

## **Attachment #12**

An Act Relating to Commercial Law – General Regulatory Provisions – The Data  
Security Breach Notification Act (draft 699 – Relating to Commercial Law)



2019 --

699 - Relating to Commercial Law

**STATE OF RHODE ISLAND**

**IN GENERAL ASSEMBLY**

**JANUARY SESSION, A.D. 2019**

**A N A C T**

**RELATING TO COMMERCIAL LAW -- GENERAL REGULATORY PROVISIONS -- THE  
DATA SECURITY BREACH NOTIFICATION ACT**

Introduced By:

Date Introduced:

Referred To:

It is enacted by the General Assembly as follows:

1 SECTION 1. Title 6 of the General Laws entitled "COMMERCIAL LAW - GENERAL  
2 REGULATORY PROVISIONS" is hereby amended by adding thereto the following chapter:

3 CHAPTER 48.1

4 THE DATA SECURITY BREACH NOTIFICATION ACT

5 **6-48.1-1. Short title.**

6 This chapter shall be known and may be cited as "The Data Security Breach Notification  
7 Act".

8 **6-48.1-2. Definitions.**

9 As used in this chapter:

10 (1) "Agency" means any agency, executive office, department, board, commission, bureau,  
11 division or authority of the state, or any of its branches, or of any political subdivision thereof.

12 (2) "Breach of security" means the unauthorized acquisition or unauthorized use of  
13 unencrypted data or, encrypted electronic data and the confidential process or key that is capable  
14 of compromising the security, confidentiality, or integrity of personal information, maintained by  
15 a person or agency that creates a substantial risk of identity theft or fraud against a resident of the  
16 state. A good faith but unauthorized acquisition of personal information by a person or agency, or  
17 employee or agent thereof, for the lawful purposes of such person or agency, is not a breach of  
18 security unless the personal information is used in an unauthorized manner or subject to further  
19 unauthorized disclosure.

20 (3) "Data" means any material upon which written, drawn, spoken, visual, or  
21 electromagnetic information or images are recorded or preserved, regardless of physical form or  
22 characteristics.

23 (4) "Electronic" means relating to technology having electrical, digital, magnetic, wireless,  
24 optical, electromagnetic or similar capabilities.

25 (5) "Encrypted" means the transformation of data through the use of a one hundred twenty-  
26 eight (128) bit or higher algorithmic process into a form in which there is a low probability of

1 assigning meaning without use of a confidential process or key, unless further defined by regulation  
2 of the department of business regulation.

3 (6) "Notice" shall include:

4 (i) Written notice;

5 (ii) Electronic notice, if notice provided is consistent with the provisions regarding  
6 electronic records and signatures set forth in 15 U.S.C. § 7001(c); and chapter 127.1 of title 42; or

7 (iii) Substitute notice, if the person or agency required to provide notice demonstrates that  
8 the cost of providing written notice will exceed two hundred fifty thousand dollars (\$250,000), or  
9 that the affected class of Rhode Island residents to be notified exceeds five hundred thousand  
10 (500,000) residents, or that the person or agency does not have sufficient contact information to  
11 provide notice.

12 (7) "Person" means a natural person, corporation, association, partnership or other legal  
13 entity.

14 (8) "Personal information" means a resident's first name and last name or first initial and  
15 last name in combination with any one or more of the following data elements that relate to such  
16 resident:

17 (i) Social security number;

18 (ii) Driver's license number or state-issued identification card number; or

19 (iii) Financial account number, or credit or debit card number, with or without any required  
20 security code, access code, personal identification number or password, that would permit access  
21 to a resident's financial account;

22 Provided, however, "personal information" shall not include information that is lawfully  
23 obtained from publicly available information, or from federal, state or local government records  
24 lawfully made available to the general public.

25 (9) "Substitute notice" shall consist of all of the following:

26 (i) Electronic mail notice, if the person or agency has electronic mail addresses for the

1 members of the affected class of Rhode Island residents;

2 (ii) Clear and conspicuous posting of the notice on the home page of the person or agency  
3 if the person or agency maintains a website; and

4 (iii) Publication in or broadcast through media or medium that provides notice throughout  
5 the state.

6 (b) The department of business regulation may adopt regulations, from time to time, to  
7 revise the definition of "encrypted", as used in this chapter, to reflect applicable technological  
8 advancements.

