

House Study Bill 14 - Introduced

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

A BILL FOR

- 1 An Act modifying certain provisions relating to personal
- 2 information security breach protection.
- 3 BE IT ENACTED BY THE GENERAL ASSEMBLY OF THE STATE OF IOWA:

1 Section 1. Section 715C.1, subsections 5 and 11, Code 2019,
2 are amended to read as follows:

3 5. *“Encryption”* means the use of an algorithmic process
4 pursuant to accepted industry standards, or any other accepted
5 industry standard process, to transform data into a form in
6 which the data is rendered unreadable or unusable without the
7 use of a confidential process or key.

8 11. a. *“Personal information”* means an individual’s first
9 name or first initial and last name in combination with any
10 one or more of the following data elements that relate to the
11 individual if any of the data elements are not encrypted,
12 redacted, or otherwise altered by any method or technology in
13 such a manner that the name or data elements are unreadable or
14 are encrypted, redacted, or otherwise altered by any method or
15 technology but the keys to unencrypt, unredact, or otherwise
16 read the data elements have been obtained through the breach
17 of security:

18 (1) Social security number.

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

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

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

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

32 (6) Medical history, medical treatment by a health care
33 professional, diagnosis of mental or physical condition by a
34 health care professional, or deoxyribonucleic acid profile.

35 (7) Health insurance policy number, subscriber

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

3 (8) Taxpayer identification number.

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

6 (10) Passport number.

7 b. "Personal information" also includes an account username
8 or electronic mail address, in combination with any required
9 password or account security information that would permit
10 access to a consumer's online account.

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

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

17 1. a. Any person who owns or licenses computerized data
18 that includes a consumer's personal information that is used
19 in the course of the person's business, vocation, occupation,
20 or volunteer activities and that was subject to a breach
21 of security shall give notice of the breach of security
22 following discovery of such breach of security, or receipt of
23 notification under subsection 2, to any consumer whose personal
24 information was included in the information that was breached.
25 The consumer notification shall be made in the most expeditious
26 manner possible and without unreasonable delay, ~~consistent~~
27 with but no later than forty-five days after the discovery
28 of such breach of security or receipt of notification under
29 subsection 2, unless a longer time is necessary because of the
30 legitimate needs of law enforcement as provided in subsection
31 3, and consistent with any measures necessary to sufficiently
32 determine contact information for the affected consumers,
33 determine the scope of the breach, and restore the reasonable
34 integrity, security, and confidentiality of the data.

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

1 information relating to a consumer's online account as
2 described in section 715C.1, subsection 11, paragraph "b",
3 and no other personal information described in section
4 715C.1, subsection 11, the person or business may comply with
5 the notification requirements of this section by providing
6 notification of the security breach to the consumer whose
7 personal information was subject to the breach of security,
8 in electronic or other form, that directs the consumer to
9 promptly change the consumer's password or account security
10 information, or to take any other appropriate steps to protect
11 the consumer's online account with the person or business and
12 all other online accounts for which the consumer uses the
13 same account username or electronic mail address and password
14 or account security information. However, in providing
15 notification of a breach of security in electronic form to an
16 online account that is affected or compromised by the breach
17 of security, a person or business may provide notification
18 by such method only when the consumer is connected to the
19 online account from an internet protocol address or online
20 location from which the person or business knows the consumer
21 customarily accesses the online account, and the notification
22 is provided to the consumer in a clear and conspicuous manner.

23 6. a. Notwithstanding subsection 1, notification is
24 not required if, after an appropriate investigation or
25 after consultation with the relevant federal, state, or
26 local agencies responsible for law enforcement, the person
27 determined that no reasonable likelihood of financial harm to
28 the consumers whose personal information has been acquired has
29 resulted or will result from the breach. Such a determination
30 must be documented in writing and the documentation must be
31 maintained for five years.

32 b. In the event that notification is not required pursuant
33 to this subsection, the person shall provide the written
34 determination required in paragraph "a" to the director of the
35 consumer protection division of the office of the attorney

1 general within five business days after documenting such
2 determination.

3 8. Any person who owns or licenses computerized data that
4 includes a consumer's personal information that is used in
5 the course of the person's business, vocation, occupation,
6 or volunteer activities and that was subject to a breach of
7 security requiring notification to more than five hundred
8 ~~residents of this state~~ consumers pursuant to ~~this section~~
9 subsection 1, or any of the laws, rules, regulations,
10 procedures, guidance, or guidelines set forth in subsection
11 7, shall give written notice of the breach of security to the
12 director of the consumer protection division of the office of
13 the attorney general within five business days after giving
14 notice of the breach of security to any consumer pursuant to
15 this section. The written notice shall include all of the
16 following:

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

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

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

23 d. The name, address, telephone number, and electronic mail
24 address of an individual who may be contacted by the consumer
25 protection division of the office of the attorney general for
26 any additional information about the breach of security.

27 Sec. 3. Section 715C.2, subsection 7, unnumbered paragraph
28 1, Code 2019, is amended to read as follows:

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

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

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

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

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

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

24 EXPLANATION

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

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

29 The bill expands the definition of "encryption" in Code
30 section 715C.1 to include, in addition to the use of an
31 algorithmic process pursuant to accepted industry standards,
32 any other accepted industry standard process. The bill adds
33 certain medical information, health insurance information,
34 tax information, passport information, and electronic account
35 information to the definition of "personal information".

1 Current law requires a person who owns or licenses personal
2 information that is subject to a breach of security to give
3 notice to affected consumers in the most expeditious manner
4 possible and without unreasonable delay. The bill provides
5 that such notice to affected consumers must occur no later than
6 45 days after the discovery or notification of the breach of
7 security, unless delayed for law enforcement reasons.

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

25 Current law provides that a person who owns or licenses
26 personal information that is subject to breach of security does
27 not need to provide notification of the security breach to
28 affected consumers if the person makes a written determination
29 that there is no reasonable likelihood of financial harm to
30 affected consumers. The bill requires a person who makes
31 such a determination to provide this written determination
32 to the director of the consumer protection division of the
33 office of the attorney general within five business days after
34 documenting the determination.

35 Current law requires a person who owns or licenses personal

1 information that is subject to a breach of security requiring
2 notification to more than 500 consumers in the state, as
3 required by Code section 715C.2, to give written notice
4 of the breach of security to the director of the consumer
5 protection division of the office of the attorney general.
6 The bill provides that written notification to the attorney
7 general is also required for breaches of security where
8 written notification to more than 500 consumers in the state
9 is required by a person's primary or functional federal
10 regulator, a state or federal law that gives greater protection
11 to personal information than provided in Code section 715C.2,
12 or certain federal law. The bill also specifies that written
13 notification to the attorney general must include a sample
14 copy of any notification sent to consumers, the approximate
15 number of affected or potentially affected consumers, a
16 description of any services offered to affected consumers, and
17 contact information for an individual who may be contacted for
18 additional information regarding the breach of security.

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

S.F. _____ H.F. _____

1 requirements apply to a security breach of this nature.