CHAPTER 95

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

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

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

C.56:8-161 Definitions relative to security of personal information.

10. As used in sections 10 through 15 of P.L.2005, c.226 (C.56:8-161 through C.56:8-166):

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

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

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

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

"Individual" means a natural person.

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

"Personal information" means an individual's first name or first initial and last name linked with any one or more of the following data elements: (1) Social Security number; (2) driver's license number or State identification card number; (3) account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account; or (4) user name,email address, or any other account holder identifying information,in combination with any password or security question and answer that would permit access to an online account. Dissociated data that, if linked, would constitute personal information is personal information if the means to link the dissociated data were accessed in connection with access to the dissociated data.

For the purposes of sections 10 through 15 of P.L.2005, C.226 (C.56:8-161 through C.56:8-166), personal information shall not include publicly available information that is lawfully made available to the general public from federal, state or local government records, or widely distributed media.

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

"Public entity" includes the State, and any county, municipality, district, public authority, public agency, and any other political subdivision or public body in the State. For the purposes of sections 10 through 15 of P.L.2005, c.226 (C.56:8-161 through C.56:8-166), public entity does not include the federal government.

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

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

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

C.56:8-163 Disclosure of breach of security to customers.

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

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

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

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

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

(1) Written notice;

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

(3) Substitute notice, if the business or public entity demonstrates that the cost of providing notice would exceed $250,000, or that the affected class of subject persons to be

notified exceeds 500,000, or the business or public entity does not have sufficient contact information. Substitute notice shall consist of all of the following:

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

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

(c) Notification to major Statewide media.

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

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

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

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

3. This act shall take effect on the first day of the fourth month next following enactment.

Approved May 10, 2019.