

SHB 1078 - H AMD 79

By Representative Hudgins

ADOPTED AS AMENDED 03/04/2015

1 Strike everything after the enacting clause and insert the
2 following:

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

14

15 **Sec. 2.** RCW 19.255.010 and 2005 c 368 s 2 are each amended to
16 read as follows:

17 (1) Any person or business that conducts business in this state
18 and that owns or licenses ~~((computerized))~~ data that includes
19 personal information shall disclose any breach of the security of
20 the system following discovery or notification of the breach in the
21 security of the data to any resident of this state whose
22 ~~((unencrypted))~~ personal information was, or is reasonably believed
23 to have been, acquired by an unauthorized person and the personal
24 information was not secured. ~~((The disclosure shall be made in the~~
25 ~~most expedient time possible and without unreasonable delay,~~
26 ~~consistent with the legitimate needs of law enforcement, as provided~~
27 ~~in subsection (3) of this section, or any measures necessary to~~

1 ~~determine the scope of the breach and restore the reasonable~~
2 ~~integrity of the data system.))~~ Notice is not required if the breach
3 of the security of the system is not reasonably likely to subject
4 consumers to a risk of harm. The breach of secured personal
5 information must be disclosed if the information acquired and
6 accessed is not secured during a security breach or if the
7 confidential process, encryption key, or other means to decipher the
8 secured information was acquired by an unauthorized person.

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

15 (3) The notification required by this section may be delayed if
16 the data owner or licensee contacts a law enforcement agency after
17 discovery of a breach of the security of the system and a law
18 enforcement agency determines that the notification will impede a
19 criminal investigation. The notification required by this section
20 shall be made after the law enforcement agency determines that it
21 will not compromise the investigation.

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

30 (5) For purposes of this section, "personal information" means
31 an individual's first name or first initial and last name in
32 combination with any one or more of the following data elements(~~(7~~
33 ~~when either the name or the data elements are not encrypted))~~):

34 (a) Social security number;

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

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

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

11 (7) For purposes of this section, "secured" means encrypted in a
12 manner that meets or exceeds the national institute of standards and
13 technology (NIST) standard or is otherwise modified so that the
14 personal information is rendered unreadable, unusable, or
15 undecipherable by an unauthorized person.

16 (8) For purposes of this section and except under subsections
17 ((~~8~~)) (9) and (10) of this section, "notice" may be provided by
18 one of the following methods:

19 (a) Written notice;

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

23 (c) Substitute notice, if the person or business demonstrates
24 that the cost of providing notice would exceed two hundred fifty
25 thousand dollars, or that the affected class of subject persons to
26 be notified exceeds five hundred thousand, or the person or business
27 does not have sufficient contact information. Substitute notice
28 shall consist of all of the following:

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

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

33 (iii) Notification to major statewide media.

34

1 ~~((8))~~ (9) A person or business that maintains its own
2 notification procedures as part of an information security policy
3 for the treatment of personal information and is otherwise
4 consistent with the timing requirements of this section is in
5 compliance with the notification requirements of this section if the
6 person or business notifies subject persons in accordance with its
7 policies in the event of a breach of security of the system.

8 ~~((9))~~ (10) A covered entity under the federal health insurance
9 portability and accountability act of 1996, 42 U.S.C. Sec. 1320d et
10 seq., is deemed to have complied with the requirements of this
11 section with respect to protected health information if it has
12 complied with section 13402 of the federal health information
13 technology for economic and clinical health act, Public Law 111-5 as
14 it existed on the effective date of this section. Covered entities
15 shall notify the attorney general pursuant to subsection (15) of
16 this section in compliance with the timeliness of notification
17 requirements of section 13402 of the federal health information
18 technology for economic and clinical health act, Public Law 111-5 as
19 it existed on the effective date of this section, notwithstanding
20 the notification requirement in subsection (16) of this section.

