

=====

LC000486

=====

JANUARY SESSION, A.D. 2015

RELATING TO CRIMINAL OFFENSES - IDENTITY THEFT PROTECTION

Referred To: Senate Judiciary

~~(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~~

1 ~~unauthorized access, destruction, use, modification, or disclosure.~~

2 ~~(3) A business that discloses computerized unencrypted personal information about a~~
3 ~~Rhode Island resident pursuant to a contract with a nonaffiliated third party shall require by~~
4 ~~contract that the third party implement and maintain reasonable security procedures and practices~~
5 ~~appropriate to the nature of the information, to protect the personal information from~~
6 ~~unauthorized access, destruction, use, modification, or disclosure.~~

7 ~~**11-49.2-3. Notification of breach.**~~ (a) Any state agency or person that owns, maintains
8 ~~or licenses computerized data that includes personal information, shall disclose any breach of the~~
9 ~~security of the system which poses a significant risk of identity theft following discovery or~~
10 ~~notification of the breach in the security of the data to any resident of Rhode Island whose~~
11 ~~unencrypted personal information was, or is reasonably believed to have been, acquired by an~~
12 ~~unauthorized person or a person without authority, to acquire said information. The disclosure~~
13 ~~shall be made in the most expedient time possible and without unreasonable delay, consistent~~
14 ~~with the legitimate needs of law enforcement, as provided in subdivision (c), or any measures~~
15 ~~necessary to determine the scope of the breach and restore the reasonable integrity of the data~~
16 ~~system.~~

17 ~~(b) Any state agency or person that maintains computerized unencrypted data that~~
18 ~~includes personal information that the state agency or person does not own shall notify the owner~~
19 ~~or licensee of the information of any breach of the security of the data which poses a significant~~
20 ~~risk of identity theft immediately, following discovery, if the personal information was, or is~~
21 ~~reasonably believed to have been, acquired by an unauthorized person.~~

22 ~~(c) The notification required by this section may be delayed if a law enforcement agency~~
23 ~~determines that the notification will impede a criminal investigation. The notification required by~~
24 ~~this section shall be made after the law enforcement agency determines that it will not~~
25 ~~compromise the investigation.~~

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

31 ~~**11-49.2-4. Notification of breach — Consultation with law enforcement.**~~
32 ~~Notification of a breach is not required if, after an appropriate investigation or after consultation~~
33 ~~with relevant federal, state, or local law enforcement agencies, a determination is made that the~~
34 ~~breach has not and will not likely result in a significant risk of identity theft to the individuals~~

1 ~~whose personal information has been acquired.~~

2 ~~**11-49.2 5. Definitions.**~~ The following definitions apply to this section:

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

5 ~~-(b) For purposes for this section, "breach of the security of the system" means~~
6 ~~unauthorized acquisition of unencrypted computerized data that compromises the security,~~
7 ~~confidentiality, or integrity of personal information maintained by the state agency or person.~~
8 ~~Good faith acquisition of personal information by an employee or agent of the agency for the~~
9 ~~purposes of the agency is not a breach of the security of the system; provided, that the personal~~
10 ~~information is not used or subject to further unauthorized disclosure.~~

11 ~~-(c) For purposes of this section, "personal information" means an individual's first name~~
12 ~~or first initial and last name in combination with any one or more of the following data elements,~~
13 ~~when either the name or the data elements are not encrypted:~~

14 ~~-(1) Social security number;~~

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

16 ~~-(3) Account number, credit or debit card number, in combination with any required~~
17 ~~security code, access code, or password that would permit access to an individual's financial~~
18 ~~account.~~

19 ~~-(d) For purposes of this section, "notice" may be provided by one of the following~~
20 ~~methods:~~

21 ~~-(1) Written notice;~~

22 ~~-(2) Electronic notice, if the notice provided is consistent with the provisions regarding~~
23 ~~electronic records and signatures set for the in Section 7001 of Title 15 of the United States Code;~~

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

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

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

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

33 ~~**11-49.2 6. Penalties for violation.**~~ (a) Each violation of this chapter is a civil violation
34 ~~for which a penalty of not more than a hundred dollars (\$100) per occurrence and not more than~~

1 ~~twenty-five thousand dollars (\$25,000) may be adjudged against a defendant.~~