9 **6-48.1-3. Regulations.**

10 (a) The department of business regulation shall adopt regulations, relative to any person  
11 that owns or licenses personal information, about a resident of the state. Such regulations shall be  
12 designed to safeguard the personal information of residents of the state and shall be consistent with  
13 the safeguards for protection of personal information set forth in the federal regulations by which  
14 the person is regulated. The objectives of the regulations shall be to: ensure the security and  
15 confidentiality of customer information in a manner fully consistent with industry standards;  
16 protect against anticipated threats or hazards to the security or integrity of such information; and  
17 protect against unauthorized access to or use of such information that may result in substantial harm  
18 or inconvenience to any consumer. The regulations shall take into account the size, scope and type  
19 of business of the person, the amount of resources available to such person, the amount of stored  
20 data, and the need for security and confidentiality of both consumer and employee information.

21 (b) The supervisor of records, with the advice and consent of the division of enterprise  
22 technology strategy and services (ETSS) to the extent of its jurisdiction to set information  
23 technology standards under § 42-11-2.8, shall establish rules and regulations designed to safeguard  
24 the personal information of residents of the state that is owned or licensed. The rules and regulations  
25 shall be applicable to:

26 (1) Executive offices and any agencies, departments, boards, commissions and



1 instrumentalities within an executive office; and

2 (2) Any authority created by the general assembly, and the rules and regulations shall take  
3 into account the size, scope and type of services provided thereby, the amount of resources available  
4 thereto, the amount of stored data, and the need for security and confidentiality of both consumer  
5 and employee information. The objectives of the rules or regulations shall be to:

6 (i) Ensure the security and confidentiality of personal information;

7 (ii) Protect against anticipated threats; or

8 (iii) Hazards to the security or integrity of such information; and to protect against  
9 unauthorized access to or use of such information that could result in substantial harm or  
10 inconvenience to any resident of the state.

11 (c) The legislative branch, the judicial branch, the attorney general, the secretary of state,  
12 the state treasurer and the state auditor general shall adopt rules and regulations designed to  
13 safeguard the personal information of residents of the state for their respective departments and  
14 shall take into account the size, scope and type of services provided by their departments, the  
15 amount of resources available thereto, the amount of stored data, and the need for security and  
16 confidentiality of both consumer and employee information. The objectives of the rules and  
17 regulations shall be to:

18 (i) Ensure the security and confidentiality of customer information in a manner fully  
19 consistent with industry standards;

20 (ii) Protect against anticipated threats or hazards to the security or integrity of such  
21 information; and

22 (iii) Protect against unauthorized access to or use of such information that could result in  
23 substantial harm or inconvenience to any resident of the state.

24 **6-48.1-4. Duty to report security breach or unauthorized use of personal information.**

25 (a) A person or agency that maintains or stores, but does not own or license data that  
26 includes personal information about a resident of the state, shall provide notice, as soon as

1 practicable and without unreasonable delay, when such person or agency:

2 (1) Knows or has reason to know of a breach of security; or

3 (2) When the person or agency knows or has reason to know that the personal information  
4 of such resident was acquired or used by an unauthorized person or used for an unauthorized  
5 purpose, to the owner or licensor in accordance with this chapter. In addition to providing notice  
6 as provided herein, the person or agency shall cooperate with the owner or licensor of such  
7 information. Cooperation shall include, but not be limited to, informing the owner or licensor of  
8 the breach of security or unauthorized acquisition or use, the date or approximate date of the  
9 incident and the nature thereof, and any steps the person or agency has taken or plans to take relating  
10 to the incident, except that "cooperation" shall not be deemed to require the disclosure of  
11 confidential business information or trade secrets, or to provide notice to a resident that may have  
12 been affected by the breach of security or unauthorized acquisition or use.

13 (b) A person or agency that owns or licenses data that includes personal information about  
14 a resident of the state, shall provide notice, as soon as practicable and without unreasonable delay,  
15 when such person or agency:

16 (1) Knows or has reason to know of a breach of security; or

17 (2) When the person or agency knows or has reason to know that the personal information  
18 of such resident was acquired or used by an unauthorized person or used for an unauthorized  
19 purpose, to the attorney general, the director of business regulation and to such resident, in  
20 accordance with this chapter. The notice to be provided to the attorney general and the director,  
21 and consumer reporting agencies or state agencies, if any, shall include, but not be limited to, the  
22 nature of the breach of security or unauthorized acquisition or use, the number of residents of the  
23 state affected by such incident at the time of notification, and any steps the person or agency has  
24 taken or plans to take relating to the incident.

