FIRST REGULAR SESSION

SENATE BILL NO. 207

95TH GENERAL ASSEMBLY

INTRODUCED BY SENATOR RUPP.

Read 1st time January 15, 2009, and ordered printed.

TERRY L. SPIELER, Secretary.

0794S.01I

Unofficial Bill Copy

AN ACT

To amend chapter 407, RSMo, by adding thereto one new section relating to data security breaches.

Be it enacted by the General Assembly of the State of Missouri, as follows:

Section A. Chapter 407, RSMo, is amended by adding thereto one new section, to be known as section 407.1500, to read as follows:

407.1500. 1. As used in this section, the following terms mean:

(1) "Breach of security" or "breach", unauthorized acquisition of personal information maintained in computerized form by a person that compromises the security, confidentiality, or integrity of the personal information. Good faith acquisition of personal information by a person or that person's employee or agent for a legitimate purpose of that person is not a breach of security, provided that the personal information is not used in violation of applicable law or in a manner that harms or poses an actual threat to the security, confidentiality, or integrity of the personal information;

(2) "Consumer", an individual who is a resident of this state;

(3) "Consumer reporting agency", the same as defined by the federal Fair Credit Reporting Act, 15 U.S.C. Section 1681a;

(4) "Encryption", the use of an algorithmic process to transform data into a form in which the data is rendered unreadable or unusable without the use of a confidential process or key;

(5) "Health insurance information", an individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals records;

(6) "Medical information", any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional;

(7) "Owns or licenses" includes, but is not limited to, personal information that a business retains as part of the internal customer account of the business or for the purpose of using the information in transactions with the person to whom the information relates;

(8) "Person", any individual, corporation, business trust, estate, trust, partnership, limited liability company, association, joint venture, government, governmental subdivision, governmental agency, governmental instrumentality, public corporation, or any other legal or commercial entity;

(9) "Personal information", an individual's first name or first initial and last name in combination with any one or more of the following data elements that relate to the individual if any of the data elements are not encrypted, redacted, or otherwise altered by any method or technology in such a manner that the name or data elements are unreadable:

(a) Social Security number;

(b) Driver's license number or other unique identification number created or collected by a government body;

(c) Financial account number, credit card number, 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;

(d) Account number, credit, debit, or other number identifying a payment device, if circumstances exist in which such a number could be used without additional identifying information, access codes, or passwords;

(e) Account passwords or personal identification numbers (PINs) or other access codes;

(f) Unique electronic identifier or routing code, in combination with any required security code, access code, or password that would permit access to an individual's financial account;

(g) Unique biometric data, such as a fingerprint, retina or iris image, or other unique physical representation or digital representation of biometric data;

Unofficial Bill Copy

(h) Medical information;

(i) Health insurance information; or

(j) The individual's digitized or other electronic signature.

"Personal information" does not include information that is lawfully obtained from publicly available sources, or from federal, state, or local government records lawfully made available to the general public;

(10) "Redacted", altered or truncated such that no more than four digits of a social security number or the last four digits of a driver's license number, state identification card number, or account number is accessible as part of the personal information.

2. (1) Any person that acquires, owns, or licenses personal information of residents of Missouri or any person that conducts business in Missouri that owns or licenses personal information in any form shall provide notice to the affected consumer that there has been a breach of security following discovery or notification of the breach. The disclosure notification shall be:

(a) Made without unreasonable delay;

(b) Consistent with the legitimate needs of law enforcement, as provided in this section; and

(c) Consistent with any measures necessary to determine sufficient contact information and to determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the data system.

(2) Any person that maintains or possesses records or data containing personal information of residents of Missouri that the person does not own or license, or any person that conducts business in Missouri that maintains or possesses records or data containing personal information that the person does not own or license, shall notify the owner or licensee of the information of any breach of security immediately following discovery of the breach, consistent with the legitimate needs of law enforcement as provided in this section.

