

Senate Study Bill 3200

SENATE FILE _____
BY (PROPOSED COMMITTEE ON
COMMERCE BILL BY
CHAIRPERSON WARNSTADT)

Passed Senate, Date _____ Passed House, Date _____
Vote: Ayes _____ Nays _____ Vote: Ayes _____ Nays _____
Approved _____

A BILL FOR

1 An Act relating to identity theft, including providing for the
2 notification of a breach in the security of computerized data
3 that includes personal information, establishing a business
4 duty to safeguard personal information against a breach of
5 security, and providing penalties.
6 BE IT ENACTED BY THE GENERAL ASSEMBLY OF THE STATE OF IOWA:
7 TLSB 6517SC 82
8 rn/nh/8

PAG LIN

1 1 Section 1. NEW SECTION. 715C.1 DEFINITIONS.
1 2 As used in this chapter, unless the context otherwise
1 3 requires:
1 4 1. "Breach of security" means unauthorized acquisition of
1 5 computerized data maintained by a person that materially
1 6 compromises the security, confidentiality, or integrity of
1 7 personal information maintained by the person. Good faith
1 8 acquisition of personal information by a person or that
1 9 person's employee or agent for a legitimate purpose of that
1 10 person is not a breach of security, provided that the personal
1 11 information is not used in violation of applicable law or in a
1 12 manner that harms or poses an actual threat to the security,
1 13 confidentiality, or integrity of the personal information.
1 14 2. "Consumer" means an individual who is a resident of
1 15 this state.
1 16 3. "Consumer reporting agency" means the same as defined
1 17 by the federal Fair Credit Reporting Act, 15 U.S.C. } 1681a.
1 18 4. "Debt" means the same as provided in section 537.7102.
1 19 5. "Encryption" means the use of an algorithmic process to
1 20 transform data into a form in which the data is rendered
1 21 unreadable or unusable without the use of a confidential
1 22 process or key.
1 23 6. "Extension of credit" means the right to defer payment
1 24 of debt or to incur debt and defer its payment offered or
1 25 granted primarily for personal, family, or household purposes.
1 26 7. "Financial institution" means the same as defined in
1 27 section 536C.2, subsection 6.
1 28 8. "Identity theft" means the same as provided in section
1 29 715A.8.
1 30 9. "Payment card" means the same as defined in section
1 31 715A.10, subsection 3, paragraph "b".
1 32 10. "Person" means an individual; corporation; business
1 33 trust; estate; trust; partnership; limited liability company;
1 34 association; joint venture; government; governmental
1 35 subdivision, agency, or instrumentality; public corporation;
2 1 or any other legal or commercial entity.
2 2 11. "Personal information" means an individual's first
2 3 name or first initial and last name in combination with any
2 4 one or more of the following data elements that relate to the
2 5 individual if neither the name nor the data elements are
2 6 encrypted, redacted, or otherwise altered by any method or
2 7 technology in such a manner that the name or data elements are
2 8 unreadable:
2 9 a. Social security number.
2 10 b. Driver's license number or other unique identification
2 11 number created or collected by a government body.
2 12 c. Financial account number, credit card number, or debit
2 13 card number in combination with any required security code,
2 14 access code, or password that would permit access to an
2 15 individual's financial account.

2 16 d. Unique electronic identifier or routing code, in
2 17 combination with any required security code, access code, or
2 18 password.

2 19 12. "Redacted" means altered or truncated so that no more
2 20 than the last four digits of a social security number or other
2 21 numbers designated in section 715A.8, subsection 1, paragraph
2 22 "a", is accessible as part of the data.

2 23 Sec. 2. NEW SECTION. 715C.2 SECURITY BREACH == CONSUMER
2 24 NOTIFICATION == REMEDIES.

2 25 1. Any person who owns, maintains, or otherwise possesses
2 26 data that includes a consumer's personal information that is
2 27 used in the course of the person's business, vocation,
2 28 occupation, or volunteer activities and who was subject to a
2 29 breach of security shall give notice of the breach of security
2 30 following discovery of such breach of security, or receipt of
2 31 notification under subsection 2, to any consumer whose
2 32 personal information was included in the information that was
2 33 breached. The consumer notification shall be made in the most
2 34 expeditious manner possible and without unreasonable delay,
2 35 consistent with the legitimate needs of law enforcement as
3 1 provided in subsection 3, and consistent with any measures
3 2 necessary to sufficiently determine contact information for
3 3 the affected consumers, determine the scope of the breach, and
3 4 restore the reasonable integrity, security, and
3 5 confidentiality of the data.

3 6 2. Any person who maintains or otherwise possesses
3 7 personal information on behalf of another person shall notify
3 8 the owner or licensor of the information of any breach of
3 9 security immediately following discovery of such breach of
3 10 security if a consumer's personal information was included in
3 11 the information that was breached.