25 Upon receipt of this notice, the director of business regulation shall identify any relevant  
26 consumer reporting agency or state agency, as deemed appropriate by the director, and forward the



1 names of the identified consumer reporting agencies and state agencies to the notifying person or  
2 agency. Such person or agency shall, as soon as practicable and without unreasonable delay, also  
3 provide notice, in accordance with this chapter, to the consumer reporting agencies and state  
4 agencies identified by the director of business regulation.

5 The notice to be provided to the resident shall include, but not be limited to, the consumer's  
6 right to obtain a police report, how a consumer requests a security freeze and the necessary  
7 information to be provided when requesting the security freeze, and any fees required to be paid to  
8 any of the consumer reporting agencies; provided, however, that the notification shall not include  
9 the nature of the breach or unauthorized acquisition or use or the number of residents of the state  
10 affected by the breach or unauthorized access or use.

11 (c) If an agency is within the executive department, it shall provide written notification of  
12 the nature and circumstances of the breach or unauthorized acquisition or use to the division of  
13 enterprise technology strategy and services and the administrator as soon as practicable and without  
14 unreasonable delay following the discovery of a breach of security or unauthorized acquisition or  
15 use, and shall comply with all policies and procedures adopted by that administrator pertaining to  
16 the reporting and investigation of such an incident.

17 **6-48.1-5. Cooperation with law enforcement.**

18 Notwithstanding the provisions of § 6-48.1-4, notice may be delayed if a law enforcement  
19 agency determines that provision of notice may impede a criminal investigation and has notified  
20 the attorney general, in writing thereof, and informs the person or agency of such determination. If  
21 notice is delayed due to that determination, and as soon as the law enforcement agency determines  
22 and informs the person or agency that notification no longer poses a risk of impeding an  
23 investigation, notice shall be provided, as soon as practicable, and without unreasonable delay. The  
24 person or agency shall cooperate with law enforcement in its investigation of any breach of security  
25 or unauthorized acquisition or use, which shall include the sharing of information relevant to the  
26 incident; provided, however, that such disclosure shall not require the disclosure of confidential

1 business information or trade secrets.

2 **6-48.1-6. Applicability of other state and federal laws.**

3 This chapter does not relieve a person or agency from the duty to comply with the  
4 requirements of any applicable general or public law or federal law regarding the protection and  
5 privacy of personal information; provided, however, a person who maintains procedures for  
6 responding to a breach of security pursuant to federal laws, rules, regulations, guidance, or  
7 guidelines, is deemed to be in compliance with this chapter, if the person notifies affected Rhode  
8 Island residents, in accordance with the maintained or required procedures when a breach occurs;  
9 provided, further, that the person also notifies the attorney general and the director of the office  
10 business regulation of the breach, as soon as practicable and without unreasonable delay following  
11 the breach. The notice to be provided to the attorney general and the director of business regulation  
12 shall consist of, but not be limited to, any steps the person or agency has taken or plans to take  
13 relating to the breach pursuant to the applicable federal law, rule, regulation, guidance or  
14 guidelines; provided, further, that if the person or agency does not comply with applicable federal  
15 laws, rules, regulations, guidance or guidelines, then it shall be subject to the provisions of this  
16 chapter.

17 **6-48.1-7. Public enforcement.**

18 (a) The attorney general may bring an action against a person or otherwise to remedy  
19 violations of this chapter and for other relief that may be appropriate.

20 (b) Whenever the attorney general has reason to believe that any person is using or is about  
21 to use any method, act, or practice declared to be in violation of this chapter, and that proceedings  
22 would be in the public interest, the attorney general may bring an action in the name of the state  
23 against that person to restrain by temporary restraining order or preliminary or permanent  
24 injunction the use of such method, act or practice. The action may be brought in the superior court  
25 of the county in which the person resides or has their principal place of business, or in the  
26 providence county superior court if the person has no place of business within the state. If more



1 than one person is joined as a defendant, the action may be brought in the superior court of the  
2 county where any one defendant resides or has their principal place of business. The court may  
3 issue temporary restraining orders or preliminary or permanent injunctions, and make other orders  
4 or judgments as may be necessary to restore to any person who has suffered any ascertainable loss  
5 by reason of the use or employment of such unlawful method, act or practice any monies or  
6 property, real or personal, which may have been acquired by means of that method, act, or practice.  
7 If the court finds that a person has employed any method, act or practice which they knew or should  
8 have known to be in violation of this chapter, the court may require that person to pay to the state  
9 a civil penalty of not more than five thousand dollars (\$5,000) for each violation, and also may  
10 require the person to pay the reasonable costs of investigation and litigation of such violation,  
11 including reasonable attorneys' fees. If the court finds any method, act, or practice in violation of  
12 this chapter, the court may issue any orders or judgments as may be necessary to restore any person  
13 who has suffered any ascertainable loss of any monies or property, real or personal, or up to three  
14 (3), but not less than two (2) times that amount, if the court finds that the use of the act or practice  
15 was a willful violation of this chapter, a civil penalty to be paid to the state of not more than five  
16 thousand dollars (\$5,000) for each violation, and also may require the person to pay the reasonable  
17 costs of investigation and litigation of the violation, including reasonable attorneys' fees.

