House Study Bill 526 - Introduced

SENATE/HOUSE FILE _____
BY (PROPOSED ATTORNEY GENERAL BILL)

A BILL FOR

An Act modifying certain provisions relating to personal information security breach protection.

BE IT ENACTED BY THE GENERAL ASSEMBLY OF THE STATE OF IOWA:

S.F. _____ H.F. _____

Section 1. Section 715C.1, subsections 1, 5, and 11, Code 2018, are amended to read as follows:

1. "*Breach of security*" means unauthorized acquisition, or reasonable belief of unauthorized acquisition, of personal information maintained in ~~computerized~~ any form, including but not limited to electronic or paper 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.

5. "*Encryption*" means the use of an one-hundred-twenty-eight-bit or higher algorithmic process to transform data into a form in which the data is rendered unreadable or unusable without the use of a confidential process or key.

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.

(6) Medical information, including but not limited to information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional.

(7) Health insurance information, including but not limited to an individual's health insurance policy number, subscriber identification number, or any unique identifier used by a health insurer to identify an individual.

(8) Tax identification number.

b. "*Personal information*" also includes a financial account number, credit card number, or debit card number alone.

c. "*Personal information*" also includes an account username or electronic mail address, in combination with any required password or account security information that would permit access to an individual's online account.

~~*b.*~~ *d.* "*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.

Sec. 2. Section 715C.2, subsections 1, 6, 7, and 8, Code 2018, are amended to read as follows:

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, but no later than forty-five days after the discovery of such breach of security or receipt of notification under subsection 2, 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.

6. *a.* 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.

b. In the event that notification is not required pursuant to this subsection, the person shall provide the written determination required in paragraph "*a*" to the director of the consumer protection division of the office of the attorney general within five business days after documenting such determination.

7. ~~This section does~~ Subsections 1 through 6 shall 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 Gramm-Leach-Bliley Act of 1999, 15 U.S.C. §6801 – 6809.

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~~ consumers pursuant to ~~this section~~ subsection 1 or any of the laws, rules, regulations, procedures, guidance, or guidelines set forth in subsection 7 shall give written notice of the breach of security ~~following discovery of such breach of security, or receipt of notification under subsection 2,~~ 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. The written notice shall include the following:

a. A sample copy of any notification sent to consumers.

b. The approximate number of consumers affected or potentially affected by the breach of security.

c. A description of any services offered to consumers affected or potentially affected by the breach of security, and instructions as to how consumers may use such services.

d. The name, address, telephone number, and electronic mail

address of an individual who may be contacted by the consumer protection division of the office of the attorney general for any additional information about the breach of security.

e. The federal employer identification number of the person, which the consumer protection division of the office of the attorney general may share with any state agency for the purpose of fraud detection. Notwithstanding chapter 22 or any other provision of law to the contrary, the federal employer identification number shall be maintained in a separate confidential file or other confidential medium.

EXPLANATION

The inclusion of this explanation does not constitute agreement with the explanation's substance by the members of the general assembly.

This bill modifies various provisions relating to personal information security breach protection.

The bill makes several changes to the definitions listed in Code section 715C.1. The bill expands the definition of "breach of security" to include the reasonable belief of unauthorized acquisition of personal information, which may be in any form, including electronic or paper form. However, the bill removes the unauthorized acquisition of personal information that was transferred from computerized form to another medium from the definition of "breach of security". The definition of "encryption" is modified to mean the use of an 128-bit or higher algorithmic process. The bill modifies the definition of "personal information" by providing that it may include a financial account number, credit card number, or debit card number alone. The bill also includes certain medical information, health insurance information, tax information, and electronic account information in the definition of "personal information".

Current law requires a person who owns or licenses personal information that is subject to a breach of security to give notice to affected consumers in the most expeditious manner possible and without unreasonable delay. The bill provides

that such notice to affected consumers must occur no later than 45 days after the discovery of the breach of security.

Current law provides that a person who owns or licenses personal information that is subject to breach of security does not need to provide notification of the security breach to affected consumers if the person makes a written determination that there is no reasonable likelihood of financial harm to affected consumers. The bill removes the term "financial", allowing a person to refrain from providing notification if the person makes a written determination that there is no reasonable likelihood of harm to affected consumers. The bill also requires a person who makes such a determination to provide this written determination to the director of the consumer protection division of the office of the attorney general within five business days after documenting the determination.

Current law requires a person who owns or licenses personal information that is subject to a breach of security requiring notification to more than 500 consumers in the state, as required by Code section 715C.2, to give written notice of the breach of security to the director of the consumer protection division of the office of the attorney general. The bill provides that written notification to the attorney general is also required for breaches of security where written notification to more than 500 consumers in the state is required by a person's primary or functional federal regulator, a state or federal law that gives greater protection to personal information than provided in Code section 715C.2, or certain federal law. The bill also specifies that written notification to the attorney general must include a sample copy of any notification sent to consumers, the approximate number of affected or potentially affected consumers, a description of any services offered to affected consumers, contact information for an individual who may be contacted for additional information regarding the breach of security,

and a federal employer identification number, which will be maintained in a confidential file.