ASSEMBLY, No. 3078

STATE OF NEW JERSEY

215th LEGISLATURE

INTRODUCED JUNE 14, 2012

Sponsored by:
Assemblywoman ANNETTE QUIJANO
District 20 (Union)

SYNOPSIS

Revises penalties imposed on businesses for failure to report security breach of computer system.

CURRENT VERSION OF TEXT

As introduced.

AN ACT concerning the security of computerized records and amending P.L.2005, c.226.

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

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

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

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 <u>thus</u> is new matter.

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.

<u>g. Any business or public entity that willfully, knowingly or recklessly violates the provisions of this section shall be subject to a civil penalty of $5,000 for a first offense, $10,000 for a second offense, and $15,000 for a third or subsequent offense. The civil penalty prescribed in this subsection shall be collected and enforced by summary proceedings pursuant to the provisions of the “Penalty Enforcement Law of 1999,” P.L.1999, c.274 (C.2A:58-10 et seq.).</u>

(cf: P.L.2005, c.226, s.12)

2. Section 15 of P.L.2005, c.226 (C.56:8-166) is amended to read as follows:

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] and 11 of P.L.2005, c.226 (C.56:8-161 and C.56:8-162), and section 13 of P.L.2005, c.226 (C.56:8-164) [this amendatory and supplementary act].
(cf: P.L.2005, c.226, s.15)

3. This act shall take effect immediately.

STATEMENT

This bill revises the penalties imposed on a business or public entity that maintains personal information within a computer network and fails to report a breach of those computerized records to customers and to the New Jersey State Police.

Under current law, any business or public entity operating in New Jersey that compiles or maintains computerized records that include personal information is required to report a breach of security of computerized records to every affected customer who is a resident of this State. Businesses are also required to report this information to the New Jersey State Police.

A failure to report this breach of security is an unlawful practice under the Consumer Fraud Act. An unlawful practice under the Consumer Fraud Act is punishable by a monetary penalty of not more than $10,000 for a first offense and not more than $20,000 for any subsequent offense. In addition, violations can result in cease and desist orders issued by the Attorney General, the assessment of punitive damages and the awarding of treble damages and costs to the injured party.

This bill revises the current monetary penalties by establishing a defined monetary fine, and then increasing that fine based on the number of offenses committed by a business or public entity. Under the bill, for or a first offense of failing to report a data security breach a business or public entity would be required to pay $5,000, for a second offense $10,000, and for a third offense or subsequent offense $15,000.