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

4 ~~**11-49.2-7. Agencies with security breach procedures. —** Any state agency or person~~
5 ~~that maintains its own security breach procedures as part of an information security policy for the~~
6 ~~treatment of personal information and otherwise complies with the timing requirements of § 11-~~
7 ~~49.2-3, shall be deemed to be in compliance with the security breach notification requirements of~~
8 ~~§ 11-49.2-3, provided such person notifies subject persons in accordance with such person's~~
9 ~~policies in the event of a breach of security. Any person that maintains such a security breach~~
10 ~~procedure pursuant to the rules, regulations, procedures or guidelines established by the primary~~
11 ~~or functional regulator, as defined in 15 USC 6809(2), shall be deemed to be in compliance with~~
12 ~~the security breach notification requirements of this section, provided such person notifies subject~~
13 ~~persons in accordance with the policies or the rules, regulations, procedures or guidelines~~
14 ~~established by the primary or functional regulator in the event of a breach of security of the~~
15 ~~system. A financial institution, trust company, credit union or its affiliates that is subject to and~~
16 ~~examined for, and found in compliance with the Federal Interagency Guidelines on Response~~
17 ~~Programs for Unauthorized Access to Customer Information and Customer Notice shall be~~
18 ~~deemed in compliance with this chapter. A provider of health care, health care service plan,~~
19 ~~health insurer, or a covered entity governed by the medical privacy and security rules issued by~~
20 ~~the federal Department of Health and Human Services, Parts 160 and 164 of Title 45 of the Code~~
21 ~~of Federal Regulations, established pursuant to the Health Insurance Portability and~~
22 ~~Accountability Act of 1996 (HIPAA) shall be deemed in compliance with this chapter.~~

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

25 CHAPTER 49.3

26 IDENTITY THEFT PROTECTION ACT OF 2015

27 **11-49.3-1. Short title. --** This chapter shall be known and may be cited as the "Rhode
28 Island Identity Theft Protection Act of 2015."

29 **11-49.3-2. Risk-based information security program. --** (a) A municipal agency, state
30 agency or person that stores, collects, processes, maintains, acquires, uses, owns or licenses
31 personal information about a Rhode Island resident shall implement and maintain a risk-based
32 information security program which contains reasonable security procedures and practices
33 appropriate to the size and scope of the organization, the nature of the information and the
34 purpose for which the information was collected in order to protect the personal information from

1 unauthorized access, use, modification, destruction or disclosure and to preserve the
2 confidentiality, integrity, and availability of such information. A municipal agency, state agency
3 or person shall not retain personal information for a period longer than is reasonably required to
4 provide the services requested, to meet the purpose for which it was collected, or in accordance
5 with a written retention policy or as may be required by law. A municipal agency, state agency or
6 person shall destroy all personal information, regardless of the medium that such information is
7 in, in a secure manner, including, but not limited to, shredding, pulverization, incineration, or
8 erasure.

9 (b) A municipal agency, state agency or person that discloses personal information about
10 a Rhode Island resident to a nonaffiliated third party shall require by written contract that the
11 third party implement and maintain reasonable security procedures and practices appropriate to
12 the size and scope of the organization, the nature of the information and the purpose for which the
13 information was collected in order to protect the personal information from unauthorized access,
14 use, modification, destruction, or disclosure.

15 **11-49.3-3. Definitions.** -- (a) The following definitions apply to this section:

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

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

27 (3) "Health Insurance Information" means an individual's health insurance policy number
28 or subscriber identification number, any unique identifier used by a health insurer to identify the
29 individual, or any information in an individual's application and claims history, including any
30 appeals records.

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

34 (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) "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.

(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 either the name or 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 or without 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 account.

(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 for the in 15 U.S.C. §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

1 affected class of subject persons to be notified exceeds fifty thousand dollars (\$50,000), or the
2 municipal agency, state agency or person does not have sufficient contact information. Substitute
3 notice shall consist of all of the following:

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

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

8 (C) Notification to major statewide media.

