HOUSE BILL NO. 74

INTRODUCED BY R. LYNCH

BY REQUEST OF THE DEPARTMENT OF JUSTICE

A BILL FOR AN ACT ENTITLED: "AN ACT REVISING DATA SYSTEM SECURITY BREACH NOTIFICATION LAWS; REQUIRING THE ATTORNEY GENERAL AND INSURANCE COMMISSIONER TO BE NOTIFIED OF A DATA SYSTEM SECURITY BREACH; AND AMENDING SECTIONS 2-6-501, 2-6-504, 30-14-1704, AND 33-19-321, MCA."

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

(Refer to Introduced Bill)

Strike everything after the enacting clause and insert:

Section 1. Section 2-6-501, MCA, is amended to read:

"2-6-501. Definitions. For the purposes of this part, the following definitions apply:

(1) "Breach of the security of a data system" or "breach" means unauthorized acquisition of computerized data that:

(a) materially compromises the security, confidentiality, or integrity of the personal information maintained by a state agency or by a third party on behalf of the state agency; and

(b) causes or is reasonably believed to cause loss or injury to a person.

(2) "Individual" means a human being.

(3) "Person" means an individual, a partnership, a corporation, an association, or a public organization of any character.

(4) (a) "Personal information" means a first name or first initial and last name in combination with any one or more of the following data elements when the name and the data elements are not encrypted:

(i) a social security number ~~or tax identification number~~;

(ii) a driver's license number, an identification number issued pursuant to 61-12-501, a tribal identification number or enrollment number, or a similar identification number issued by any state, the District of Columbia, the Commonwealth of Puerto Rico, Guam, the Virgin Islands, or American Samoa; ~~or~~

(iii) an account number, ~~or~~ credit or debit card number, ~~in combination with any required~~ security code, access code, or password that would permit access to a person's financial account;

(iv) medical record information as defined in 33-19-104;

(v) a taxpayer identification number; or

(vi) an identity protection personal identification number issued by the United States internal revenue service.

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

(5) "Redaction" means the alteration of personal information contained within data to make all or a significant part of the data unreadable. The term includes truncation, which means that no more than the last four digits of an identification number are accessible as part of the data.

(6) (a) "State agency" means an agency, authority, board, bureau, college, commission, committee, council, department, hospital, institution, office, university, or other instrumentality of the legislative or executive branch of state government. The term includes an employee of a state agency acting within the course and scope of employment.

(b) The term does not include an entity of the judicial branch.

(7) "Third party" means:

(a) a person with a contractual obligation to perform a function for a state agency; or

(b) a state agency with a contractual or other obligation to perform a function for another state agency."

Section 2. Section 2-6-504, MCA, is amended to read:

"2-6-504. Notification of breach of security of data system. (1) (a) Upon discovery or notification of a breach of the security of a data system, a state agency that maintains computerized data containing personal information in the data system shall make reasonable efforts to notify any person whose unencrypted personal information was or is reasonably believed to have been acquired by an unauthorized person.

(b) The notification must be made without unreasonable delay, consistent with the legitimate needs of law enforcement as provided in subsection (3) or with any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the data system.

(2) (a) A third party that receives personal information from a state agency and maintains that information in a computerized data system in order to perform a state agency function shall:

(i) notify the state agency immediately following discovery of the breach of the security of a data system if the personal information is reasonably believed to have been acquired by an unauthorized person; and

(ii) make reasonable efforts upon discovery or notification of a breach of the security of a data system to notify any person whose unencrypted personal information is reasonably believed to have been acquired by an unauthorized person as part of the breach of the security of a data system. This notification must be provided in the same manner as the notification required in subsection (1).

(b) A state agency notified of a breach by a third party has no independent duty to provide notification of the breach if the third party has provided notification of the breach in the manner required by subsection (2)(a) but shall provide notification if the third party fails to do so in a reasonable time and may recover from the third party its reasonable costs for providing the notice.

(3) The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation and requests a delay of notification. The notification required by this section must be made after the law enforcement agency determines that the notification will not compromise the investigation.

(4) All state agencies and third parties to whom personal information is disclosed by a state agency shall develop and maintain:

(a) an information security policy designed to safeguard personal information; and

(b) breach notification procedures that provide reasonable notice to individuals as provided in subsections (1) and (2).

(5) A state agency that is required to issue a notification pursuant to this section shall simultaneously submit an electronic copy of the notification and a statement providing the date and method of distribution of the notification to the attorney general's consumer protection office, excluding any information that personally identifies any individual who is entitled to receive notification. If a notification is made to more than one individual, a single copy of the notification must be submitted that indicates the number of individuals in the state who received notification."

