Z-0165.2

SENATE BILL 5047

State of Washington   64th Legislature   2015 Regular Session

By Senators Braun, Conway, Rivers, Fraser, Kohl-Welles, and Hasegawa; by request of Attorney General

Prefiled 01/07/15.

1   AN ACT Relating to enhancing the protection of consumer financial
2 information; amending RCW 19.255.010 and 42.56.590; and creating a
3 new section.

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

5   NEW SECTION. **Sec. 1.** The legislature recognizes that data
6 breaches of personal information can compromise financial security
7 and be costly to consumers. The legislature intends to strengthen the
8 data breach notification requirements to better safeguard personal
9 information, prevent identity theft, and ensure that the attorney
10 general receives notification when breaches occur so that appropriate
11 action may be taken to protect consumers. The legislature also
12 intends to provide consumers whose personal information has been
13 jeopardized due to a data breach with the information needed to
14 secure financial accounts and make the necessary reports in a timely
15 manner to minimize harm from identity theft.

16   **Sec. 2.** RCW 19.255.010 and 2005 c 368 s 2 are each amended to
17 read as follows:
18   (1) Any person or business that conducts business in this state
19 and that owns or licenses ((computerized)) data that includes
20 personal information shall disclose any breach of the security of the

1 system following discovery or notification of the breach in the
2 security of the data to any resident of this state whose
3 ((unencrypted)) personal information was, or is reasonably believed
4 to have been, acquired by an unauthorized person. ((The disclosure
5 shall be made in the most expedient time possible and without
6 unreasonable delay, consistent with the legitimate needs of law
7 enforcement, as provided in subsection (3) of this section, or any
8 measures necessary to determine the scope of the breach and restore
9 the reasonable integrity of the data system.)) Notice is not required
10 if the breach of the security of the system is not reasonably likely
11 to subject consumers to a risk of criminal activity.

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

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

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

31   (5) For purposes of this section, "personal information" means an
32 individual's first name or first initial and last name in combination
33 with any one or more of the following data elements((, when either
34 the name or the data elements are not encrypted)):
35   (a) Social security number;
36   (b) Driver's license number or Washington identification card
37 number; or
38   (c) Full account number ((or)), credit or debit card number, ((in
39 combination with)) or any required security code, access code, or

1 password that would permit access to an individual's financial
2 account.

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

7   (7) For purposes of this section and except under subsections (8)
8 and (9) of this section, "notice" may be provided by one of the
9 following methods:

10   (a) Written notice;

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

14   (c) Substitute notice, if the person or business demonstrates
15 that the cost of providing notice would exceed two hundred fifty
16 thousand dollars, or that the affected class of subject persons to be
17 notified exceeds five hundred thousand, or the person or business
18 does not have sufficient contact information. Substitute notice shall
19 consist of all of the following:

20   (i) E-mail notice when the person or business has an e-mail
21 address for the subject persons;

22   (ii) Conspicuous posting of the notice on the web site page of
23 the person or business, if the person or business maintains one; and

24   (iii) Notification to major statewide media.

25   (8) A person or business that maintains its own notification
26 procedures as part of an information security policy for the
27 treatment of personal information and is otherwise consistent with
28 the timing requirements of this section is in compliance with the
29 notification requirements of this section if the person or business
30 notifies subject persons in accordance with its policies in the event
31 of a breach of security of the system.

32   (9) A covered entity under the federal health insurance
33 portability and accountability act of 1996, 42 U.S.C. Sec. 1320d et
34 seq., is deemed to have complied with the notice requirements in
35 subsection (1) of this section if it has complied completely with
36 section 13402(f) of the federal health information technology for
37 economic and clinical health act, Public Law 111-5. This subsection
38 may not be construed to exempt a covered entity from any other
39 provision of this section.

1   (10) Any waiver of the provisions of this section is contrary to
2   public policy, and is void and unenforceable.
3   ((+10+)) (11)(a) Any ((customer)) consumer injured by a violation
4   of this section may institute a civil action to recover damages.
5   (b) Any person or business that violates, proposes to violate, or
6   has violated this section may be enjoined.
7   (c) The rights and remedies available under this section are
8   cumulative to each other and to any other rights and remedies
9   available under law.
10   ((d) A person or business under this section shall not be
11   required to disclose a technical breach of the security system that
12   does not seem reasonably likely to subject customers to a risk of
13   criminal activity.))
14   (12) Any person or business that is required to issue
15   notification pursuant to this section shall meet all of the following
16   requirements:
17   (a) The notification must be written in plain language; and
18   (b) The notification must include, at a minimum, the following
19   information:
20   (i) The name and contact information of the reporting person or
21   business subject to this section;
22   (ii) A list of the types of personal information that were or are
23   reasonably believed to have been the subject of a breach; and
24   (iii) The toll-free telephone numbers and addresses of the major
25   credit reporting agencies if the breach exposed personal information.
26   (13) Any person or business that is required to issue a
27   notification pursuant to this section to more than five hundred
28   Washington residents as a result of a single breach shall
29   electronically submit a single sample copy of that security breach
30   notification, excluding any personally identifiable information, to
31   the attorney general. The person or business shall also provide to
32   the attorney general the number of Washington consumers affected by
33   the breach, or an estimate if the exact number is not known.
34   (14) Notification to affected consumers and to the attorney
35   general under this section must be made in the most expedient time
36   possible and without unreasonable delay, no more than thirty calendar
37   days after the breach was discovered, consistent with the legitimate
38   needs of law enforcement as provided in subsection (3) of this
39   section, or any measures necessary to determine the scope of the
40   breach and restore the reasonable integrity of the data system.

