

JAN 24 2005

COMMERCE, REGULATION & LABOR

HOUSE FILE 2107

BY WISE

Passed House, Date _____

Passed Senate, Date _____

Vote: Ayes _____ Nays _____

Vote: Ayes _____ Nays _____

Approved _____

A BILL FOR

1 An Act to require notification of a breach of the security of a
2 system of computerized data containing personal information
3 and providing for civil remedies.

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

- 5
- 6
- 7
- 8
- 9
- 10
- 11
- 12
- 13
- 14
- 15
- 16
- 17
- 18
- 19
- 20
- 21
- 22
- 23
- 24

HF 2107

1 Section 1. NEW SECTION. 715C.1 DEFINITIONS.

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

4 1. "Breach of the security of the system" means
5 unauthorized acquisition of computerized data that compromises
6 the security, confidentiality, or integrity of personal
7 information maintained by an information holder. Good faith
8 acquisition of personal information by an employee or agent of
9 the information holder for the purposes of the information
10 holder is not a breach of the security of the system, provided
11 that the personal information is not used or subject to
12 further unauthorized disclosure.

13 2. "Information holder" means any person that conducts
14 business in this state, or any agency of this state or any of
15 its political subdivisions, that owns or licenses computerized
16 data that includes personal information.

17 3. "Personal information" means a person's first name, or
18 first initial, and last name in combination with any one or
19 more of the following data elements, when either the name or
20 the data elements are not encrypted:

21 a. Social security number.

22 b. Driver's license or nonoperator's identification card
23 number.

24 c. Account number or credit or debit card number, in
25 combination with any required security code, access code, or
26 password that would permit access to a person's financial
27 account.

28 "Personal information" does not include publicly available
29 information that is lawfully made available to the general
30 public from federal, state, or local government records.

31 Sec. 2. NEW SECTION. 715C.2 DISCLOSURE OF BREACH OF
32 SECURITY.

33 1. An information holder shall disclose any breach of the
34 security of the system following discovery or notification of
35 the breach in the security of the data held by the information

1 holder to any resident of this state whose personal
2 information was, or is reasonably believed to have been,
3 acquired by an unauthorized person. The disclosure shall be
4 made in the most expedient manner possible and without
5 unreasonable delay, consistent with the legitimate needs of
6 law enforcement, as provided in subsection 3, or any measures
7 necessary to determine the scope of the breach and restore the
8 reasonable integrity of the data system.

9 2. An information holder that maintains computerized data
10 that includes personal information that the information holder
11 does not own shall notify the owner or licensee of the
12 information of any breach of the security of the data
13 immediately following discovery if the personal information
14 was, or is reasonably believed to have been, acquired by an
15 unauthorized person.

16 3. The notification required by this section may be
17 delayed if a law enforcement agency determines that the
18 notification will impede a criminal investigation. The
19 notification required by this section shall be made after the
20 law enforcement agency determines that it will not compromise
21 the investigation.

22 4. For purposes of this section, notice shall be provided
23 by one of the following methods:

24 a. Written notice.

25 b. Electronic notice, if the notice provided is consistent
26 with the provisions regarding electronic records and
27 signatures set forth in chapter 554D and 15 U.S.C. § 7001.

28 c. Substitute notice, if the information holder
29 demonstrates that the cost of providing notice would exceed
30 two hundred fifty thousand dollars, or that the affected class
31 of subject persons to be notified exceeds five hundred
32 thousand persons, or the information holder does not have
33 sufficient contact information. Substitute notice shall
34 consist of all of the following:

35 (1) Notice by electronic mail when the information holder

1 has an electronic mail address for the subject person.

2 (2) Conspicuous posting of the notice on the information
3 holder's internet website, if the information holder maintains
4 an internet website.

5 (3) Notification to major statewide media.

6 5. Notwithstanding subsection 4, an information holder
7 that maintains its own notification procedures as part of an
8 information security policy for the treatment of personal
9 information and is otherwise consistent with the timing
10 requirements of this section shall be deemed to be in
11 compliance with the notification requirements of this section
12 if the information holder notifies subject persons in
13 accordance with its policies in the event of a breach of
14 security of the system.

15 Sec. 3. NEW SECTION. 715C.3 REMEDIES.

16 1. Any person who is neither an agency of this state nor a
17 political subdivision of this state, and who is injured by a
18 violation of this chapter, may institute a civil action to
19 recover actual damages, court costs, interest, and attorney
20 fees, and to enjoin the information holder from further action
21 in violation of this chapter.

22 2. The rights and remedies available under this section
23 are cumulative to each other and to any other rights and
24 remedies available under law.

25 EXPLANATION

26 This bill requires an information holder that owns or
27 licenses computerized data that includes personal information
28 to disclose any breach of the person's security of the data to
29 those residents of this state whose personal information was
30 or may have been acquired by an unauthorized person. An
31 "information holder" is defined as any person that conducts
32 business in this state and includes a state agency or a
33 political subdivision of the state. The bill requires an
34 information holder that maintains computerized data that
35 includes personal information that the information holder does

1 not own to notify the owner of the data of any breach in the
2 security of the data.

3 The notification shall be provided immediately unless a law
4 enforcement agency determines that the notification will
5 impede a criminal investigation. The notice may be made in
6 writing, through electronic means, or by substitute notice as
7 defined by the bill.

8 The bill provides that a person who is injured by the
9 failure to be notified of a security breach required by the
10 bill may file a civil action for an injunction and actual
11 damages, attorney fees, interest, and court costs.

12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35