2022 -- H 7883

========
LC004811
========

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. 2022

_____

A N A C T

RELATING TO CRIMINAL OFFENSES -- IDENTITY THEFT PROTECTION ACT OF 2015

Introduced By: Representatives Ruggiero, Craven, Hull, Williams, Morales, Ajello, Carson, Cortvriend, Slater, and Baginski
Date Introduced: March 04, 2022

Referred To: House Innovation, Internet, & Technology

It is enacted by the General Assembly as follows:

SECTION 1. Chapter 11-49.3 of the General Laws entitled "Identity Theft Protection Act of 2015" is hereby amended by adding thereto the following section:

11-49.3-7. Cybersecurity incident response group.

(a) The governor shall establish a cybersecurity incident response group, which shall include the superintendent of the Rhode Island state police, or designee, adjutant general of the Rhode Island national guard, or designee, director of the Rhode Island division of information technology, or designee, director of the Rhode Island emergency management agency, or designee and the secretary of state, or designee.

(b) The cybersecurity incident response group shall:

(1) Establish communication protocols in the event of a breach or an incident of cybersecurity in any agency or public body. The protocols shall include, but not be limited to:

(i) A list of potential cybersecurity breaches or incidents that would require reporting;

(ii) State and local entities covered within the communication plan;

(iii) Mechanisms to communicate a cybersecurity breach or incidents in a timely manner to members of the public and other relevant parties who may be affected by the breach; and

(iv) Primary contact at each agency or public body.

(c) The cybersecurity incident response group shall also establish long-term policy planning and goals for the state regarding evolving cybersecurity threats and how to address them in a coordinated manner.

(d) The cybersecurity incident response group shall be subject to chapter 46 of title 42, ("open meetings"), and chapter 2 of title 38, ("access to public records").

SECTION 2. Sections 11-49.3-3 and 11-49.3-4 of the General Laws in Chapter 11-49.3 entitled "Identity Theft Protection Act of 2015" is hereby amended to read as follows:

11-49.3-3. Definitions.

(a) The following definitions apply to this section:

(1) "Breach of the security of the system" means unauthorized access or acquisition of unencrypted, computerized data information that compromises the security, confidentiality, or integrity of personal information maintained by the municipal agency, state agency, or person. Good-faith acquisition of personal information by an employee or agent of the agency for the purposes of the agency is not a breach of the security of the system; provided, that the personal information is not used or subject to further unauthorized disclosure.

(2) "Encrypted" means the transformation of data through the use of a one hundred twenty-eight (128) bit or higher algorithmic process into a form in which there is a low probability of assigning meaning without use of a confidential process or key. Data shall not be considered to be encrypted if it is acquired in combination with any key, security code, or password that would permit access to the encrypted data.

(3) "Health insurance information" means an individual's health insurance policy number, subscriber identification number, or any unique identifier used by a health insurer to identify the individual.

(4) "Incident" means any action taken through the use of an information system or network that results in an actual or potentially adverse effect on an information system, network, and/or the information residing therein.

~~(4)~~(5) "Medical information" means any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a healthcare professional or provider.

~~(5)~~(6) "Municipal agency" means any department, division, agency, commission, board, office, bureau, authority, quasi-public authority, or school, fire, or water district within Rhode Island, other than a state agency, and any other agency that is in any branch of municipal government and exercises governmental functions other than in an advisory nature.

~~(6)~~(7) "Owner" means the original collector of the information.

~~(7)~~(8) "Person" shall include any individual, sole proprietorship, partnership, association, corporation, joint venture, business, legal entity, trust, estate, cooperative, or other commercial entity.

~~(8)~~(9) "Personal information" means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when the name and the data elements are not encrypted or are in hard copy, paper format:

(i) Social security number;

(ii) Driver's license number, Rhode Island identification card number, or tribal identification number;

(iii) Account number, credit, or debit card number, in combination with any required security code, access code, password, or personal identification number, that would permit access to an individual's financial account;

(iv) Medical or health insurance information; or

(v) E-mail address with any required security code, access code, or password that would permit access to an individual's personal, medical, insurance, or financial account.

~~(9)~~(10) "Remediation service provider" means any person who or that, in the usual course of business, provides services pertaining to a consumer credit report including, but not limited to, credit report monitoring and alerts, that are intended to mitigate the potential for identity theft.

~~(10)~~(11) "State agency" means any department, division, agency, commission, board, office, bureau, authority, or quasi-public authority within Rhode Island; either branch of the Rhode Island general assembly or an agency or committee thereof; the judiciary; or any other agency that is in any branch of Rhode Island state government and that exercises governmental functions other than in an advisory nature.

