SHB 1078 - H AMD **79**
By Representative Hudgins

ADOPTED AS AMENDED 03/04/2015

Strike everything after the enacting clause and insert the following:

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

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

(1) Any person or business that conducts business in this state and that owns or licenses ((~~computerized~~)) data that includes personal information shall disclose any breach of the security of the system following discovery or notification of the breach in the 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 and the personal information was not secured. ((~~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.~~)) Notice is not required if the breach of the security of the system is not reasonably likely to subject consumers to a risk of harm. The breach of secured personal information must be disclosed if the information acquired and accessed is not secured during a security breach or if the confidential process, encryption key, or other means to decipher the secured information was acquired by an unauthorized person.

(2) Any person or business that maintains ((~~computerized~~)) data that 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 the data owner or licensee contacts a law enforcement agency after discovery of a breach of the security of the system and 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) 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, "secured" means encrypted in a manner that meets or exceeds the national institute of standards and technology (NIST) standard or is otherwise modified so that the personal information is rendered unreadable, unusable, or undecipherable by an unauthorized person.

(8) For purposes of this section and except under subsections ((~~(8)~~)) (9) and (10) 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 dollars, or that the affected class of subject persons to be notified exceeds five hundred thousand, or the person or business does not have sufficient contact information. Substitute notice shall consist of all of the following:

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

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

(iii) Notification to major statewide media.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

security of the system following discovery or notification of the breach in the 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 and the personal information was not secured. ((~~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.~~)) Notice is not required if the breach of the security of the system is not reasonably likely to subject consumers to a risk of harm. The breach of secured personal information must be disclosed if the information acquired and accessed is not secured during a security breach or if the confidential process, encryption key, or other means to decipher the secured information was acquired by an unauthorized person.

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

(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 the data owner or licensee contacts a law enforcement agency after discovery of a breach of the security of the system and 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) 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, "secured" means encrypted in a manner that meets or exceeds the national institute of standards and technology (NIST) standard or is otherwise modified so that the personal information is rendered unreadable, unusable, or undecipherable by an unauthorized person.

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

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

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

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

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

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

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

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

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

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

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

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

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

(14) Any agency that is required to issue a notification pursuant to this section to more than five hundred Washington residents as a result of a single breach shall, by the time notice is provided to affected individuals, electronically submit a single sample 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.

(15) 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 forty-five calendar days after the breach was discovered, unless at the request of law enforcement as provided in subsection (3) of this section, or due to any measures

necessary to determine the scope of the breach and restore the 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 ---