

---

**SUBSTITUTE HOUSE BILL 1078**

---

**State of Washington**

**64th Legislature**

**2015 Regular Session**

**By** House Technology & Economic Development (originally sponsored by Representatives Hudgins, Morris, Robinson, Kirby, Gregerson, Stanford, Ryu, Magendanz, and Pollet; by request of Attorney General)

READ FIRST TIME 02/20/15.

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 and the personal  
5 information was not secured. (~~The disclosure shall be made in the~~  
6 ~~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 (2) Any person or business that maintains (~~computerized~~) data  
18 that includes personal information that the person or business does  
19 not own shall notify the owner or licensee of the information of any  
20 breach of the security of the data immediately following discovery,  
21 if the personal information was, or is reasonably believed to have  
22 been, acquired by an unauthorized person.

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

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

38 (5) For purposes of this section, "personal information" means an  
39 individual's first name or first initial and last name in combination

1 with any one or more of the following data elements(~~(, when either~~  
2 ~~the name or the data elements are not encrypted)~~):

3 (a) Social security number;

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

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

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

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

19 (8) For purposes of this section and except under subsections  
20 ((+8)) (9) and (10) of this section, "notice" may be provided by one  
21 of the following methods:

22 (a) Written notice;

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

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

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

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

36 (iii) Notification to major statewide media.

37 ((+8)) (9) A person or business that maintains its own  
38 notification procedures as part of an information security policy for  
39 the treatment of personal information and is otherwise consistent  
40 with the timing requirements of this section is in compliance with

1 the notification requirements of this section if the person or  
2 business notifies subject persons in accordance with its policies in  
3 the event of a breach of security of the system.

4 ~~((9))~~ (10) A covered entity under the federal health insurance  
5 portability and accountability act of 1996, 42 U.S.C. Sec. 1320d et  
6 seq., is deemed to have complied with the requirements of this  
7 section with respect to protected health information if it has  
8 complied with section 13402 of the federal health information  
9 technology for economic and clinical health act, Public Law 111-5 as  
10 it existed on the effective date of this section. Covered entities  
11 shall notify the attorney general pursuant to subsection (15) of this  
12 section. Prior to commencing an action against a covered entity  
13 pursuant to subsection (17) of this section, the attorney general  
14 shall confer with the secretary of health and human services, and the  
15 attorney general may not commence such action if the secretary  
16 confirms that the covered entity complied with section 13402 of the  
17 federal health information technology for economic and clinical  
18 health act, Public Law 111-5 as it existed on the effective date of  
19 this section.

20 (11) A financial institution under the authority of the office of  
21 the comptroller of the currency, the federal deposit insurance  
22 corporation, or the federal reserve system is deemed to have complied  
23 with the requirements of this section with respect to "sensitive  
24 customer information" as defined in the interagency guidelines  
25 establishing information security standards, 12 C.F.R. Part 30,  
26 Appendix B, 12 C.F.R. Part 208, Appendix D-2, 12 C.F.R. Part 225,  
27 Appendix F, and 12 C.F.R. Part 364, Appendix B, as they existed on  
28 the effective date of this section, if the financial institution  
29 provides notice to affected consumers pursuant to the interagency  
30 guidelines and the notice complies with the customer notice  
31 provisions of the interagency guidelines establishing information  
32 security standards and the interagency guidance on response programs  
33 for unauthorized access to customer information and customer notice  
34 under 12 C.F.R. Part 364 as it existed on the effective date of this  
35 section. The entity shall notify the attorney general pursuant to  
36 subsection (15) of this section in addition to providing notice to  
37 its primary federal regulator.

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

1       ~~((10))~~ (13)(a) Any ~~((customer))~~ consumer injured by a violation  
2 of this section may institute a civil action to recover damages.

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

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

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

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

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

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

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

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

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

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

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

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

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

16       (1)(a) Any agency that owns or licenses (~~computerized~~) data  
17 that includes personal information shall disclose any breach of the  
18 security of the system following discovery or notification of the  
19 breach in the security of the data to any resident of this state  
20 whose (~~unencrypted~~) personal information was, or is reasonably  
21 believed to have been, acquired by an unauthorized person and the  
22 personal information was not secured. ((The disclosure shall be made  
23 in the most expedient time possible and without unreasonable delay,  
24 consistent with the legitimate needs of law enforcement, as provided  
25 in subsection (3) of this section, or any measures necessary to  
26 determine the scope of the breach and restore the reasonable  
27 integrity of the data system.)) Notice is not required if the breach  
28 of the security of the system is not reasonably likely to subject  
29 consumers to a risk of harm. The breach of secured personal  
30 information must be disclosed if the information acquired and  
31 accessed is not secured during a security breach or if the  
32 confidential process, encryption key, or other means to decipher the  
33 secured information was acquired by an unauthorized person.

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

36       (2) Any agency that maintains (~~computerized~~) data that includes  
37 personal information that the agency does not own shall notify the  
38 owner or licensee of the information of any breach of the security of  
39 the data immediately following discovery, if the personal information

1 was, or is reasonably believed to have been, acquired by an  
2 unauthorized person.

3 (3) The notification required by this section may be delayed if  
4 the data owner or licensee contacts a law enforcement agency after  
5 discovery of a breach of the security of the system and a law  
6 enforcement agency determines that the notification will impede a  
7 criminal investigation. The notification required by this section  
8 shall be made after the law enforcement agency determines that it  
9 will not compromise the investigation.

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

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

22 (a) Social security number;

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

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

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

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

38 (8) For purposes of this section and except under subsections  
39 ((~~8~~)) (9) and (10) of this section, notice may be provided by one  
40 of the following methods:

1 (a) Written notice;

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

5 (c) Substitute notice, if the agency demonstrates that the cost  
6 of providing notice would exceed two hundred fifty thousand dollars,  
7 or that the affected class of subject persons to be notified exceeds  
8 five hundred thousand, or the agency does not have sufficient contact  
9 information. Substitute notice shall consist of all of the following:

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

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

14 (iii) Notification to major statewide media.

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

22 ~~((+9))~~ (10) A covered entity under the federal health insurance  
23 portability and accountability act of 1996, 42 U.S.C. Sec. 1320d et  
24 seq., is deemed to have complied with the requirements of this  
25 section with respect to protected health information if it has  
26 complied with 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. Covered entities  
29 shall notify the attorney general pursuant to subsection (14) of this  
30 section.

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

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

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

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



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

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

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

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

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

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

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

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

24       (15) Notification to affected individuals and to the attorney  
25 general must be made in the most expedient time possible and without  
26 unreasonable delay, no more than forty-five calendar days after the  
27 breach was discovered, unless at the request of law enforcement as  
28 provided in subsection (3) of this section, or consistent with any  
29 measures necessary to determine the scope of the breach and restore  
30 the reasonable integrity of the data system.

--- END ---