(b) For purposes of this section, personal information does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

(c) For purposes of this section, "notice" may be provided by one of the following methods:

(i) Written notice;

(ii) 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

(iii) Substitute notice, if the municipal agency, state agency, or person demonstrates that the cost of providing notice would exceed twenty-five thousand dollars ($25,000), or that the affected class of subject persons to be notified exceeds fifty thousand (50,000), or the municipal agency, state agency, or person does not have sufficient contact information. Substitute notice shall consist of all of the following:

(A) E-mail notice when the municipal agency, state agency, or person has an e-mail address for the subject persons;

(B) Conspicuous posting of the notice on the municipal agency's, state agency's or person's website page, if the municipal agency, state agency, or person maintains one; and

(C) Notification to major statewide media.

11-49.3-4. Notification of breach.

(a)(1) Any municipal agency, state agency, or person that stores, owns, collects, processes, maintains, acquires, uses, or licenses data that includes personal information shall provide notification as set forth in this section of any disclosure of personal information, or any breach of the security of the system, that poses a significant risk of identity theft to any resident of Rhode Island whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person or entity.

(2) ~~The notification shall be made in the most expedient time possible, but no later than forty-five (45) calendar days after confirmation of the breach and the ability to ascertain the information required to fulfill the notice requirements contained in subsection (d) of this section, and shall be consistent with the legitimate needs of law enforcement as provided in subsection (c) of this section. In the event that more than five hundred (500) Rhode Island residents are to be notified, the municipal agency, state agency, or person shall notify the attorney general and the major credit reporting agencies as to the timing, content, and distribution of the notices and the approximate number of affected individuals. Notification to the attorney general and the major credit reporting agencies shall be made without delaying notice to affected Rhode Island residents.~~

(2) An initial notification shall be made in the most expedient time possible, but no later than twenty-four (24) hours after confirmation of a cybersecurity incident or breach, to the cybersecurity incident response group and the attorney general. Notification requirements contained in subsection (d) of this section shall be made no later than fifteen (15) calendar days after confirmation of a cybersecurity incident or breach. In all notification requirements, the municipal agency, state agency, or person shall notify the attorney general and the major credit reporting agencies as to the timing, content, and distribution of the notices and the approximate number of affected individuals. Notification to the attorney general and the major credit reporting agencies shall be made without delaying notice to affected Rhode Island residents.

(3) A secondary notification shall be made to the cybersecurity incident response group and the attorney general which includes the full details of the agency's informational technology security and operational requirements employed to protect the agency's data, including, but not limited to, documentation and reporting of remedial or corrective action plans to address any deficiencies in the information security policies, procedures, and practices of the agency.

(b) The notification required by this section may be delayed if a federal, state, or local law

enforcement agency determines that the notification will impede a criminal investigation. The federal, state, or local law enforcement agency must notify the municipal agency, state agency, or person of the request to delay notification without unreasonable delay. If notice is delayed due to such determination, then, as soon as the federal, state, or municipal law enforcement agency determines and informs the municipal agency, state agency, or person that notification no longer poses a risk of impeding an investigation, notice shall be provided as soon as practicable pursuant to subsection (a)(2). The municipal agency, state agency, or person shall cooperate with federal, state, or municipal law enforcement in its investigation of any breach of security or unauthorized acquisition or use, which shall include the sharing of information relevant to the incident; provided however, that such disclosure shall not require the disclosure of confidential business information or trade secrets.

(c) Any municipal agency, state agency, or person required to make notification under this section and fails to do so is liable for a violation as set forth in § 11-49.3-5.

(d) The notification to individuals must include the following information to the extent known:

(1) A general and brief description of the incident, including how the security breach occurred and the number of affected individuals;

(2) The type of information that was subject to the breach;

(3) Date of breach, estimated date of breach, or the date range within which the breach occurred;

(4) Date that the breach was discovered;

(5) A clear and concise description of any remediation services offered to affected individuals including toll free numbers and websites to contact: (i) The credit reporting agencies; (ii) Remediation service providers; (iii) The attorney general; and

(6) A clear and concise description of the consumer's ability to file or obtain a police report; how a consumer requests a security freeze and the necessary information to be provided when requesting the security freeze; and that fees may be required to be paid to the consumer reporting agencies.

SECTION 3. This act shall take effect upon passage.

========
LC004811
========

EXPLANATION

BY THE LEGISLATIVE COUNCIL

OF

A N A C T

RELATING TO CRIMINAL OFFENSES -- IDENTITY THEFT PROTECTION ACT OF 2015

***

This act would create a cybersecurity incident response group that would promulgate cybersecurity breach related protocols for agencies and public bodies, require immediate notice of a breach within twenty-four (24) hours to the cybersecurity incident response group and the attorney general, and notice to the affected individuals no later than fifteen (15) days after the discovery of the breach.

This act would take effect upon passage.

========
LC004811
========