

General Laws of Rhode Island

Title 11 – Criminal Offenses

Chapter 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 unencrypted 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 unencrypted 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 unencrypted 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 in subsection (c) is liable for a fine as set forth in § 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 § 11-49.2-3, shall be deemed to be in compliance with the security breach notification requirements of § 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.