultation with relevant federal, State and local agencies
25 responsible for law enforcement, the business or public entity
26 establishes that misuse of the information is not reasonably
27 possible. Any determination shall be documented in writing and
28 retained for five years.

29 b. Any business or public entity that compiles or maintains
30 computerized records that include personal information on behalf of
31 another business or public entity shall notify that business or public
32 entity, who shall notify its New Jersey customers, as provided in
33 subsection a. of this section, of any breach of security of the
34 computerized records immediately following discovery, if the
35 personal information was, or is reasonably believed to have been,
36 accessed by an unauthorized person.

37 c. (1) Any business or public entity required under this section
38 to disclose a breach of security of a customer's personal information
39 shall, in advance of the disclosure to the customer, report the breach
40 of security and any information pertaining to the breach to the
41 Division of State Police in the Department of Law and Public
42 Safety for investigation or handling, which may include
43 dissemination or referral to other appropriate law enforcement
44 entities.

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.

1 (2) The notification required by this section shall be delayed if a
2 law enforcement agency determines that the notification will
3 impede a criminal or civil investigation and that agency has made a
4 request that the notification be delayed. The notification required
5 by this section shall be made after the law enforcement agency
6 determines that its disclosure will not compromise the investigation
7 and notifies that business or public entity.

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

10 (1) Written notice;

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

15 (3) Substitute notice, if the business or public entity
16 demonstrates that the cost of providing notice would exceed
17 \$250,000, or that the affected class of subject persons to be notified
18 exceeds 500,000, or the business or public entity does not have
19 sufficient contact information. Substitute notice shall consist of all
20 of the following:

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

23 (b) Conspicuous posting of the notice on the Internet web site
24 page of the business or public entity, if the business or public entity
25 maintains one; and

26 (c) Notification to major Statewide media.

27 e. Notwithstanding subsection d. of this section, a business or
28 public entity that maintains its own notification procedures as part
29 of an information security policy for the treatment of personal
30 information, and is otherwise consistent with the requirements of
31 this section, shall be deemed to be in compliance with the
32 notification requirements of this section if the business or public
33 entity notifies subject customers in accordance with its policies in
34 the event of a breach of security of the system.

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

44 g. (1) Notwithstanding subsection d. of this section, in the case
45 of a breach of security involving a user name or password, in
46 combination with any password or security question and answer
47 that would permit access to an online account, and no other
48 personal information as defined in section 10 of P.L.2005, c.226

1 (C.56:8-161), the business or public entity may provide the
2 notification in electronic or other form that directs the customer
3 whose personal information has been breached to promptly change
4 any password and security question or answer, as applicable, or to
5 take other appropriate steps to protect the online account with the
6 business or public entity and all other online accounts for which the
7 customer uses the same user name or email address and password or
8 security question or answer.

9 (2) Any business or public entity that furnishes an email account
10 shall not provide notification to the email account that is subject to
11 a security breach. The business or public entity shall provide notice
12 by another method described in this section or by clear and
13 conspicuous notice delivered to the customer online when the
14 customer is connected to the online account from an Internet
15 Protocol address or online location from which the business or
16 public entity knows the customer customarily accesses the account.

17 (cf: P.L.2019, c.95, s.2)

18
19 2. This act shall take effect immediately.

20 21 22 STATEMENT

23
24 This bill revises the "Identity Theft Prevention Act," P.L.2005,
25 c.226 (C.56:11-44 et al.) to provide that, in the event of any breach
26 of security of computerized records, the disclosure to a customer
27 whose personal information was breached shall be made within five
28 business days, except as is consistent with the legitimate needs of
29 law enforcement, or any measures necessary to determine the scope
30 of the breach and restore the reasonable integrity of the data system.
31 Current law requires that the disclosure be made in the most
32 expedient time possible and without unreasonable delay, which is
33 not changed under the bill.

34 Current law also provides that disclosure of a breach of security
35 to a customer shall not be required if the business or public entity
36 establishes that misuse of the information is not reasonably
37 possible. The bill clarifies that this determination can only be made
38 after an appropriate investigation by the business or public entity
39 and consultation with relevant federal, State and local agencies
40 responsible for law enforcement.