3 12 3. The consumer notification requirements of this section
3 13 may be delayed if a law enforcement agency determines that the
3 14 notification will impede a criminal investigation and the
3 15 agency has made a written request that the notification be
3 16 delayed. The notification required by this section shall be
3 17 made after the law enforcement agency determines that the
3 18 notification will not compromise the investigation and
3 19 notifies the person required to give notice in writing.

3 20 4. For purposes of this section, notification to the
3 21 consumer may be provided by one of the following methods:

3 22 a. Written notice.

3 23 b. Electronic notice if the person's customary method of
3 24 communication with the consumer is by electronic means or is
3 25 consistent with the provisions regarding electronic records
3 26 and signatures set forth in chapter 554D and the federal
3 27 Electronic Signatures in Global and National Commerce Act, 15
3 28 U.S.C. } 7001.

3 29 c. Telephone notice, provided that the contact is made
3 30 directly with the affected consumer.

3 31 d. Substitute notice, if the person demonstrates that the
3 32 cost of providing notice would exceed two hundred fifty
3 33 thousand dollars, that the affected class of consumers to be
3 34 notified exceeds three hundred fifty thousand persons, or if
3 35 the person does not have sufficient contact information to
4 1 provide notice. Substitute notice shall consist of the
4 2 following:

4 3 (1) Electronic mail notice when the person has an
4 4 electronic mail address for the affected consumers.

4 5 (2) Conspicuous posting of the notice or a link to the
4 6 notice on the internet web site of the person if the person
4 7 maintains an internet web site.

4 8 (3) Notification to major statewide media.

4 9 5. Notice pursuant to this section shall include, at a
4 10 minimum, all of the following:

4 11 a. A description of the breach of security.

4 12 b. The approximate date of the breach of security.

4 13 c. The type of personal information obtained as a result
4 14 of the breach of security.

4 15 d. Contact information for consumer reporting agencies.

4 16 e. Advice to the consumer to report suspected incidents of
4 17 identity theft to law enforcement, including the federal trade
4 18 commission.

4 19 6. Notwithstanding subsection 1, notification is not
4 20 required if, after an appropriate investigation or after
4 21 consultation with the relevant federal, state, or local
4 22 agencies responsible for law enforcement, the person
4 23 determined that no reasonable likelihood of harm to the
4 24 consumers whose personal information has been acquired has
4 25 resulted or will result from the breach. Such a determination
4 26 must be documented in writing and the documentation must be

4 27 maintained for five years.

4 28 7. This section does not apply to any of the following:

4 29 a. A person who complies with notification requirements or
4 30 breach of security procedures that provide greater protection
4 31 to personal information and at least as thorough disclosure
4 32 requirements than that provided by this section pursuant to
4 33 the rules, regulations, procedures, guidance, or guidelines
4 34 established by the person's primary or functional federal
4 35 regulator.

5 1 b. A person who complies with a state or federal law that
5 2 provides greater protection to personal information and at
5 3 least as thorough disclosure requirements for breach of
5 4 security or personal information than that provided by this
5 5 section.

5 6 c. A person who is subject to and complies with
5 7 regulations promulgated pursuant to Title V of the
5 8 Gramm=Leach=Bliley Act of 1999, 15 U.S.C. } 6801=6809.

5 9 8. a. The attorney general may take appropriate action to
5 10 enact this chapter or bring an action on behalf of an injured
5 11 person for an injunction, actual damages incurred by the
5 12 person, attorney fees, interest, and court costs.

5 13 b. The rights and remedies available under this section
5 14 are cumulative to each other and to any other rights and
5 15 remedies available under the law.

5 16 Sec. 3. NEW SECTION. 715C.3 PERSONAL INFORMATION ==
5 17 BUSINESS DUTY TO SAFEGUARD == RIGHT OF ACTION == DAMAGES AND
5 18 PENALTIES.

5 19 1. Any person who accepts a payment card in connection
5 20 with transactions occurring in the ordinary course of business
5 21 has a duty to comply with or adhere to payment card industry
5 22 data security standards. A financial institution may bring an
5 23 action against a person who is subject to a breach of security
5 24 if the person is found at the time of the breach to have
5 25 engaged in or violated such data security standards.

5 26 2. In an action commenced by a financial institution to
5 27 recover damages pursuant to subsection 1, the financial
5 28 institution shall submit in writing a request that the person
5 29 alleged to have violated this section certify compliance with
5 30 the standards pursuant to a payment card industry=approved
5 31 independent auditor or another person authorized to issue such
5 32 a certification. A presumption of compliance shall exist if a
5 33 person contracts for or utilizes the services of a third party
5 34 to collect, maintain, or store personal information used in
5 35 connection with a payment card, and contractually requires
6 1 that the third party ensure compliance with the standards on
6 2 an ongoing basis.

6 3 3. a. A financial institution prevailing in an action for
6 4 failure to safeguard personal information against a breach of
6 5 security may recover actual damages arising from the failure.
6 6 Actual damages shall include any costs incurred by the
6 7 financial institution in relation to the following:

6 8 (1) Cancellation or reissuance of a payment card affected
6 9 by the security breach.

