2018 -- S 2790

========
LC004830
========

S T A T E O F R H O D E I S L A N D

IN GENERAL ASSEMBLY

JANUARY SESSION, A.D. 2018

A N A C T

RELATING TO STATE AFFAIRS AND GOVERNMENT - BREACH OF PERSONAL INFORMATION NOTIFICATION ACT

Introduced By: Senators Morgan, and Paolino

Date Introduced: April 06, 2018

Referred To: Senate Judiciary

It is enacted by the General Assembly as follows:

SECTION 1. Title 42 of the General Laws entitled "STATE AFFAIRS AND GOVERNMENT" is hereby amended by adding thereto the following chapter:

CHAPTER 127.2

BREACH OF PERSONAL INFORMATION NOTIFICATION ACT

42-127.2-1. Purpose.

The intent of the general assembly is to help ensure that the personal information of residents of this state is protected by providing procedures for notification of security breaches related to personal information and thereby encouraging individuals and commercial entities, as defined in this chapter, to provide reasonable security for unencrypted personal information.

42-127.2-2. Definitions.

As used in this chapter:

(1) "Breach of the security of a system" means the unauthorized access and acquisition of unencrypted and unredacted computerized data that compromises the security or confidentiality of personal information maintained by an individual or entity as part of a database of personal information regarding multiple individuals and that causes, or the individual or entity reasonably believes has caused, or will cause identity theft or other fraud to any resident of this state.

(i) Good faith acquisition of personal information by an employee or agent of an individual or entity for the purposes of the individual or the entity is not a breach of the security

of the system, provided that the personal information is not used for a purpose other than a lawful purpose of the individual or entity or subject to further unauthorized disclosure.

(2) "Encrypted" means transformation of data through the use of an algorithmic process into a form in which there is a low probability of assigning meaning without use of a confidential process or key, or securing the information by another method that renders the data elements unreadable or unusable.

(3) "Entity" includes corporations, business trusts, estates, partnerships, limited partnerships, limited liability partnerships, limited liability companies, associations, organizations, joint ventures, governments, governmental subdivisions, agencies, or instrumentalities, or any other legal entity, whether for profit or not-for-profit.

(4) "Financial institution" has the meaning given that term in 15 U.S.C. § 68093.

(5) "Individual" means a natural person.

(6) "Notice" means:

(i) Written notice to the postal address in the records of the individual or entity;

(ii) Telephone notice;

(iii) Electronic notice; or

(iv) Substitute notice, if the individual or the entity required to provide notice demonstrates that the cost of providing notice will exceed fifty thousand dollars ($50,000) or that the affected class of residents to be notified exceeds one hundred thousand (100,000) persons, or that the individual or the entity does not have sufficient contact information or consent to provide notice as described in subsections (i), (ii) or (iii) of this section. Substitute notice consists of any two (2) of the following:

(A) Email notice if the individual or the entity has email addresses for the members of the affected class of residents; and

(B) Conspicuous posting of the notice on the website of the individual or the entity if the individual or the commercial entity maintains a website; and

(C) Notice to major statewide media.

(7) "Personal information" means the first name or first initial and last name in combination with and linked to any one or more of the following data elements that relate to a resident of this state, when the data elements are neither encrypted nor redacted:

(i) Social security number;

(ii) Driver's license number or state identification card number issued in lieu of a driver's license; or

(iii) Financial account number, or credit card or debit card number, in combination with

any required security code, access code, or password that would permit access to a resident's financial accounts.

(iv) The term does not include information that is lawfully obtained from publicly available information, or from federal, state, or local government records lawfully made available to the general public.

(8) "Redact" means alteration or truncation of data such that no more than the following are accessible as part of the personal information;

(i) Five (5) digits of a social security number; or

(ii) The last four (4) digits of a driver's license number, state identification card number or account number.

42-127.2-3. Disclosure of breach of security of computerized personal information by an individual or entity.

(a) General rule. An individual or entity that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system following discovery or notification of the breach of the security of the system to any resident of this state whose unencrypted and unredacted personal information was or is reasonably believed to have been accessed and acquired by an unauthorized person and that causes, or the individual or entity reasonably believes has caused or will cause, identity, theft or other fraud to any resident of this state. Except as provided in subsection (d) of this section or in order to take any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the system, the disclosure shall be made without unreasonable delay.

(b) Encrypted information. An individual or entity must disclose the breach of the security of the system if encrypted information is accessed and acquired in an unencrypted form, or if the security breach involves a person with access to the encryption key and the individual or entity reasonably believes that such breach has caused or will cause identity theft or other fraud to any resident of this state.

(c) An individual or entity that maintains computerized data that includes personal information that the individual or entity does not own or license shall notify the owner or licensee of the information of any breach of the security of the system as soon as practicable following discovery, if the personal information was or the entity reasonably believes was accessed and acquired by an unauthorized person.

(d) Notice required by this section may be delayed if a law enforcement agency determines and advises the individual or entity that the notice will impede a criminal or civil investigation, or homeland or national security. Notice required by this section must be made

without unreasonable delay after the law enforcement agency determines that notification will no longer impede the investigation or jeopardize national or homeland security.

42-127.2-4. Procedures deemed in compliance with security breach requirements.

(a) Information privacy or security policy. An entity that maintains its own notification procedures as part of an information privacy or security policy for the treatment of personal information and that are consistent with the timing requirements of this chapter shall be deemed to be in compliance with the notification requirements of this chapter if it notifies residents of this state in accordance with its procedures in the event of a breach of security of the system.

(b) Compliance with federal requirements.

(1) A financial institution that complies with the notification requirements prescribed by the federal interagency guidance on response programs for unauthorized access to customer information and customer notice is deemed to be in compliance with this chapter.

(2) An entity that complies with the notification requirements or procedures pursuant to the rules, regulation, procedures, or guidelines established by the entity's primary or functional federal regulator shall be in compliance with this chapter.

42-127.2-5. Violations.

(a) A violation of this chapter that results in injury or loss to residents of this state may be enforced by the office of the attorney general as an unfair trade practice pursuant to chapter 13.1 of title 6.

(b) Except as provided by subsection (c) of this section, the office of the attorney general shall have exclusive authority to bring action and may obtain either actual damages for a violation of this chapter or a civil penalty not to exceed one hundred fifty thousand dollars ($150,000) per breach of the security of the system or series of breaches of a similar nature that are discovered in a single investigation.

(c) A violation of this chapter by a state-chartered or licensed financial institution shall be enforceable exclusively by the financial institutions' primary state regulator.

42-127.2-6. Applicability.

This chapter shall apply to the discovery or notification of a breach of the security of the system that occurs on or after the effective date of this chapter.

42-127.2-7. Severability.

If any provision of this chapter or its application to any person or circumstance is held invalid, the invalidity does not affect other provisions or applications of this chapter which can be given effect without the invalid provision or application, and to this end the provisions of this chapter are severable.

SECTION 2. This act shall take effect on July 1, 2018.

========
LC004830
========

EXPLANATION

BY THE LEGISLATIVE COUNCIL

OF

A N A C T

RELATING TO STATE AFFAIRS AND GOVERNMENT - BREACH OF PERSONAL INFORMATION NOTIFICATION ACT

***

This act would establish procedures to notify individuals of any breaches of their unencrypted personal information and penalties for any violation.

This act would take effect on July 1, 2018.

========
LC004830
========