(3) The notice required by this section shall be delayed if a law enforcement agency informs the person that notification may impede a criminal investigation or jeopardize national or homeland security, provided that such request by law enforcement is made in writing or the person documents such request contemporaneously in writing, including the name of the law enforcement officer making the request

Unofficial Bill Copy

and the officer's law enforcement agency engaged in the investigation. The notice required by this section shall be provided without unreasonable delay after the law enforcement agency communicates to the person its determination that notice will no longer impede the investigation or jeopardize national or homeland security.

(4) The notice required by this section shall be clear and conspicuous. The notice shall at minimum include a description of the following:

(a) The incident in general terms and the approximate date of the breach of security;

(b) The type of personal information that was obtained as a result of the breach of security;

(c) The general acts of the business to protect the personal information from further unauthorized access;

(d) A telephone number that the affected consumer may call for further information and assistance, if one exists;

(e) Contact information for consumer reporting agencies;

(f) Advice that directs the affected consumer to remain vigilant by reviewing account statements and monitoring free credit reports.

(5) Notwithstanding subdivisions (1) and (2) of this subsection, notification is not required if, after an appropriate investigation or after consultation with the relevant federal, state, or local agencies responsible for law enforcement, the person determines that no reasonable likelihood of financial harm to the consumers whose personal information has been acquired has resulted or will result from the breach. Such a determination shall be documented in writing and the documentation shall be maintained for five years.

(6) For purposes of this section, notice to affected consumers shall be provided by one of the following methods:

(a) Written notice;

(b) Electronic notice for those consumers for whom the person has a valid e-mail address and who have agreed to receive communications electronically, if the notice provided is consistent with the provisions of 15 U.S.C. Section 7001 regarding electronic records and signatures for notices legally required to be in writing;

(c) Telephonic notice, if such contact is made directly with the affected consumers;

Unofficial Bill Copy

(d) Substitute notice, if:

a. The person demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars; or

b. The class of affected consumers to be notified exceeds five hundred thousand; or

c. If the person does not have sufficient contact information or consent to satisfy paragraphs (a), (b), or (c) of this subdivision, for only those affected consumers without sufficient contact information or consent; or

d. If the person is unable to identify particular affected consumers, for only those unidentifiable consumers.

(7) Substitute notice under paragraph (d) of subdivision (6) of this subsection shall consist of all the following:

a. E-mail notice when the person has an electronic mail address for the affected consumer;

b. Conspicuous posting of the notice or a link to the notice on the Internet web site of the person if the person maintains an Internet web site; and

c. Notification to major statewide media.

(8) In the event a person provides notice to more than one thousand persons at one time pursuant to this section, the person shall notify, without unreasonable delay, the attorney general's office and all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in 15 U.S.C. Section 1681a(p), of the timing, distribution, and content of the notice.

3. (1) A person that maintains its own notice procedures as part of an information security policy for the treatment of personal information, and whose procedures are otherwise consistent with the timing requirements of this section, is deemed to be in compliance with the notice requirements of this section if the person notifies affected consumers in accordance with its policies in the event of a breach of security of the system.

(2) A person that is regulated by state or federal law and that maintains procedures for a breach of the security of the system pursuant to the laws, rules, regulations, guidances, or guidelines established by its primary or functional state or federal regulator is deemed to be in compliance with this section if the person notifies

Unofficial Bill Copy

affected consumers in accordance with the maintained procedures when a breach occurs.

(3) A financial institution that is subject to and in compliance with the Federal Interagency Guidance Response Programs for Unauthorized Access to Customer Information and Customer Notice, issued on March 29, 2005, by the board of governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision, and any revisions, additions, or substitutions relating to said interagency guidance, shall be deemed to be in compliance with this section.

4. The attorney general may bring an action to obtain actual damages for a willful and knowing violation of this section and may seek a civil penalty not to exceed one hundred fifty thousand dollars per breach of the security of the system or series of breaches of a similar nature that are discovered in a single investigation.

Unofficial Bill Copy