SENATE BILL 5341
_____

State of Washington   60th Legislature   2007 Regular Session

By Senators Kline, Weinstein and Hobbs

Read first time 01/17/2007.   Referred to Committee on Consumer Protection & Housing.

1   AN ACT Relating to breaches of security that compromise personal
2   information; amending RCW 19.255.010 and 42.56.590; adding a new
3   section to chapter 19.86 RCW; and prescribing penalties.

4   BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF WASHINGTON:

5   **Sec. 1.** RCW 19.255.010 and 2005 c 368 s 2 are each amended to read
6   as follows:
7   (1) Any person or business that conducts business in this state and
8   that owns or licenses computerized data that includes personal
9   information shall disclose any breach of the security of the system
10   following discovery or notification of the breach in the security of
11   the data to any resident of this state whose unencrypted personal
12   information was, or is reasonably believed to have been, acquired by an
13   unauthorized person.   The disclosure shall be made in the most
14   expedient time possible and without unreasonable delay, consistent with
15   the legitimate needs of law enforcement, as provided in subsection (3)
16   of this section, or any measures necessary to determine the scope of
17   the breach and restore the reasonable integrity of the data system.
18   (2) Any person or business that maintains computerized data that
19   includes personal information that the person or business does not own

shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

(3) The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section shall be made after the law enforcement agency determines that it will not compromise the investigation.

(4) For purposes of this section, "breach of the security of the system" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business. Good faith acquisition of personal information by an employee or agent of the person or business for the purposes of the person or business is not a breach of the security of the system when the personal information is not used or subject to further unauthorized disclosure.

(5) For purposes of this section, "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, when either the name or the data elements are not encrypted:

(a) Social security number;

(b) Driver's license number or Washington identification card number; or

(c) Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

(6) For purposes of this section, "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

(7) For purposes of this section and except under subsection (8) of this section, "notice" may be provided by one of the following methods:

(a) Written notice;

(b) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. Sec. 7001; or

(c) Substitute notice, if the person or business demonstrates that the cost of providing notice would exceed two hundred fifty thousand

1 dollars, or that the affected class of subject persons to be notified

2 exceeds five hundred thousand, or the person or business does not have

3 sufficient contact information. Substitute notice shall consist of all

4 of the following:

5   (i) E-mail notice when the person or business has an e-mail address

6 for the subject persons;

7   (ii) Conspicuous posting of the notice on the web site page of the

8 person or business, if the person or business maintains one; and

9   (iii) Notification to major statewide media.

10   (8) A person or business that maintains its own notification

11 procedures as part of an information security policy for the treatment

12 of personal information and is otherwise consistent with the timing

13 requirements of this section is in compliance with the notification

14 requirements of this section if the person or business notifies subject

15 persons in accordance with its policies in the event of a breach of

16 security of the system.

17   (9) Any waiver of the provisions of this section is contrary to

18 public policy, and is void and unenforceable.

19   (10)(a) Any customer injured by a violation of this section may

20 institute a civil action to recover damages. A court may award damages

21 up to the actual amount of economic damages or five hundred dollars,

22 whichever is greater.

23   (b) Any business that violates, proposes to violate, or has

24 violated this section may be enjoined.

25   (c) The rights and remedies available under this section are

26 cumulative to each other and to any other rights and remedies available

27 under law.

28   (d) A person or business under this section shall not be required

29 to disclose a technical breach of the security system that does not

30 seem reasonably likely to subject customers to a risk of criminal

31 activity.

32   **Sec. 2.** RCW 42.56.590 and 2005 c 368 s 1 are each amended to read

33 as follows:

34   (1)(a) Any agency that owns or licenses computerized data that

35 includes personal information shall disclose any breach of the security

36 of the system following discovery or notification of the breach in the

37 security of the data to any resident of this state whose unencrypted

personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subsection (3) of this section, or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

(b) For purposes of this section, "agency" means the same as in RCW 42.17.020.

(2) Any agency that maintains computerized data that includes personal information that the agency does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

(3) The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section shall be made after the law enforcement agency determines that it will not compromise the investigation.

(4) For purposes of this section, "breach of the security of the system" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the agency. Good faith acquisition of personal information by an employee or agent of the agency for the purposes of the agency is not a breach of the security of the system when the personal information is not used or subject to further unauthorized disclosure.

(5) For purposes of this section, "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, when either the name or the data elements are not encrypted:

(a) Social security number;

(b) Driver's license number or Washington identification card number; or

(c) Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

1　　(6) For purposes of this section, "personal information" does not
2　include publicly available information that is lawfully made available
3　to the general public from federal, state, or local government records.
4　　(7) For purposes of this section and except under subsection (8) of
5　this section, notice may be provided by one of the following methods:
6　　(a) Written notice;
7　　(b) Electronic notice, if the notice provided is consistent with
8　the provisions regarding electronic records and signatures set forth in
9　15 U.S.C. Sec. 7001; or
10　　(c) Substitute notice, if the agency demonstrates that the cost of
11　providing notice would exceed two hundred fifty thousand dollars, or
12　that the affected class of subject persons to be notified exceeds five
13　hundred thousand, or the agency does not have sufficient contact
14　information. Substitute notice shall consist of all of the following:
15　　(i) E-mail notice when the agency has an e-mail address for the
16　subject persons;
17　　(ii) Conspicuous posting of the notice on the agency's web site
18　page, if the agency maintains one; and
19　　(iii) Notification to major statewide media.
20　　(8) An agency that maintains its own notification procedures as
21　part of an information security policy for the treatment of personal
22　information and is otherwise consistent with the timing requirements of
23　this section is in compliance with the notification requirements of
24　this section if it notifies subject persons in accordance with its
25　policies in the event of a breach of security of the system.
26　　(9) Any waiver of the provisions of this section is contrary to
27　public policy, and is void and unenforceable.
28　　(10)(a) Any customer injured by a violation of this section may
29　institute a civil action to recover damages. A court may award damages
30　up to the actual amount of economic damages or five hundred dollars,
31　whichever is greater.
32　　(b) Any business that violates, proposes to violate, or has
33　violated this section may be enjoined.
34　　(c) The rights and remedies available under this section are
35　cumulative to each other and to any other rights and remedies available
36　under law.
37　　(d) An agency shall not be required to disclose a technical breach

1 of the security system that does not seem reasonably likely to subject
2 customers to a risk of criminal activity.

3 <u>NEW SECTION.</u> **Sec. 3.** A new section is added to chapter 19.86 RCW
4 to read as follows:
5   Any violation of RCW 19.255.010 or 42.56.590 constitutes an unfair
6 or deceptive practice in violation of this chapter.

--- END ---