21 (11) A financial institution under the authority of the office
22 of the comptroller of the currency, the federal deposit insurance
23 corporation, the national credit union administration, or the
24 federal reserve system is deemed to have complied with the
25 requirements of this section with respect to "sensitive customer
26 information" as defined in the interagency guidelines establishing
27 information security standards, 12 C.F.R. Part 30, Appendix B, 12
28 C.F.R. Part 208, Appendix D-2, 12 C.F.R. Part 225, Appendix F, and
29 12 C.F.R. Part 364, Appendix B, and 12 C.F.R. Part 748, Appendices A
30 and B, as they existed on the effective date of this section, if the
31 financial institution provides notice to affected consumers pursuant
32 to the interagency guidelines and the notice complies with the
33 customer notice provisions of the interagency guidelines
34 establishing information security standards and the interagency

1 guidance on response programs for unauthorized access to customer
2 information and customer notice under 12 C.F.R. Part 364 as it
3 existed on the effective date of this section. The entity shall
4 notify the attorney general pursuant to subsection (15) of this
5 section in addition to providing notice to its primary federal
6 regulator.

7 (12) Any waiver of the provisions of this section is contrary to
8 public policy, and is void and unenforceable.

9 ~~((10))~~ (13)(a) Any ~~((customer))~~ consumer injured by a
10 violation of this section may institute a civil action to recover
11 damages.

12 (b) Any person or business that violates, proposes to violate,
13 or has violated this section may be enjoined.

14 (c) The rights and remedies available under this section are
15 cumulative to each other and to any other rights and remedies
16 available under law.

17 ~~((d) A person or business under this section shall not be~~
18 ~~required to disclose a technical breach of the security system that~~
19 ~~does not seem reasonably likely to subject customers to a risk of~~
20 ~~criminal activity.))~~

21 (14) Any person or business that is required to issue
22 notification pursuant to this section shall meet all of the
23 following requirements:

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

25 (b) The notification must include, at a minimum, the following
26 information:

27 (i) The name and contact information of the reporting person or
28 business subject to this section;

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

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

34

1 (15) Any person or business that is required to issue a
2 notification pursuant to this section to more than five hundred
3 Washington residents as a result of a single breach shall, by the
4 time notice is provided to affected consumers, electronically submit
5 a single sample copy of that security breach notification, excluding
6 any personally identifiable information, to the attorney general.
7 The person or business shall also provide to the attorney general
8 the number of Washington consumers affected by the breach, or an
9 estimate if the exact number is not known.

10 (16) Notification to affected consumers and to the attorney
11 general under this section must be made in the most expedient time
12 possible and without unreasonable delay, no more than forty-five
13 calendar days after the breach was discovered, unless at the request
14 of law enforcement as provided in subsection (3) of this section, or
15 due to any measures necessary to determine the scope of the breach
16 and restore the reasonable integrity of the data system.

17 (17) The attorney general may bring an action in the name of the
18 state, or as parens patriae on behalf of persons residing in the
19 state, to enforce this section. For actions brought by the attorney
20 general to enforce this section, the legislature finds that the
21 practices covered by this section are matters vitally affecting the
22 public interest for the purpose of applying the consumer protection
23 act, chapter 19.86 RCW. For actions brought by the attorney general
24 to enforce this section, a violation of this section is not
25 reasonable in relation to the development and preservation of
26 business and is an unfair or deceptive act in trade or commerce and
27 an unfair method of competition for purposes of applying the
28 consumer protection act, chapter 19.86 RCW. An action to enforce
29 this section may not be brought under RCW 19.86.090.

30

31 **Sec. 3.** RCW 42.56.590 and 2007 c 197 s 9 are each amended to
32 read as follows:

33 (1)(a) Any agency that owns or licenses (~~computerized~~) data
34 that includes personal information shall disclose any breach of the

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

17 (b) For purposes of this section, "agency" means the same as in
18 RCW 42.56.010.

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

25 (3) The notification required by this section may be delayed if
26 the data owner or licensee contacts a law enforcement agency after
27 discovery of a breach of the security of the system and a law
28 enforcement agency determines that the notification will impede a
29 criminal investigation. The notification required by this section
30 shall be made after the law enforcement agency determines that it
31 will not compromise the investigation.

32 (4) For purposes of this section, "breach of the security of the
33 system" means unauthorized acquisition of (~~computerized~~) data that
34 compromises the security, confidentiality, or integrity of personal

1 information maintained by the agency. Good faith acquisition of
2 personal information by an employee or agent of the agency for the
3 purposes of the agency is not a breach of the security of the system
4 when the personal information is not used or subject to further
5 unauthorized disclosure.

