

CERTIFICATION OF ENROLLMENT

**SUBSTITUTE SENATE BILL 6043**

Chapter 368, Laws of 2005

59th Legislature  
2005 Regular Session

PERSONAL INFORMATION--NOTICE OF SECURITY BREACHES

EFFECTIVE DATE: 7/24/05

Passed by the Senate March 8, 2005  
YEAS 47 NAYS 0

BRAD OWEN

\_\_\_\_\_  
**President of the Senate**

Passed by the House April 12, 2005  
YEAS 97 NAYS 1

FRANK CHOPP

\_\_\_\_\_  
**Speaker of the House of Representatives**

Approved May 10, 2005.

CHRISTINE GREGOIRE  
\_\_\_\_\_  
**Governor of the State of Washington**

CERTIFICATE

I, Thomas Hoemann, Secretary of the Senate of the State of Washington, do hereby certify that the attached is **SUBSTITUTE SENATE BILL 6043** as passed by the Senate and the House of Representatives on the dates hereon set forth.

THOMAS HOEMANN

\_\_\_\_\_  
**Secretary**

FILED

May 10, 2005 - 9:40 a.m.

**Secretary of State  
State of Washington**

---

**SUBSTITUTE SENATE BILL 6043**

---

Passed Legislature - 2005 Regular Session

**State of Washington                      59th Legislature                      2005 Regular Session**

**By** Senate Committee on Financial Institutions, Housing & Consumer Protection (originally sponsored by Senators Brandland, Fairley, Benson, Keiser, Schmidt, Spanel, Benton, Franklin, Berkey, Kohl-Welles and Rasmussen)

READ FIRST TIME 03/02/05.

1            AN ACT Relating to breaches of security that compromise personal  
2 information; adding a new section to chapter 42.17 RCW; and adding a  
3 new chapter to Title 19 RCW.

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

5            NEW SECTION.    **Sec. 1.** A new section is added to chapter 42.17 RCW  
6 under the subchapter heading "public records" to read as follows:

7            (1)(a) Any agency that owns or licenses computerized data that  
8 includes personal information shall disclose any breach of the security  
9 of the system following discovery or notification of the breach in the  
10 security of the data to any resident of this state whose unencrypted  
11 personal information was, or is reasonably believed to have been,  
12 acquired by an unauthorized person. The disclosure shall be made in  
13 the most expedient time possible and without unreasonable delay,  
14 consistent with the legitimate needs of law enforcement, as provided in  
15 subsection (3) of this section, or any measures necessary to determine  
16 the scope of the breach and restore the reasonable integrity of the  
17 data system.

18            (b) For purposes of this section, "agency" means the same as in RCW  
19 42.17.020.

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

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

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

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

24 (a) Social security number;

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

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

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

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

35 (a) Written notice;

36 (b) Electronic notice, if the notice provided is consistent with  
37 the provisions regarding electronic records and signatures set forth in  
38 15 U.S.C. Sec. 7001; or

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

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

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

10 (iii) Notification to major statewide media.

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

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

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

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

29 NEW SECTION. **Sec. 2.** (1) Any person or business that conducts  
30 business in this state and that owns or licenses computerized data that  
31 includes personal information shall disclose any breach of the security  
32 of the system following discovery or notification of the breach in the  
33 security of the data to any resident of this state whose unencrypted  
34 personal information was, or is reasonably believed to have been,  
35 acquired by an unauthorized person. The disclosure shall be made in  
36 the most expedient time possible and without unreasonable delay,  
37 consistent with the legitimate needs of law enforcement, as provided in

1 subsection (3) of this section, or any measures necessary to determine  
2 the scope of the breach and restore the reasonable integrity of the  
3 data system.

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

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

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

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

27 (a) Social security number;

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

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

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

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

38 (a) Written notice;

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

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

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

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

14 (iii) Notification to major statewide media.

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

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

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

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

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

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

35 NEW SECTION. **Sec. 3.** Section 2 of this act constitutes a new

1 chapter in Title 19 RCW.

Passed by the Senate March 8, 2005.

Passed by the House April 12, 2005.

Approved by the Governor May 10, 2005.

Filed in Office of Secretary of State May 10, 2005.