

---

SENATE BILL 6425

---

State of Washington                      60th Legislature                      2008 Regular Session

By Senators Franklin, Benton, Prentice, and Rasmussen

Read first time 01/16/08.              Referred to Committee on Financial  
Institutions & Insurance.

1            AN ACT Relating to personal information associated with debit and  
2 credit cards issued by financial institutions; amending RCW 19.255.010;  
3 adding new sections to chapter 19.255 RCW; creating new sections; and  
4 providing an effective date.

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

6            NEW SECTION.    **Sec. 1.** In 2005, the Washington state legislature  
7 passed data breach legislation that requires any person or business  
8 that conducts business in this state or that owns or licenses  
9 computerized data that includes consumer personal information to  
10 disclose any breach of the security of the system following discovery  
11 or notification of the breach in the security of the data to Washington  
12 state residents whose unencrypted personal information was, or is  
13 reasonably believed to have been, acquired by an unauthorized person.  
14 Because persons or businesses who have allowed a breach to occur rarely  
15 have the information necessary to contact affected consumers, financial  
16 institutions are called upon to notify affected consumers about the  
17 data breach.

18            This notification process creates reoccurring financial and  
19 operational issues when information custodians fail to safeguard

1 consumer personal information. In the aftermath of a system breach  
2 that results in compromised debit and credit card information, card-  
3 issuing financial institutions incur significant costs in determining  
4 the nature and scope of the breach, communicating with consumers,  
5 absorbing losses due to unauthorized use of cards or other personal  
6 information, ongoing fraud monitoring costs to protect against future  
7 fraud, and the costs associated with reissuing cards that have been  
8 compromised as a result of the breach.

9 It is the legislature's intent to encourage financial institutions  
10 to communicate with compromised consumers and take steps to protect  
11 consumers from fraud and harm by creating a direct cause of action for  
12 financial institutions against data custodians that unnecessarily  
13 retain consumer personal information or fail to meet rudimentary  
14 precautions designed to protect consumer personal information.

15 NEW SECTION. **Sec. 2.** The definitions in this section apply  
16 throughout this chapter unless the context clearly requires otherwise.

17 (1) "Access device" means a card or device issued by a financial  
18 institution that contains a magnetic stripe, microprocessor chip, radio  
19 frequency identification, or other means for storage of information  
20 that includes, but is not limited to, a credit card, debit card, or  
21 stored value card.

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

30 (3) "Financial institution" has the same meaning as in RCW  
31 30.22.040.

32 (4) Except under RCW 19.255.010(4), "notice" may be provided by one  
33 of the following methods:

34 (a) Written notice;

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

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

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

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

11 (iii) Notification to major statewide media.

12 (5)(a) "Personal information" means an individual's first name or  
13 first initial and last name in combination with any one or more of the  
14 following data elements, when either the name or the data elements are  
15 not encrypted:

16 (i) Social security number;

17 (ii) Driver's license number or Washington identification card  
18 number; or

19 (iii) Account number or credit or debit card number, in combination  
20 with any required security code, access code, or password that would  
21 permit access to an individual's financial account.

22 (b) "Personal information" does not include publicly available  
23 information that is lawfully made available to the general public from  
24 federal, state, or local government records.

25 NEW SECTION. **Sec. 3.** Any person or business conducting business  
26 in Washington that accepts an access device in connection with a  
27 transaction shall dispose of personal information associated with the  
28 access device subsequent to the authorization of the transaction  
29 expeditiously and within a reasonable period of time.

30 NEW SECTION. **Sec. 4.** Any person or business that, in the regular  
31 course of business and in connection with an access device, collects or  
32 stores personal information must comply with payment card industry data  
33 security standards established by the PCI security standards council.

34 NEW SECTION. **Sec. 5.** (1) A financial institution may bring an

1 action against a person or business that has experienced a breach of  
2 the security of the system if, at the time of the breach, the person or  
3 business was in violation of section 3 or 4 of this act.