9 **11-49.3-4. Notification of breach. --** (a) (1) Any municipal agency, state agency or
10 person that stores, collects, processes, maintains, acquires, uses, owns or licenses data that
11 includes personal information, shall provide notification as set forth in this section of any
12 disclosure of personal information, or any breach of the security of the system, which poses a risk
13 of identity theft to any resident of Rhode Island whose personal information was, or is reasonably
14 believed to have been, acquired by an unauthorized person or entity. A municipal agency, state
15 agency or person that owns the personal information that is subject to a breach shall notify
16 according to this subsection (a) and any municipal agency, state agency or person that stores,
17 collects, processes, maintains, acquires, licenses or uses personal information, but does not own
18 such information, shall notify as set forth in subsection (b) of this section.

19 (2) The notification shall be made in the most expedient time possible but no later than
20 fifteen (15) calendar days after discovery. In the event that any Rhode Island residents are to be
21 notified, the municipal agency, state agency or person shall notify the attorney general and the
22 major credit reporting agencies as to the timing, content and distribution of the notices and the
23 approximate number of affected individuals. Notification to the attorney general and the major
24 credit reporting agencies shall be made without delaying notice to affected Rhode Island
25 residents.

26 (b) Any municipal agency, state agency or person that stores, collects, processes,
27 maintains, acquires, uses, licenses, provides services using, or has access to personal information
28 about Rhode Island residents that the municipal agency, state agency or person does not own shall
29 notify and cooperate fully with the owner of the information of any breach of the security of the
30 data which poses a risk of identity theft immediately following discovery, if the personal
31 information was, or is reasonably believed to have been, acquired by an unauthorized person.

32 (c) The notification required by this section may be delayed if a federal, state or local law
33 enforcement agency determines that the notification will impede a criminal investigation. The
34 federal, state or local law enforcement agency must notify the municipal agency, state agency or

1 person of the request to delay notification without unreasonable delay. If notice is delayed due to
2 such determination then as soon as the federal, state or municipal law enforcement agency
3 determines and informs the municipal agency, state agency or person that notification no longer
4 poses a risk of impeding an investigation, notice shall be provided, as soon as practicable and
5 without unreasonable delay but no later than fifteen (15) calendar days after the law enforcement
6 agency determination. The municipal agency, state agency or person shall cooperate with federal,
7 state or municipal law enforcement in its investigation of any breach of security or unauthorized
8 acquisition or use, which shall include the sharing of information relevant to the incident;
9 provided however, that such disclosure shall not require the disclosure of confidential business
10 information or trade secrets.

11 (d) The notification must be prompt and reasonable following the determination of the
12 breach unless otherwise provided in this section. Any municipal agency, state agency or person
13 required to make notification under this section and who fails to do so is liable for a violation as
14 set forth in § 11-49.3-5.

15 (e) The notification to individuals must include the following information to the extent
16 known:

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

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

20 (3) Date that the breach occurred;

21 (4) Date that the breach was discovered;

22 (5) A clear and concise description of any remediation services offered to affected
23 individuals including toll free numbers and websites to contact: (i) the credit reporting agencies;
24 (ii) remediation service providers; (iii) the Attorney General; and

25 (6) A clear and concise description of: the consumer's right to file or obtain a police
26 report; how a consumer requests a security freeze and the necessary information to be provided
27 when requesting the security freeze; and any fees required to be paid to the consumer reporting
28 agencies.

29 **11-49.3-5. Penalties for violation.** -- (a) Each reckless violation of this chapter is a civil
30 violation for which a penalty of not more than one hundred dollars (\$100) per record may be
31 adjudged against a defendant.

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

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

4 (d) Any waiver of a provision of this section is contrary to public policy and is void and
5 unenforceable.

6 **11-49.3-6. Agencies or persons with security breach procedures.** -- (a) Any municipal
7 agency, state agency or person shall be deemed to be in compliance with the security breach
8 notification requirements of § 11-49.3-4, if:

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

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

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

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

28 SECTION 3. This act shall take effect upon passage.

=====
LC000486
=====

EXPLANATION
BY THE LEGISLATIVE COUNCIL
OF
A N A C T
RELATING TO CRIMINAL OFFENSES - IDENTITY THEFT PROTECTION

- 1 This act would create the Identity Theft Protection Act of 2015, to protect personal
- 2 information from unauthorized access, use, modification, destruction or disclosure, and to
- 3 preserve the confidentiality and integrity of such information.
- 4 This act would take effect upon passage.

=====
LC000486
=====