Section 3. Section 30-14-1704, MCA, is amended to read:

"30-14-1704. Computer security breach. (1) Any person or business that conducts business in Montana and that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the data system following discovery or notification of the breach to any resident of Montana whose unencrypted personal information was or is reasonably believed to have been acquired by an unauthorized person. The disclosure must be made without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subsection (3), or consistent with 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 system 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 and requests a delay in notification. The notification required by this section must be made after the law enforcement agency determines that it will not compromise the investigation.

(4) For purposes of this section, the following definitions apply:

(a) "Breach of the security of the data system" means unauthorized acquisition of computerized data that materially compromises the security, confidentiality, or integrity of personal information maintained by the person or business and causes or is reasonably believed to cause loss or injury to a Montana resident. 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 data system, provided that the personal information is not used or subject to further unauthorized disclosure.

(b) (i) "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, state identification card number, or tribal identification card number;

(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;

(D) medical record information as defined in 33-19-104;

(E) a taxpayer identification number; or

(F) an identity protection personal identification number issued by the United States internal revenue service.

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

(5) (a) For purposes of this section, notice may be provided by one of the following methods:

(i) written notice;

(ii) electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. 7001;

(iii) telephonic notice; or

(iv) substitute notice, if the person or business demonstrates that:

(A) the cost of providing notice would exceed $250,000;

(B) the affected class of subject persons to be notified exceeds 500,000; or

(C) the person or business does not have sufficient contact information.

(b) Substitute notice must consist of the following:

(i) an electronic mail notice when the person or business has an electronic mail address for the subject persons; and

(ii) conspicuous posting of the notice on the website page of the person or business if the person or business maintains one; or

(iii) notification to applicable local or statewide media.

(6) Notwithstanding subsection (5), a person or business that maintains its own notification procedures as part of an information security policy for the treatment of personal information and that does not unreasonably delay notice is considered to be 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 data system.

(7) If a business discloses a security breach to any individual pursuant to this section and gives a notice to the individual that suggests, indicates, or implies to the individual that the individual may obtain a copy of the file on the individual from a consumer credit reporting agency, the business shall coordinate with the consumer reporting agency as to the timing, content, and distribution of the notice to the individual. The coordination may not unreasonably delay the notice to the affected individuals.

(8) Any person or business that is required to issue a notification pursuant to this section shall simultaneously submit an electronic copy of the notification and a statement providing the date and method of distribution of the notification to the attorney general's consumer protection office, excluding any information that personally identifies any individual who is entitled to receive notification. If a notification is made to more than one

individual, a single copy of the notification must be submitted that indicates the number of individuals in the state who received notification."

Section 4. Section 33-19-321, MCA, is amended to read:

"33-19-321. Computer security breach. (1) Any licensee or insurance-support organization that conducts business in Montana and that owns or licenses computerized data that includes personal information shall provide notice of any breach of the security of the system following discovery or notice of the breach of the security of the system to any individual whose unencrypted personal information was or is reasonably believed to have been acquired by an unauthorized person. The notice must be made without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subsection (3), or consistent with any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

(2) Any person to whom personal information is disclosed in order for the person to perform an insurance function pursuant to this part that maintains computerized data that includes personal information shall notify the licensee or insurance-support organization of any breach of the security of the system in which the data is maintained immediately following discovery of the breach of the security of the system if the personal information was or is reasonably believed to have been acquired by an unauthorized person.

(3) The notice required by this section may be delayed if a law enforcement agency determines that the notice will impede a criminal investigation and requests a delay of notice. The notice required by this section must be made after the law enforcement agency determines that the notice will not compromise the investigation.

(4) Licensees, insurance-support organizations, and persons to whom personal information is disclosed pursuant to this part shall develop and maintain an information security policy for the safeguarding of personal information and security breach notice procedures that provide expedient notice to individuals as provided in subsection (1).

(5) Any licensee or insurance-support organization that is required to issue a notification pursuant to this section shall simultaneously submit an electronic copy of the notification and a statement providing the date and method of distribution of the notification to the commissioner, excluding any information that personally identifies any individual who is entitled to receive notification. If a notification is made to more than one individual, a single copy of the notification must be submitted that indicates the number of individuals in the state who received notification.

~~(5)~~(6) For purposes of this section, the following definitions apply:

(a) "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 a licensee, insurance-support organization, or person to whom information is disclosed pursuant to this part. Acquisition of personal information by a licensee, insurance-support organization, or employee or agent of a person as authorized pursuant to this part is not a breach of the security of the system.

(b) (i) "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 the name and the data elements are not encrypted:

(A) social security number;

(B) driver's license number, state identification card number, or tribal identification card number;

(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;

(D) medical record information;

(E) a taxpayer identification number; or

(F) an identity protection personal identification number issued by the United States internal revenue service.

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

- END -