6 10 (2) Closing of a deposit, transaction, share draft, or
6 11 other account affected by the security breach and any action
6 12 to stop payment or block a transaction with respect to the
6 13 account.

6 14 (3) Opening or reopening of a deposit, transaction, share
6 15 draft, or other account affected by the security breach.

6 16 (4) Refunding or crediting made to an account holder to
6 17 cover the cost of any unauthorized transaction relating to the
6 18 breach of security.

6 19 (5) Notification to account holders affected by the breach
6 20 of security.

6 21 b. Reasonable attorney fees and costs shall be awarded to
6 22 the prevailing party, with the exception that an award shall
6 23 not be made to a person who failed to submit certification as
6 24 required in subsection 2.

6 25 c. An action pursuant to this section shall not be
6 26 commenced against any person other than a person who has been
6 27 found to have violated this section.

6 28 4. The attorney general may adopt rules necessary to
6 29 implement this section, which may include identification of
6 30 payment card industry standards to be applied.

6 31 EXPLANATION

6 32 This bill provides for the notification of a breach in the
6 33 security of computerized data of personal information, and
6 34 establishes a business duty to safeguard such information
6 35 against security breaches.

7 1 The bill requires a person who owns, maintains, or
7 2 otherwise possesses computerized data that includes personal

7 3 information to provide notice of any breach of the person's
7 4 security of the data to those residents of this state whose
7 5 personal information was or may have been acquired by an
7 6 unauthorized person. The bill also requires a person who
7 7 maintains computerized data that includes personal information
7 8 that the person does not own to notify the owner of the data
7 9 of any breach in the security of the data. A "person" is
7 10 defined in the bill to include persons that conduct business
7 11 in this state and state agencies. The notice shall be
7 12 provided immediately unless a law enforcement agency
7 13 determines that the notification will impede a criminal
7 14 investigation. The notice may be made in writing, through
7 15 electronic means, or by substitute notice, as defined in the
7 16 bill, and must contain information regarding a description of
7 17 the breach of security, the approximate date of the breach,
7 18 the type of personal information obtained, contact information
7 19 for consumer reporting agencies, and consumer reporting
7 20 advice.

7 21 The bill provides that notification will not be required if
7 22 an investigation or consultation with law enforcement agencies
7 23 determines that no reasonable likelihood of harm has or will
7 24 result from the breach, and that the bill's provisions do not
7 25 apply to persons complying with specified requirements or
7 26 breach of security procedures that provide greater protection
7 27 to personal information and at least as thorough disclosure
7 28 requirements as provided pursuant to the bill.

7 29 The bill provides that the attorney general may bring a
7 30 civil action on behalf of an injured person.

7 31 The bill additionally establishes a duty with respect to a
7 32 person who accepts a payment card in connection with business
7 33 transactions to adhere to payment card industry data security
7 34 standards. The bill authorizes a financial institution, as
7 35 defined in the bill by reference to include a bank, savings
8 1 and loan association, or credit union organized under the
8 2 provisions of any state or federal law, and their affiliates,
8 3 to bring an action against a person who is subject to a breach
8 4 of security if the person is found at the time of the breach
8 5 to have engaged in or violated such data security standards.

8 6 The bill requires a financial institution to submit a
8 7 written request that a person alleged to have failed to
8 8 protect personal information certify compliance with the
8 9 standards pursuant to a payment card industry-approved
8 10 independent auditor or another person authorized to issue such
8 11 a certification. A presumption in favor of compliance exists
8 12 if a person contracts for or utilizes the services of a third
8 13 party to collect, maintain, or store personal information used
8 14 in connection with a payment card, and requires that the third
8 15 party ensure compliance with the standards on an ongoing
8 16 basis.

8 17 Actual damages which may be recovered by a financial
8 18 institution can include any costs incurred by the financial
8 19 institution relating to cancellation or reissuance of a
8 20 payment card; closing of a deposit, transaction, share draft,
8 21 or other account affected and any action to stop payment or
8 22 block a transaction; opening or reopening of a deposit,
8 23 transaction, share draft, or other account; refunding or
8 24 crediting made to an account holder to cover the cost of any
8 25 unauthorized transaction; and notification to account holders
8 26 affected by the breach of security. The bill also awards
8 27 attorney fees and costs to a prevailing party unless that
8 28 party is a person who failed to comply with the written
8 29 certification request. Further, the bill provides that an
8 30 action for failure to adhere to data security standards cannot
8 31 be commenced against any person other than a person who has
8 32 been found to have violated such standards, other than an
8 33 award of attorney fees and costs if the financial institution
8 34 is not a prevailing party.

8 35 The bill provides that the attorney general shall adopt
9 1 rules necessary to implement the bill's provisions, including
9 2 identification of payment card industry standards to be
9 3 applied.