2015 R.I. HB 5220

Enacted, July 2, 2015

Reporter
2015 R.I. ALS 148; 2015 R.I. Pub. Laws 148; 2015 R.I. Pub. Ch. 148; 2015 R.I. HB 5220

RHODE ISLAND ADVANCE LEGISLATIVE SERVICE > RHODE ISLAND 2015-2016 LEGISLATIVE SESSION > PUBLIC LAWS CHAPTER 148 > HOUSE BILL 5220 (SUBSTITUTE A)

Notice

Added: Text highlighted in green
Deleted: ~~Red text with a strikethrough~~

Synopsis

AN ACT RELATING TO CRIMINAL OFFENSES - IDENTITY THEFT PROTECTION

Text

It is enacted by the General Assembly as follows:

SECTION 1. Chapter 11-49.2 of the General Laws entitled "Identity Theft Protection" is hereby repealed in its entirety.

~~CHAPTER 11-49.2~~

~~Identity Theft Protection~~

~~11-49.2-1. Short title. -- This chapter shall be known and may be cited as the "Rhode Island Identity Theft Protection Act of 2005."~~

~~11-49.2-2. Legislative findings. -- It is hereby found and declared as follows:~~

~~(1) There is a growing concern regarding the possible theft of an individual's identity and a resulting need for measures to protect the privacy of personal information. It is the intent of the general assembly to ensure that personal information about Rhode Island residents is protected. To that end, the purpose of this chapter is to require businesses that own or license personal information about Rhode Islanders to provide reasonable security for that information. For the purpose of this chapter, the phrase "owns or licenses" is intended to include, but is not limited to, personal information that a business retains as part of the business' internal customer account or for the purpose of using that information in transactions with the person to whom the information relates.~~

~~(2) A business that owns or licenses computerized unencripted personal information about a Rhode Island resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure.~~

~~(3) A business that discloses computerized unencripted personal information about a Rhode Island resident pursuant to a contract with a nonaffiliated third-party shall require by contract that the third-party implement and~~

maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure.

11-49.2-3. Notification of breach. --

(a) Any state agency or person that owns, maintains or licenses computerized data that includes personal information, shall disclose any breach of the security of the system which poses a significant risk of identity theft following discovery or notification of the breach in the security of the data to any resident of Rhode Island whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person or a person without authority, to acquire said information. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

(b) Any state agency or person that maintains computerized unencripted data that includes personal information that the state agency or person does not own shall notify the owner or licensee of the information of any breach of the security of the data which poses a significant risk of identity theft 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. The notification required by this section shall be made after the law enforcement agency determines that it will not compromise the investigation.

(d) The notification must be prompt and reasonable following the determination of the breach unless otherwise provided in this section. Any state agency or person required to make notification under this section and who fails to do so promptly following the determination of a breach or receipt of notice from law enforcement as provided for is subsection (c) is liable for a fine as set forth in Section 11-49.2-6.

11-49.2-4. Notification of breach -- Consultation with law enforcement.

-- Notification of a breach is not required if, after an appropriate

investigation or after consultation with relevant federal, state, or local law

enforcement agencies, a determination is made that the breach has not and will

not likely result in a significant risk of identity theft to the individuals

whose personal information has been acquired.

11-49.2-5. Definitions. -- The following definitions apply to this section:

(a) "Person" shall include any individual, partnership association, corporation or joint venture.

(b) For purposes for this section, "breach of the security of the system" means unauthorized acquisition of unencrypted computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the 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.

(c) For purposes of this section, "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 either the name or the data elements are not encrypted:

(1) Social security number;

(2) Driver's license number or Rhode Island Identification Card number;

~~(3) Account number, 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.~~

~~(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 for the in Section 7001 of Title 15 of the United States Code;~~

~~(3) Substitute notice, if the 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 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 state agency or person has an e-mail address for the subject persons;~~

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

~~(C) Notification to major statewide media.~~

~~11-49.2-6. Penalties for violation. --~~

~~(a) Each violation of this chapter is a civil violation for which a penalty of not more than a hundred dollars ($ 100) per occurrence and not more than twenty-five thousand dollars ($ 25,000) may be adjudged against a defendant.~~

~~(b) No Waiver of Notification. - Any waiver of a provision of this section is contrary to public policy and is void and unenforceable.~~

