ASSEMBLY, No. 2048
STATE OF NEW JERSEY
211th LEGISLATURE

INTRODUCED FEBRUARY 5, 2004

Sponsored by:
Assemblyman UPENDRA J. CHIVUKULA
District 17 (Middlesex and Somerset)

SYNOPSIS

Requires businesses to disclose any breach of security of computer systems to customers and to destroy certain personal information no longer retained.

CURRENT VERSION OF TEXT

As introduced.

AN ACT concerning the security of personal information retained by businesses.

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

1. As used in this act:

"Breach of the security of the system" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a business. Good faith acquisition of personal information by an employee or agent of the business for the purposes of the business is not a breach of the security of the system, provided that the

personal information is not used or subject to further unauthorized disclosure.

"Business" means a sole proprietorship, partnership, corporation, association, or other group, 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.

"Customer" means an individual who provides personal information to a business for the purpose of purchasing or leasing a product or obtaining a service from the business.

"Individual" means a natural person.

"Personal information" means any information that identifies, relates to, describes, or is capable of being associated with, a particular individual, including, but not limited to, his name, signature, social security number, physical characteristics or description, address, telephone number, passport number, driver's license or non-driver identification card number, insurance policy number, education, employment history, bank account number, credit card number, debit card number, or any other financial information.

"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. A business shall take all reasonable steps to 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, by shredding, erasing, or otherwise modifying the personal information in those records to make it unreadable or undecipherable through any means.

3. a. Any business that conducts business in New Jersey, and that owns or licenses computerized data that includes personal information, shall disclose any breach of the security of the system within 15 days following discovery or notification of the breach in the security of the data to any customer who is a resident of New Jersey whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The

disclosure shall be 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.

b. Any business that maintains computerized data that includes personal information that the business does not own shall notify the owner or licensee of the information of any breach of the security of the system immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

c. The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation and shall be made after the law enforcement agency determines that its disclosure will not compromise the investigation.

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 15 U.S.C. § 7001; or

(3) Substitute notice, if the business 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 does not have sufficient contact information. Substitute notice shall consist of all of the following:

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

(b) Conspicuous posting of the notice on the Web site page of the business, if the business maintains one; and

(c) Notification to major statewide media.

e. Notwithstanding subsection d. of this section, a business 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 timing requirements of this section, shall be deemed to be in compliance with the notification requirements of this section if the business notifies subject customers in accordance with its policies in the event of a breach of security of the system.

4. A violation of any provisions of this act shall be an unlawful practice subject to the penalties applicable pursuant to section 1 of P.L.1966, c.39 (C.56:8-13).

5. This act shall take effect on the 120th day following enactment.

STATEMENT

This bill requires a business to take all reasonable steps to destroy customer records within its control containing personal information which is no longer to be retained by the business. The customer records shall be destroyed by shredding, erasing, or otherwise modifying the personal information to make them unreadable or undecipherable through any means.

In addition, any business that conducts business in New Jersey and owns or licenses computerized data that includes personal information must disclose any breach of the security of the computer system within 15 days to any customer who is a resident of New Jersey whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. However, the disclosure may be delayed if a law enforcement agency determines that notification will impede a criminal investigation.

Any business that maintains computerized data that includes personal information that the business does not own shall notify the owner or licensee of the information of any breach of the security of the system immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

For purposes of this bill, notice may be written or electronic. If the business 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 does not have sufficient contact information, it may provide substitute notice, which must consist of all of the following: (1) e-mail notice when the business has an e-mail address; (2) conspicuous posting of the notice on the Web site page of the business, if the business maintains one; and (3) notification to major Statewide media. However, a business 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 timing requirements of the bill, shall be deemed to be in compliance with the notification requirements of this bill if the business notifies subject persons in accordance with its policies in the event of a breach of security of the system.

Finally, a violation of any provisions of this bill shall be an unlawful practice subject to the penalties applicable to a violation of the consumer fraud law pursuant to N.J.S.A. 56:8-13. Under N.J.S.A. 56:8-13, any business who violates any of the provisions of this bill, in addition to any other penalty provided by law, shall be liable to a penalty of not more that $10,000 for the first offense and not more than $20,000 for the second and each subsequent offense.