18 (c) At least five (5) days prior to the commencement of any action brought under this  
19 section, except when a temporary restraining order is sought, the attorney general shall notify the  
20 person of the intended action, and give the person an opportunity to confer with the attorney general  
21 in person or by counsel, or other representative as to the proposed action. The notice shall be given  
22 the person by mail, postage prepaid, to their usual place of business, or if they have no usual place  
23 of business, to their last known address.

24 (d) Any special assistant or assistant attorney general or law enforcement officer receiving  
25 notice of any alleged violation of this chapter or of any violation of an injunction or order issued in  
26 an action brought under this section shall immediately forward written notice of the same, together

1 with any information that they may have to the office of the attorney general.

2 (e) Any person who violates the terms of an injunction or other order issued under this  
3 section shall forfeit and pay to the state a civil penalty of not more than ten thousand dollars  
4 (\$10,000) for each violation. For the purposes of this section, the court issuing an injunction or  
5 order shall retain jurisdiction, and the cause shall be continued, and in that case the attorney general  
6 acting in the name of the state may petition for recovery of the civil penalty.

7 **6-48.1-8. Private enforcement.**

8 (a) Any person who has been injured by a violation of this chapter, or any rule or regulation  
9 issued thereunder, or any person whose rights are affected by another person violating the  
10 provisions of this chapter may bring an action in the superior court, whether by way of original  
11 complaint, counterclaim, cross-claim or third-party action, for damages and such equitable relief,  
12 including an injunction, as the court deems to be necessary and proper.

13 (b) Any person entitled to bring an action may, if the violation of this chapter has caused  
14 similar injury to numerous other persons similarly situated, and if the court finds in a preliminary  
15 hearing that the person adequately and fairly represents the other persons, bring the action on their  
16 own behalf and any other similarly injured and situated persons; the court shall require that notice  
17 of the action be given to unnamed plaintiffs in the most effective practicable manner. The action  
18 shall not be dismissed, settled or compromised without the approval of the court, and notice of any  
19 proposed dismissal, settlement or compromise shall be given to all members of the class of  
20 petitioners in any manner as the court directs.

21 (c) At least thirty (30) days prior to the filing of any such action, a written demand for  
22 relief, identifying the claimant and reasonably describing the violation of this chapter and the injury  
23 suffered, shall be mailed or delivered to any prospective civil defendant. Any person receiving a  
24 demand for relief who, within thirty (30) days of the mailing or delivery of the demand for relief,  
25 makes a written tender of settlement which is rejected by the claimant may, in any subsequent  
26 action, file the written tender and an affidavit concerning its rejection and thereby limit any



1 recovery to the relief tendered if the court finds that the relief tendered was reasonable in relation  
2 to the injury actually suffered by the petitioner. In all other cases, if the court finds for the petitioner,  
3 recovery shall be in the amount of actual damages or twenty-five dollars (\$25.00), whichever is  
4 greater; or up to three (3), but not less than two (2) times the amount, if the court finds that the  
5 violation of this chapter was a willful or knowing that the refusal to grant relief upon demand was  
6 made in bad faith, with knowledge or reason to know that the act or practice complained of violated  
7 this chapter. For the purposes of this chapter, the amount of actual damages to be multiplied by the  
8 court shall be the amount of the judgment on all claims arising out of the same and underlying  
9 transaction or occurrence, regardless of the existence or nonexistence of insurance coverage  
10 available in payment of the claim. In addition, the court shall award any other equitable relief,  
11 including an injunction, as it deems to be necessary and proper. The demand requirements of this  
12 section shall not apply if the claim is asserted by way of counterclaim or cross-claim, or if the  
13 prospective civil defendant does not maintain a place of business or does not keep assets within the  
14 state, but the defendant may otherwise employ the provisions of this section by making a written  
15 offer of relief, and paying the rejected tender into court as soon as practicable after receiving notice  
16 of an action commenced under this section.