~~11-49.2-7. Agencies with security breach procedures. -- Any state agency or person that maintains its own security breach procedures as part of an information security policy for the treatment of personal information and otherwise complies with the timing requirements of Section 11- 49.2-3, shall be deemed to be in compliance with the security breach notification requirements of Section 11-49.2-3, provided such person notifies subject persons in accordance with such person's policies in the event of a breach of security. Any person that maintains such a security breach procedure pursuant to the rules, regulations, procedures or guidelines established by the primary or functional regulator, as defined in *15 USC 6809*(2), shall be deemed to be in compliance with the security breach notification requirements of this section, provided such person notifies subject persons in accordance with the policies or the rules, regulations, procedures or guidelines established by the primary or functional regulator in the event of a breach of security of the system. A financial institution, trust company, credit union or its affiliates that is subject to and examined for, and found in compliance with the Federal Interagency Guidelines on Response Programs for Unauthorized Access to Customer Information and Customer Notice shall be deemed in compliance with this chapter. A provider of health care, health care service plan, health insurer, or a covered entity governed by the medical privacy and security rules issued by the federal Department of Health and Human Services, Parts 160 and 164 of Title 45 of the Code of Federal Regulations, established pursuant to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) shall be deemed in compliance with this chapter.~~

SECTION 2. Title 11 of the General Laws entitled "CRIMINAL OFFENSES" is hereby amended by adding thereto the following chapter:

CHAPTER 49.3

IDENTITY THEFT PROTECTION ACT OF 2015

11-49.3-1. Short title. --

This chapter shall be known and may be cited as the "Rhode Island Identity Theft Protection Act of 2015."

11-49.3-2. Risk-based information security program. --

(a) A municipal agency, state agency or person that stores, collects, processes, maintains, acquires, uses, owns or licenses personal information about a Rhode Island resident shall implement and maintain a risk-based information security program which contains reasonable security procedures and practices appropriate to the size and scope of the organization, the nature of the information and the purpose for which the information was collected in order to protect the personal information from unauthorized access, use, modification, destruction or disclosure and to preserve the confidentiality, integrity, and availability of such information. A municipal agency, state agency or person shall not retain personal information for a period longer than is reasonably required to provide the services requested, to meet the purpose for which it was collected, or in accordance with a written retention policy or as may be required by law. A municipal agency, state agency or person shall destroy all personal information, regardless of the medium that such information is in, in a secure manner, including, but not limited to, shredding, pulverization, incineration, or erasure.

(b) A municipal agency, state agency or person that discloses personal information about a Rhode Island resident to a nonaffiliated third party shall require by written contract that the third party implement and maintain reasonable security procedures and practices appropriate to the size and scope of the organization, the nature of the information and the purpose for which the information was collected in order to protect the personal information from unauthorized access, use, modification, destruction, or disclosure. The provisions of this section shall apply to contracts entered into after the effective date of this act.

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 or subscriber identification number, any unique identifier used by a health insurer to identify the individual.

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

(5) "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) "Owner" means the original collector of the information.

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

(8) "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, or 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) "Remediation service provider" means any person which in its 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) "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 which 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. Section 7001;*

(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, which 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.

(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 Section 11-49.3-4(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 who fails to do so is liable for a violation as set forth in Section 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.

11-49.3-5. Penalties for violation. --

(a) Each reckless violation of this chapter is a civil violation for which a penalty of not more than one hundred dollars ($ 100) per record may be adjudged against a defendant.

(b) Each knowing and willful violation of this chapter is a civil violation for which a penalty of not more than two hundred dollars ($ 200) per record may be adjudged against a defendant.

(c) Whenever the attorney general has reason to believe that a violation of this chapter has occurred and that proceedings would be in the public interest, the attorney general may bring an action in the name of the state against the business or person in violation.

11-49.3-6. Agencies or persons with security breach procedures. --

(a) Any municipal agency, state agency or person shall be deemed to be in compliance with the security breach notification requirements of Section 11-49.3-4, if:

(1) The municipal agency, state agency or person maintains its own security breach procedures as part of an information security policy for the treatment of personal information and otherwise complies with the timing requirements of Section 11-49.3-4, and notifies subject persons in accordance with such municipal agency's, state agency's, or person's notification policies in the event of a breach of security; or

(2) The person maintains a security breach procedure pursuant to the rules, regulations, procedures or guidelines established by the primary or functional regulator, as defined in *15 U.S.C. Section 6809*(2), and notifies subject persons in accordance with the policies or the rules, regulations, procedures or guidelines established by the primary or functional regulator in the event of a breach of security of the system.

(b) A financial institution, trust company, credit union or its affiliates that is subject to and examined for, and found in compliance with the Federal Interagency Guidelines on Response Programs for Unauthorized Access to Customer Information and Customer Notice shall be deemed in compliance with this chapter.

(c) A provider of health care, health care service plan, health insurer, or a covered entity governed by the medical privacy and security rules issued by the Federal Department of Health and Human Services, Parts 160 and 164 of Title 45 of the Code of Federal Regulations, established pursuant to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) shall be deemed in compliance with this chapter.

SECTION 3. This act shall take effect one year following the date of passage.

History

Approved by the Governor July 2, 2015

Date Introduced: January 29, 2015

Sponsor

Representatives Ucci, Nardolillo, Regunberg, Winfield, and Corvese