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

10. As used in sections 10 through 15 of this amendatory and supplementary act:

"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; or (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. 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 this amendatory and supplementary act, 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 this amendatory and supplementary act, 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.

L.2005,c.226,s.10.

56 :8-162 Methods of destruction of certain customer records.

11. A business or public entity shall destroy, or arrange for the destruction of, a customer's records within its custody or control containing personal information, which is no longer to be retained by the business or public entity, by shredding, erasing, or otherwise modifying the personal information in those records to make it unreadable, undecipherable or nonreconstructable through generally available means.

L.2005,c.226,s.11.

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.

L.2005,c.226,s.12.

56 :8-164 Prohibited actions relative to display of social security numbers.

13. a. No person, including any public or private entity, shall:

(1) Publicly post or publicly display an individual's Social Security number, or any four or more consecutive numbers taken from the individual's Social Security number;

(2) Print an individual's Social Security number on any materials that are mailed to the individual, unless State or federal law requires the Social Security number to be on the document to be mailed;

(3) Print an individual's Social Security number on any card required for the individual to access products or services provided by the entity;

(4) Intentionally communicate or otherwise make available to the general public an individual's Social Security number;

(5) Require an individual to transmit his Social Security number over the Internet, unless the connection is secure or the Social Security number is encrypted; or

(6) Require an individual to use his Social Security number to access an Internet web site, unless a password or unique personal identification number or other authentication device is also required to access the Internet web site.

b. Nothing in this section shall prevent a public or private entity from using a Social Security number for internal verification and administrative purposes, so long as the use does not require the release of the Social Security number to persons not designated by the entity to perform associated functions allowed or authorized by law.

c. Nothing in this section shall prevent the collection, use or release of a Social Security number, as required by State or federal law.

d. Notwithstanding this section, Social Security numbers may be included in applications and forms sent by mail, including documents sent as part of an application or enrollment process, or to establish, amend or terminate an account, contract or policy, or to confirm the accuracy of the Social Security number. A Social Security number that is permitted to be mailed under this subsection may not be printed, in whole or in part, on a postcard or other mailer not requiring an envelope, or visible on the envelope or without the envelope having been open.

e. Nothing in this section shall apply to documents that are recorded or required to be open to the public pursuant to Title 47 of the Revised Statutes. This section shall not apply to records that are required by statute, case law, or New Jersey Court Rules, to be made available to the public by entities provided for in Article VI of the New Jersey Constitution.

f. Nothing in this section shall apply to the interactive computer service provider's transmissions or routing or intermediate temporary storage or caching of an image, information or data that is otherwise subject to this section.

L.2005,c.226,s.13.

56 :8-165 Regulations concerning security of personal information.

14. The Director of the Division of Consumer Affairs in the Department of Law and Public Safety, in consultation with the Commissioner of Banking and Insurance, shall promulgate regulations pursuant to the "Administrative Procedure Act," P.L.1968, c.410 (C.52:14B-1 et seq.), necessary to effectuate sections 4 through 15 of this amendatory and supplementary act.

L.2005,c.226,s.14.

56 :8-166 Unlawful practice, violation.

15. It shall be an unlawful practice and a violation of P.L.1960, c.39 (C.56:8-1 et seq.) to willfully, knowingly or recklessly violate sections 10 through 13 of this amendatory and supplementary act.

L.2005,c.226,s.15.