SENATE, No. 1223

STATE OF NEW JERSEY

219th LEGISLATURE

INTRODUCED FEBRUARY 3, 2020

Sponsored by:
Senator SHIRLEY K. TURNER
District 15 (Hunterdon and Mercer)

SYNOPSIS

Prohibits retail sales establishment from storing certain magnetic-stripe data; requires reimbursement for costs incurred by financial institution due to breach of security.

CURRENT VERSION OF TEXT

As introduced.

AN ACT concerning the security of certain financial information and amending P.L.2002, c.101 and P.L.2005, c.226.

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

1. Section 1 of P.L.2002, c.101 (C.56:11-42) is amended to read as follows:

1. a. No retail sales establishment shall print electronically more than the last five digits of a customer's credit card account number or the expiration date of that credit card upon any sales receipt provided at the point of sale to the customer, except that the provisions of this section shall not apply to any sales receipt in which the sole means of recording the customer's credit card number is by handwriting or by an imprint or copy of the credit card.

b. No retail sales establishment shall retain or store full magnetic-stripe data, including Visa Card Verification Value 2 or MasterCard Card Validation Code 2, obtained from a credit card, debit card, or access device on any system components after a response to the retail sales establishment's authorization request has been received.

c. Notwithstanding the provisions of subsection b. of this section, a retail sales establishment may retain the account number, expiration date, and name contained on the credit card.

d. For purposes of this section:

"Access device" means a card, code, or other means of access to a consumer's account, or any combination thereof, that may be used by the consumer for the purpose of initiating electronic fund transfers.

"Credit card" means any instrument or device, whether known as a credit card, credit plate, or by any other name, issued with or without fee by an issuer for the use of the credit card holder in obtaining money, goods, services, or anything else of value on credit.

"Debit card" means any instrument or device, whether known as a debit card, automated teller machine card, or by any other name, issued with or without fee by an issuer for the use of the cardholder in obtaining money, goods, services, or anything else of value through the electronic authorization of a financial institution to debit the cardholder's account.

"Magnetic-stripe data" means data encoded on the magnetic-stripe on a credit or debit card.

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.

"System components" means any network component, server, or application that is included in or connected to credit card or debit card data.

"Visa Card Verification Value 2" and "MasterCard Card Validation Code 2" means a unique three-digit code imprinted on the signature panel of the Visa and MasterCard credit or debit cards.

(cf: P.L.2002, c.101, s.1)

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

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.

"Financial institution" means a bank, savings bank, savings and loan association, mutual savings bank, or credit union 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. The term also includes any person who issues an access device as defined in section 1 of P.L.2002, c.101 (C.56:11-42) and agrees with a customer to provide electronic fund transfer services.

"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.

(cf: P.L.2019, c.95, s.1)

3. 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 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**]** that 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.

h. A business or public entity that is required to provide notice to a customer pursuant to subsection a. or b. of this section shall be liable to a financial institution for the costs incurred by that financial institution in protecting the personal information of a customer or providing financial services to that customer as a result of a potential or actual breach of security of the computerized records of the business or public entity, including, but not limited to:

(1) The cancellation or re-issuance by any financial institution of any credit card, debit card, or access device, as those terms are defined in section 1 of P.L.2002, c.101 (C.56:11-42);

(2) The closure of any deposit, transaction, share draft, or other account and any action to stop payments or block transactions with respect to a customer's account;

(3) The opening or re-opening of any deposit, transaction, share draft, or other account for any customer of the financial institution; and

(4) Any refund or credit made to any customer of the financial institution as a result of a breach of security.

i. A financial institution may provide a customer with the name of the business or public entity that sustained a breach of security.

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

4. This act shall take effect immediately.

STATEMENT

This bill prohibits a retail sales establishment from retaining or storing the full magnetic-stripe data, including Visa Card Verification Value 2 or MasterCard Card Validation Code 2, obtained from a credit card, debit card, or access device on any system components after a response to the retail sales establishment's authorization request has been received. However, notwithstanding the above, a retail sales establishment may retain the account number, expiration date, and name contained on the credit card.

The bill also provides that a business or public entity that is required to provide notice of a breach of security of computerized records to a customer pursuant to subsection a. or b. of section 12 of P.L.2005, c.226 (C.56:8-163) will be liable to a financial institution for the costs incurred by that financial institution in protecting the personal information of a customer or providing financial services to that customer as a result of a potential or actual breach of security of the computerized records of the business or public entity, including, but not limited to:

(1) the cancellation or re-issuance by any financial institution of any credit card, debit card, or access device;

(2) the closure of any deposit, transaction, share draft, or other account and any action to stop payments or block transactions with respect to a customer's account;

(3) the opening or re-opening of any deposit, transaction, share draft, or other account for any customer of the financial institution; and

(4) any refund or credit made to any customer of the financial institution as a result of a breach of security.

The bill also adds a definition of "financial institution" to the "Identity Theft Prevention Act." It defines a financial institution as a bank, savings bank, savings and loan association, mutual savings bank, or credit union 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. The term also includes any person who issues an access device and agrees with a consumer to provide electronic fund transfer services.