CHAPTER 715C

PERSONAL INFORMATION SECURITY BREACH PROTECTION

Referred to in §331.307, 364.22, 533.331, 701.1

715C.1 Definitions.

As used in this chapter, unless the context otherwise requires:

1. *"Breach of security"* means unauthorized acquisition of personal information maintained in computerized form by a person that compromises the security, confidentiality, or integrity of the personal information. *"Breach of security"* also means unauthorized acquisition of personal information maintained by a person in any medium, including on paper, that was transferred by the person to that medium from computerized form and that compromises the security, confidentiality, or integrity of the personal information. Good faith acquisition of personal information by a person or that person's employee or agent for a legitimate purpose of that person is not a breach of security, provided that the personal information is not used in violation of applicable law or in a manner that harms or poses an actual threat to the security, confidentiality, or integrity of the personal information.

2. *"Consumer"* means an individual who is a resident of this state.

3. *"Consumer reporting agency"* means the same as defined by the federal Fair Credit Reporting Act, 15 U.S.C. §1681a.

4. *"Debt"* means the same as provided in section 537.7102.

5. *"Encryption"* means the use of an algorithmic process pursuant to accepted industry standards to transform data into a form in which the data is rendered unreadable or unusable without the use of a confidential process or key.

6. *"Extension of credit"* means the right to defer payment of debt or to incur debt and defer its payment offered or granted primarily for personal, family, or household purposes.

7. *"Financial institution"* means the same as defined in section 536C.2, subsection 6.

8. *"Identity theft"* means the same as provided in section 715A.8.

9. *"Payment card"* means the same as defined in section 715A.10, subsection 4, paragraph *"c"*.

10. *"Person"* means an individual; corporation; business trust; estate; trust; partnership; limited liability company; association; joint venture; government; governmental subdivision, agency, or instrumentality; public corporation; or any other legal or commercial entity.

11. *a.* *"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 that relate to the individual if any of the data elements are not encrypted, redacted, or otherwise altered by any method or technology in such a manner that the name or data elements are unreadable or are encrypted, redacted, or otherwise altered by any method or technology but the keys to unencrypt, unredact, or otherwise read the data elements have been obtained through the breach of security:

(1) Social security number.

(2) Driver's license number or other unique identification number created or collected by a government body.

(3) Financial account number, credit card number, or debit card number in combination with any required expiration date, security code, access code, or password that would permit access to an individual's financial account.

(4) Unique electronic identifier or routing code, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

(5) Unique biometric data, such as a fingerprint, retina or iris image, or other unique physical representation or digital representation of biometric data.

b. *"Personal information"* does not include information that is lawfully obtained from

publicly available sources, or from federal, state, or local government records lawfully made available to the general public.

12. *"Redacted"* means altered or truncated so that no more than five digits of a social security number or the last four digits of other numbers designated in section 715A.8, subsection 1, paragraph *"a"*, are accessible as part of the data.

2008 Acts, ch 1154, §1; 2014 Acts, ch 1026, §135; 2014 Acts, ch 1062, §1 – 3; 2018 Acts, ch 1091, §8
Subsection 5 amended

715C.2 Security breach — notification requirements — remedies.

1. Any person who owns or licenses computerized data that includes a consumer's personal information that is used in the course of the person's business, vocation, occupation, or volunteer activities and that was subject to a breach of security shall give notice of the breach of security following discovery of such breach of security, or receipt of notification under subsection 2, to any consumer whose personal information was included in the information that was breached. The consumer notification shall be made in the most expeditious manner possible and without unreasonable delay, consistent with the legitimate needs of law enforcement as provided in subsection 3, and consistent with any measures necessary to sufficiently determine contact information for the affected consumers, determine the scope of the breach, and restore the reasonable integrity, security, and confidentiality of the data.

2. Any person who maintains or otherwise possesses personal information on behalf of another person shall notify the owner or licensor of the information of any breach of security immediately following discovery of such breach of security if a consumer's personal information was included in the information that was breached.

3. The consumer notification requirements of this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation and the agency has made a written request that the notification be delayed. The notification required by this section shall be made after the law enforcement agency determines that the notification will not compromise the investigation and notifies the person required to give notice in writing.

4. For purposes of this section, notification to the consumer may be provided by one of the following methods:

a. Written notice to the last available address the person has in the person's records.

b. Electronic notice if the person's customary method of communication with the consumer is by electronic means or is consistent with the provisions regarding electronic records and signatures set forth in chapter 554D and the federal Electronic Signatures in Global and National Commerce Act, 15 U.S.C. §7001.

c. Substitute notice, if the person demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars, that the affected class of consumers to be notified exceeds three hundred fifty thousand persons, or if the person does not have sufficient contact information to provide notice. Substitute notice shall consist of the following:

(1) Electronic mail notice when the person has an electronic mail address for the affected consumers.

(2) Conspicuous posting of the notice or a link to the notice on the internet site of the person if the person maintains an internet site.

(3) Notification to major statewide media.

5. Notice pursuant to this section shall include, at a minimum, all of the following:

a. A description of the breach of security.

b. The approximate date of the breach of security.

c. The type of personal information obtained as a result of the breach of security.

d. Contact information for consumer reporting agencies.

e. Advice to the consumer to report suspected incidents of identity theft to local law enforcement or the attorney general.

6. Notwithstanding subsection 1, notification is not required if, after an appropriate investigation or after consultation with the relevant federal, state, or local agencies

responsible for law enforcement, the person determined that no reasonable likelihood of financial harm to the consumers whose personal information has been acquired has resulted or will result from the breach. Such a determination must be documented in writing and the documentation must be maintained for five years.

7. This section does not apply to any of the following:

a. A person who complies with notification requirements or breach of security procedures that provide greater protection to personal information and at least as thorough disclosure requirements than that provided by this section pursuant to the rules, regulations, procedures, guidance, or guidelines established by the person's primary or functional federal regulator.

b. A person who complies with a state or federal law that provides greater protection to personal information and at least as thorough disclosure requirements for breach of security or personal information than that provided by this section.

c. A person who is subject to and complies with regulations promulgated pursuant to Tit. V of the federal Gramm-Leach-Bliley Act of 1999, 15 U.S.C. §6801 – 6809.

d. A person who is subject to and complies with regulations promulgated pursuant to Tit. II, subtit. F of the federal Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. §1320d – 1320d-9, and Tit. XIII, subtit. D of the federal Health Information Technology for Economic and Clinical Health Act of 2009, 42 U.S.C. §17921 – 17954.

8. Any person who owns or licenses computerized data that includes a consumer's personal information that is used in the course of the person's business, vocation, occupation, or volunteer activities and that was subject to a breach of security requiring notification to more than five hundred residents of this state pursuant to this section shall give written notice of the breach of security to the director of the consumer protection division of the office of the attorney general within five business days after giving notice of the breach of security to any consumer pursuant to this section.

9. *a.* A violation of this chapter is an unlawful practice pursuant to section 714.16 and, in addition to the remedies provided to the attorney general pursuant to section 714.16, subsection 7, the attorney general may seek and obtain an order that a party held to violate this section pay damages to the attorney general on behalf of a person injured by the violation.

b. The rights and remedies available under this section are cumulative to each other and to any other rights and remedies available under the law.

2008 Acts, ch 1154, §2; 2013 Acts, ch 90, §257; 2014 Acts, ch 1062, §4; 2018 Acts, ch 1091, §9

Identity theft — civil cause of action, see §714.16B
Identity theft passport, see §715A.9A
Subsections 7 and 8 amended