Senate Study Bill 1071 - 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 5 and 11, Code 2019, are amended to read as follows:

5. "*Encryption*" means the use of an algorithmic process pursuant to accepted industry standards, or any other accepted industry standard 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 history, medical treatment by a health care professional, diagnosis of mental or physical condition by a health care professional, or deoxyribonucleic acid profile.

(7) Health insurance policy number, subscriber

identification number, or any other unique identifier used by a health insurer to identify an individual.

(8) Taxpayer identification number.

(9) A private key that is unique to an individual and that is used to authenticate or sign an electronic record.

(10) Passport number.

b. "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 a consumer's online account.

~~*b.*~~ *c. "Personal information"* does not include information that is lawfully obtained from a publicly available ~~sources~~ source, or from federal, state, or local government records lawfully made available to the general public.

Sec. 2. Section 715C.2, subsections 1, 6, and 8, Code 2019, are amended to read as follows:

1. *a.* 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~~ but no later than forty-five days after the discovery of such breach of security or receipt of notification under subsection 2, unless a longer time is necessary because of 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.

b. In the case of a breach of security involving personal

information relating to a consumer's online account as described in section 715C.1, subsection 11, paragraph "b", and no other personal information described in section 715C.1, subsection 11, the person or business may comply with the notification requirements of this section by providing notification of the security breach to the consumer whose personal information was subject to the breach of security, in electronic or other form, that directs the consumer to promptly change the consumer's password or account security information, or to take any other appropriate steps to protect the consumer's online account with the person or business and all other online accounts for which the consumer uses the same account username or electronic mail address and password or account security information. However, in providing notification of a breach of security in electronic form to an online account that is affected or compromised by the breach of security, a person or business may provide notification by such method only when the consumer is connected to the online account from an internet protocol address or online location from which the person or business knows the consumer customarily accesses the online account, and the notification is provided to the consumer in a clear and conspicuous manner.

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.

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 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 all of 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.

Sec. 3. Section 715C.2, subsection 7, unnumbered paragraph 1, Code 2019, is amended to read as follows:

~~This section does~~ Subsections 1 through 6 shall not apply to any of the following:

Sec. 4. Section 715C.2, Code 2019, is amended by adding the following new subsection:

NEW SUBSECTION. 09. *a.* Any employer or payroll service provider that owns or licenses computerized data relating to income tax withholdings shall notify the consumer protection

division of the office of the attorney general without unreasonable delay after discovery or notification of the unauthorized access and acquisition of unencrypted computerized data of a taxpayer identification number in combination with the income tax withholdings for that taxpayer, the unauthorized access and acquisition of which gives the employer or payroll service provider reason to believe that identity theft or other fraud has or will occur. With respect to an employer, this subsection applies only to information regarding the employer's employees, and does not apply to information regarding the employer's customers or other nonemployees.

b. In providing notification to the consumer protection division of the office of the attorney general pursuant to this subsection, the employer or payroll service provider shall provide the name and federal employer identification number of the person that was or may be affected by the breach of security. Upon receipt of such notice, the consumer protection division of the office of the attorney general shall notify the department of revenue of the breach of security.

c. Notwithstanding any other provision in this section, a breach of security involving information described in paragraph *"a"* shall be subject only to the notification requirements contained in this subsection.

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 expands the definition of "encryption" in Code section 715C.1 to include, in addition to the use of an algorithmic process pursuant to accepted industry standards, any other accepted industry standard process. The bill adds certain medical information, health insurance information, tax information, passport information, and electronic account information to 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 or notification of the breach of security, unless delayed for law enforcement reasons.

The bill provides that, in the case of a security breach only involving personal information about a consumer's online account, a person or business may comply with the notification requirements of Code section 715C.2 by providing notification to the consumer whose personal information was subject to the security breach, in electronic or other form, that directs the consumer to take certain steps to protect the consumer's online account with that person or business and all other online accounts for which the same account information is used. However, in providing notification of a security breach in electronic form to an online account that is affected or compromised by the security breach, a person or business may only do so when the consumer is connected to the online account from an internet protocol address or online location from which the person or business knows the customer customarily accesses the account, and the notification is provided in a clear and conspicuous manner.

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 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, and contact information for an individual who may be contacted for additional information regarding the breach of security.

The bill provides that any employer or payroll service provider that owns or licenses computerized data relating to income tax withholdings shall notify the consumer protection division without unreasonable delay after discovery or notification of the breach of security of a taxpayer identification number in combination with the income tax withholdings for that taxpayer, the security breach of which gives the employer or payroll service provider reason to believe that identify theft or other fraud has or will occur. With respect to an employer, such notification requirements only apply to information regarding the employer's employees. In providing notification to the consumer protection division, the employer or payroll service provider shall provide the name and federal employer identification number of the person affected. Upon receiving the notice, the consumer protection division shall notify the department of revenue of the security breach. The bill specifies that no other notification

l requirements apply to a security breach of this nature.