4 (2)(a) Before filing an action under subsection (1) of this  
5 section, a financial institution must provide to the person or business  
6 written notice requesting that the person or business provide  
7 certification or an assessment of the person's or business's compliance  
8 with payment card industry data security standards, which must be  
9 issued by a payment card industry-approved auditor or another person  
10 authorized to issue that certification or assessment under payment card  
11 industry data security standards.

12 (b) The court shall, on motion, dismiss with prejudice an action  
13 brought under this section if the person or business provides to the  
14 financial institution the certification of compliance required under  
15 (a) of this subsection not later than thirty days after receiving the  
16 notice.

17 (3) A presumption that a person or business has complied with  
18 section 4 of this act exists if:

19 (a) The person or business contracts for or otherwise uses the  
20 services of a third party to collect, maintain, or store sensitive  
21 personal information in connection with an access device;

22 (b) The person or business requires that the third party attest to  
23 or offer proof of compliance with payment card industry data security  
24 standards; and

25 (c) The person or business contractually requires the third party's  
26 continued compliance with payment card industry data security  
27 standards.

28 NEW SECTION. **Sec. 6.** Notwithstanding any other provision of law,  
29 a financial institution that brings an action under section 3 or 4 of  
30 this act may obtain actual damages arising from the violation. Actual  
31 damages include any cost incurred by the financial institution in  
32 connection with:

33 (1) The cancellation or reissuance of an access device affected by  
34 the breach;

35 (2) The closing of a deposit, transaction, share draft, or other  
36 account affected by the breach and any action to stop payment or block  
37 a transaction with respect to the account;

1 (3) The opening or reopening of a deposit, transaction, share  
2 draft, or other account affected by the breach;

3 (4) A refund or credit made to an account holder to cover the cost  
4 of any unauthorized transaction related to the breach;

5 (5) The notification of account holders affected by the breach;

6 (6) Credit monitoring services on accounts affected by the breach  
7 for a period of one year from the time the financial institution is  
8 notified of the breach; and

9 (7) Reasonable attorneys' fees and costs associated with the  
10 action.

11 **Sec. 7.** RCW 19.255.010 and 2005 c 368 s 2 are each amended to read  
12 as follows:

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

24 (2) Any person or business that maintains computerized data that  
25 includes personal information that the person or business does not own  
26 shall notify the owner or licensee of the information of any breach of  
27 the security of the data immediately following discovery, if the  
28 personal information was, or is reasonably believed to have been,  
29 acquired by an unauthorized person.

30 (3) The notification required by this section may be delayed if a  
31 law enforcement agency determines that the notification will impede a  
32 criminal investigation. The notification required by this section  
33 shall be made after the law enforcement agency determines that it will  
34 not compromise the investigation.

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

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

6 (5) For purposes of this section, "personal information" means an  
7 individual's first name or first initial and last name in combination  
8 with any one or more of the following data elements, when either the  
9 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) Account number or credit or debit card number, in combination  
14 with any required security code, access code, or password that would  
15 permit access to an individual's financial account.

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

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

21 (a) Written notice;

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

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

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

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

35 (iii) Notification to major statewide media.

36 (8)) A person or business that maintains its own notification  
37 procedures as part of an information security policy for the treatment  
38 of personal information and is otherwise consistent with the timing

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

5 ~~((+9))~~ (5) Any waiver of the provisions of this section is  
6 contrary to public policy, and is void and unenforceable.

7 ~~((+10))~~ (6)(a) Any customer injured by a violation of this section  
8 may institute a civil action to recover damages.

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

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

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

18 NEW SECTION. **Sec. 8.** Sections 2 through 6 of this act are each  
19 added to chapter 19.255 RCW.

20 NEW SECTION. **Sec. 9.** This act applies prospectively and not  
21 retroactively. It applies only to causes of action that arise on or  
22 after January 1, 2009.

23 NEW SECTION. **Sec. 10.** This act takes effect January 1, 2009.

--- END ---