H-3929.4

HOUSE BILL 2838

State of Washington 60th Legislature 2008 Regular Session

By Representatives Williams, Roach, Kirby, Simpson, Ericks, and Haler

Read first time 01/16/08. Referred to Committee on Insurance, Financial Services & Consumer Protection.

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

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

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

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

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

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

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

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

(2) "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.

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

(4) Except under RCW 19.255.010(4), "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.

(5)(a) "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:

(i) Social security number;

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

(iii) 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.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Sec. 7. 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. 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)~~)) (5) Any waiver of the provisions of this section is contrary to public policy, and is void and unenforceable.

((~~(10)~~)) (6)(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. 8.** Sections 2 through 6 of this act are each added to chapter 19.255 RCW.

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

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

--- END ---