17 (d) A person may assert a claim under this section in a district court, whether by way of  
18 original complaint, counterclaim, cross-claim or third-party action, for money damages only. The  
19 damages may include double or treble damages, attorneys' fees and costs, as herein provided. The  
20 demand requirements and provision for tender of offer of settlement provided in this section shall  
21 also be applicable under this section; provided, that no rights to equitable relief shall be created  
22 under this subsection, nor shall a person asserting a claim hereunder be able to assert any claim on  
23 behalf of other similarly injured and situated persons as provided in § 6-48.1-8(b).

24 (e) If the court finds in any action commenced hereunder that there has been a violation of  
25 this chapter, the plaintiff shall, in addition to other relief provided for by this section and  
26 irrespective of the amount in controversy, be awarded reasonable attorneys' fees and costs incurred



1 in connection with said action; provided, however, the court shall deny recovery of attorneys' fees  
2 and costs which are incurred after the rejection of a reasonable written offer of settlement made  
3 within thirty (30) days of the mailing or delivery of the written demand for relief required by this  
4 section.

5 (f) Any person entitled to bring an action under this section shall not be required to initiate,  
6 pursue or exhaust any remedy established by any regulation, administrative procedure, local, state  
7 or federal law or statute or the common law, in order to bring an action under this section or to  
8 obtain injunctive relief or recover damages or attorneys' fees or costs or other relief, as provided in  
9 this section. Failure to exhaust administrative remedies shall not be a defense to any proceeding  
10 under this section, except as provided in subsection (g) of this section.

11 (g)(1) The court may upon motion by the defendant before the time for answering and after  
12 a hearing suspend proceedings brought under this section to permit the defendant to initiate action  
13 in which the plaintiff shall be named a party before any appropriate regulatory board or officer  
14 providing adjudicatory hearings to complainants if the defendant's evidence indicates that:

15 (i) There is a substantial likelihood that final action by the court favorable to the plaintiff  
16 would require of the defendant conduct or practices that would disrupt or be inconsistent with a  
17 regulatory scheme that regulates or covers the actions or transactions complained of by the plaintiff  
18 established and administered under law by any state or federal regulatory board or officer acting  
19 under statutory authority of the state or of the United States; or

20 (ii) That regulatory board, agency, department, or officer has a substantial interest in  
21 reviewing the transactions or actions prior to judicial action under this chapter, and that the  
22 regulatory board or officer has the power to provide substantially the relief sought by the plaintiff  
23 and the class, if any, which the plaintiff represents, under this section.

24 (2) Upon suspending proceedings under this section the court may enter any interlocutory  
25 or temporary orders it deems necessary and proper pending final action by the regulatory board,  
26 agency, department, or officer and trial, if any, in the court, including issuance of injunctions,

1 certification of a class, and orders concerning the presentation of the matter to the regulatory board,  
2 agency, department, or officer. The court shall issue appropriate interlocutory orders, decrees and  
3 injunctions to preserve the status quo between the parties pending final action by the regulatory  
4 board, agency, department, or officer and trial and shall stay all proceedings in any court or before  
5 any regulatory board, agency, department, or officer in which plaintiff and defendant are  
6 necessarily involved. The court may issue further orders, injunctions or other relief while the matter  
7 is before the regulatory board, agency, department, or officer and shall terminate the suspension  
8 and bring the matter forward for trial if it finds:

9 (i) That proceedings before the regulatory board, agency, department, or officer are  
10 unreasonably delayed or otherwise unreasonably prejudicial to the interests of a party before the  
11 court; or

12 (ii) That the regulatory board, agency, department, or officer has not taken final action  
13 within six (6) months of the beginning of the order suspending proceedings under this chapter.

14 (h) Recovering or failing to recover an award of damages or other relief in any  
15 administrative or judicial proceeding, except proceedings authorized by this section, by any person  
16 entitled to bring an action under this section, shall not constitute a bar to, or limitation upon relief  
17 authorized by this section.

18 SECTION 2. This act shall take effect on January 1, 2020.

=====

699 - Relating to Commercial Law

=====

EXPLANATION  
BY THE LEGISLATIVE COUNCIL  
OF

A N A C T

RELATING TO COMMERCIAL LAW -- GENERAL REGULATORY PROVISIONS -- THE  
DATA SECURITY BREACH NOTIFICATION ACT

\*\*\*

1           This act would establish a comprehensive statutory scheme to protect electronic data from  
2   identity theft and fraud. It would also require that all victims of data breaches be notified of the  
3   breach. In addition, the act would create many public and private monetary and equitable remedies  
4   for data security breach.

5           This act would take effect on January 1, 2020.

=====  
699 - Relating to Commercial Law  
=====