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.

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

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

NEW SECTION. **Sec. 1.** A new section is added to chapter 42.17 RCW under the subchapter heading "public records" 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. 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.

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

(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 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) Account number or credit or debit card number, in combination with 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 subsection (8) 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 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) Any waiver of the provisions of this section is contrary to public policy, and is void and unenforceable.

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

(b) Any 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) 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.

NEW SECTION. **Sec. 2.** (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. 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.

(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 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) Account number or credit or debit card number, in combination with 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 subsection (8) 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) 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) Any waiver of the provisions of this section is contrary to public policy, and is void and unenforceable.

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

(b) Any 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.

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

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.