1   (15) The legislature finds that the practices covered by this
2   section are matters vitally affecting the public interest for the
3   purpose of applying the consumer protection act, chapter 19.86 RCW. A
4   violation of this chapter is not reasonable in relation to the
5   development and preservation of business and is an unfair or
6   deceptive act in trade or commerce and an unfair method of
7   competition for purposes of applying the consumer protection act,
8   chapter 19.86 RCW.

9   **Sec. 3.** RCW 42.56.590 and 2007 c 197 s 9 are each amended to
10   read as follows:
11   (1)(a) Any agency that owns or licenses ((computerized)) data
12   that includes personal information shall disclose any breach of the
13   security of the system following discovery or notification of the
14   breach in the security of the data to any resident of this state
15   whose ((unencrypted)) personal information was, or is reasonably
16   believed to have been, acquired by an unauthorized person. ((The
17   disclosure shall be made in the most expedient time possible and
18   without unreasonable delay, consistent with the legitimate needs of
19   law enforcement, as provided in subsection (3) of this section, or
20   any measures necessary to determine the scope of the breach and
21   restore the reasonable integrity of the data system.)) Notice is not
22   required if the breach of the security of the system is not
23   reasonably likely to subject consumers to a risk of criminal
24   activity.
25   (b) For purposes of this section, "agency" means the same as in
26   RCW 42.56.010.
27   (2) Any agency that maintains ((computerized)) data that includes
28   personal information that the agency does not own shall notify the
29   owner or licensee of the information of any breach of the security of
30   the data immediately following discovery, if the personal information
31   was, or is reasonably believed to have been, acquired by an
32   unauthorized person.
33   (3) The notification required by this section may be delayed if a
34   law enforcement agency determines that the notification will impede a
35   criminal investigation. The notification required by this section
36   shall be made after the law enforcement agency determines that it
37   will not compromise the investigation.
38   (4) For purposes of this section, "breach of the security of the
39   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) Full account number ((or)), credit or debit card number, ((in
combination with)) or 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 subsections (8)
and (9) 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 agency demonstrates that the cost
of providing notice would exceed two hundred fifty thousand dollars,
or that the affected class of subject persons to be notified exceeds
five hundred thousand, or the agency does not have sufficient contact
information. Substitute notice shall consist of all of the following:

(i) E-mail notice when the agency has an e-mail address for the
subject persons;

(ii) Conspicuous posting of the notice on the agency's web site
page, if the agency maintains one; and

(iii) Notification to major statewide media.

(8) An agency that maintains its own notification procedures as
part of an information security policy for the treatment of personal

1   information and is otherwise consistent with the timing requirements
2   of this section is in compliance with the notification requirements
3   of this section if it notifies subject persons in accordance with its
4   policies in the event of a breach of security of the system.

5   (9) A covered entity under the federal health insurance
6   portability and accountability act of 1996, 42 U.S.C. Sec. 1320d et
7   seq., is deemed to have complied with the notice requirements in
8   subsection (1) of this section if it has complied completely with
9   section 13402(f) of the federal health information technology for
10 economic and clinical health act, Public Law 111-5. This subsection
11 may not be construed to exempt a covered entity from any other
12 provision of this section.

13 (10) Any waiver of the provisions of this section is contrary to
14 public policy, and is void and unenforceable.

15 ((~~(10)~~)) (11)(a) Any ((~~customer~~)) individual injured by a
16 violation of this section may institute a civil action to recover
17 damages.

18 (b) Any ((~~business~~)) agency that violates, proposes to violate,
19 or has violated this section may be enjoined.

20 (c) The rights and remedies available under this section are
21 cumulative to each other and to any other rights and remedies
22 available under law.

23 ((~~(d) An agency shall not be required to disclose a technical~~
24 ~~breach of the security system that does not seem reasonably likely to~~
25 ~~subject customers to a risk of criminal activity.~~))

26 (12) Any agency that is required to issue notification pursuant
27 to this section shall meet all of the following requirements:

28 (a) The notification must be written in plain language; and

29 (b) The notification must include, at a minimum, the following
30 information:

31 (i) The name and contact information of the reporting agency
32 subject to this section;

33 (ii) A list of the types of personal information that were or are
34 reasonably believed to have been the subject of a breach;

35 (iii) The toll-free telephone numbers and addresses of the major
36 credit reporting agencies if the breach exposed personal information.

37 (13) Any agency that is required to issue a notification pursuant
38 to this section to more than five hundred Washington residents as a
39 result of a single breach shall electronically submit a single sample
40 copy of that security breach notification, excluding any personally

identifiable information, to the attorney general. The agency shall also provide to the attorney general the number of Washington residents affected by the breach, or an estimate if the exact number is not known.

(14) Notification to affected individuals and to the attorney general must be made in the most expedient time possible and without unreasonable delay, no more than thirty calendar days after the breach was discovered, 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.

--- END ---

SB 5047