6 (5) For purposes of this section, "personal information" means
7 an individual's first name or first initial and last name in
8 combination with any one or more of the following data elements(~~(7~~
9 ~~when either the name or the data elements are not encrypted)~~):

10 (a) Social security number;

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

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

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

21 (7) For purposes of this section, "secured" means encrypted in a
22 manner that meets or exceeds the national institute of standards and
23 technology (NIST) standard or is otherwise modified so that the
24 personal information is rendered unreadable, unusable, or
25 undecipherable by an unauthorized person.

26 (8) For purposes of this section and except under subsections
27 (~~(+8)~~) (9) and (10) of this section, notice may be provided by one
28 of the following methods:

29 (a) Written notice;

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

33 (c) Substitute notice, if the agency demonstrates that the cost
34 of providing notice would exceed two hundred fifty thousand dollars,

1 or that the affected class of subject persons to be notified exceeds
2 five hundred thousand, or the agency does not have sufficient
3 contact information. Substitute notice shall consist of all of the
4 following:

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

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

9 (iii) Notification to major statewide media.

10 ~~((+8))~~ (9) An agency that maintains its own notification
11 procedures as part of an information security policy for the
12 treatment of personal information and is otherwise consistent with
13 the timing requirements of this section is in compliance with the
14 notification requirements of this section if it notifies subject
15 persons in accordance with its policies in the event of a breach of
16 security of the system.

17 ~~((+9))~~ (10) A covered entity under the federal health insurance
18 portability and accountability act of 1996, 42 U.S.C. Sec. 1320d et
19 seq., is deemed to have complied with the requirements of this
20 section with respect to protected health information if it has
21 complied with section 13402 of the federal health information
22 technology for economic and clinical health act, Public Law 111-5 as
23 it existed on the effective date of this section. Covered entities
24 shall notify the attorney general pursuant to subsection (14) of
25 this section in compliance with the timeliness of notification
26 requirements of section 13402 of the federal health information
27 technology for economic and clinical health act, Public Law 111-5 as
28 it existed on the effective date of this section, notwithstanding
29 the notification requirement in subsection (15) of this section.

30 (11) Any waiver of the provisions of this section is contrary to
31 public policy, and is void and unenforceable.

32 ~~((+10))~~ (12)(a) Any ~~((customer))~~ individual injured by a
33 violation of this section may institute a civil action to recover
34 damages.

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

3 (c) The rights and remedies available under this section are
4 cumulative to each other and to any other rights and remedies
5 available under law.

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

9 (13) Any agency that is required to issue notification pursuant
10 to this section shall meet all of the following requirements:

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

12 (b) The notification must include, at a minimum, the following
13 information:

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

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

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

21 (14) Any agency that is required to issue a notification
22 pursuant to this section to more than five hundred Washington
23 residents as a result of a single breach shall, by the time notice
24 is provided to affected individuals, electronically submit a single
25 sample copy of that security breach notification, excluding any
26 personally identifiable information, to the attorney general. The
27 agency shall also provide to the attorney general the number of
28 Washington residents affected by the breach, or an estimate if the
29 exact number is not known.

30 (15) Notification to affected individuals and to the attorney
31 general must be made in the most expedient time possible and without
32 unreasonable delay, no more than forty-five calendar days after the
33 breach was discovered, unless at the request of law enforcement as
34 provided in subsection (3) of this section, or due to any measures

1 necessary to determine the scope of the breach and restore the
2 reasonable integrity of the data system."

EFFECT:

- Eliminates the HIPAA exemption requirement that the Attorney General confer with the Secretary of Health and Human Services prior to commencing action under the Consumer Protection Act.
- Changes the timeline of when notification for a data breach involving more than five hundred Washington residents must be provided from 45 days to 60 days under the HIPAA exemption.
- Adds the National Credit Union Association to the GLBA exemption.
- Changes the exception to the 45 day notification requirement from unless "consistent with" any measures necessary to "due to" any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

--- END ---

16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34