

Unofficial Draft Copy

As of: June 19, 2006 (5:19pm)

LC8800

**** Bill No. ****

Introduced By *****

By Request of the *****

A Bill for an Act entitled: "An Act requiring state and local agencies to provide notification if electronic data breaches occur; expanding record destruction procedures to state and local agencies; providing penalties; requiring Lewis and Clark County attorney to respond if electronic data breach suspected within department of justice; and amending sections 30-14-1702, 30-14-1703, 30-14-1704, and 30-14-1705, MCA; ."

Be it enacted by the Legislature of the State of Montana:

Section 1. Section 30-14-1702, MCA, is amended to read:

"30-14-1702. ~~(Effective March 1, 2006)~~ Definitions. As used in 30-14-1701 through 30-14-1705, unless the context requires otherwise, the following definitions apply:

(1) (a) "Agency" means all branches of state government and any constitutionally or legally constituted department, board, or commission of state, county, or city government or any political subdivision of the state, including the office of the clerk of the supreme court, any university system unit as defined in 17-7-102, and any school district.

(b) The term includes the state compensation fund or the board of directors of the Montana self-insurers guaranty fund except when either is subject to 33-19-321.

Unofficial Draft Copy

As of: June 19, 2006 (5:19pm)

LC8800

~~(1)~~ (2) (a) "Business" means a sole proprietorship, partnership, corporation, association, or other group, however organized and whether or not organized to operate at a profit, including a financial institution organized, chartered, or holding a license or authorization certificate under the law of this state, any other state, the United States, or any other country or the parent or the subsidiary of a financial institution. The term includes an entity that destroys records. The term also includes industries regulated by the public service commission or under Title 30, chapter 10.

(b) The term does not include industries regulated under Title 33.

~~(2)~~ (3) "Customer" means an individual who provides personal information to a business for the purpose of purchasing or leasing a product or obtaining a service from the business.

~~(3)~~ (4) "Individual" means a natural person.

~~(4)~~ (5) "Personal information" means an individual's name, signature, address, or telephone number, in combination with one or more additional pieces of information about the individual, consisting of the individual's passport number, driver's license or state identification number, insurance policy number, bank account number, credit card number, debit card number, passwords or personal identification numbers required to obtain access to the individual's finances, or any other financial information as provided by rule. A social security number, in and of itself, constitutes personal information.

~~(5)~~ (6) (a) "Records" means any material, regardless of the

Unofficial Draft Copy

As of: June 19, 2006 (5:19pm)

LC8800

physical form, on which personal information is recorded.

(b) The term does not include publicly available directories containing personal information that an individual has voluntarily consented to have publicly disseminated or listed, such as name, address, or telephone number."

{ Internal References to 30-14-1702:
30-14-1701* x 30-14-1702* x }

Section 2. Section 30-14-1703, MCA, is amended to read:

"30-14-1703. ~~(Effective March 1, 2006)~~ Record destruction.

(1) A business shall take all reasonable steps to destroy or arrange for the destruction of a customer's records within its custody or control containing personal information that is no longer necessary to be retained by the business by shredding, erasing, or otherwise modifying the personal information in those records to make it unreadable or undecipherable.

(2) (a) An agency not described in subsection (2) (b) shall follow retention and disposal requirements provided for in Title 2, chapter 6, part 2.

(b) An agency of the judicial branch shall follow retention and disposal requirements provided by rule by the supreme court."

{ Internal References to 30-14-1703:
30-14-1701* 30-14-1702* }

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

"30-14-1704. ~~(Effective March 1, 2006)~~ Computer security breach. (1) Any agency, 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 agency, person or business that maintains computerized data that includes personal information that the agency, 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

Unofficial Draft Copy

As of: June 19, 2006 (5:19pm)

LC8800

personal information maintained by the agency, 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 agency, person or business for the purposes of the agency, 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 or state 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.

(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 agency, 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 agency, person or business does not have sufficient contact information.

(b) Substitute notice must consist of the following:

(i) an electronic mail notice when the agency, 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 agency, person or business if the agency, person or business maintains one; or

(iii) notification to applicable local or statewide media.

(6) Notwithstanding subsection (5), a an agency, 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 agency, 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 an agency or a business discloses a security breach to any individual pursuant to this section and gives a notice to

Unofficial Draft Copy

As of: June 19, 2006 (5:19pm)

LC8800

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 agency or 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."

{ *Internal References to 30-14-1704:*
30-14-1701* 30-14-1702* }

Section 4. Section 30-14-1705, MCA, is amended to read:

"30-14-1705. ~~(Effective March 1, 2006)~~ Department or county attorney to restrain unlawful acts -- penalty. (1) Whenever the department has reason to believe that an agency other than the department itself or a person has violated this part and that proceeding would be in the public interest, the department may bring an action in the name of the state against the agency or the person to restrain by temporary or permanent injunction or temporary restraining order the use of the unlawful method, act, or practice upon giving appropriate notice to that agency or person pursuant to 30-14-111(2).

(2)(a) An individual, business or agency other than the department that has reason to believe that the department has violated this part and that proceeding would be in the public interest may contact the county attorney for Lewis and Clark County to request an action against the department.

(b) The action may include a temporary or permanent

Unofficial Draft Copy

As of: June 19, 2006 (5:19pm)

LC8800

injunction or a temporary restraining order regarding the use of the unlawful method, act, or practice.

(c) (i) The county attorney for Lewis and Clark County shall first give appropriate notice to the department, stating generally the relief sought.

(ii) The notice must be served at least 20 days before the hearing of the action if the relief sought is a temporary or permanent injunction.

(iii) The notice for a temporary restraining order is governed by 27-19-315.

~~(2)~~ (3) The provisions of 30-14-111(3) and (4) and 30-14-112 through 30-14-115 apply to this part.

~~(3)~~ (4) (a) A violation of this part by a business or a person is a violation of 30-14-103, and the penalties for a violation of this part are as provided in 30-14-142.

(b) (i) An agency that violates 30-14-1704 may be required to pay for a credit report for any individual whose personal information was disclosed to an unauthorized person or obtained through a breach of computer security.

(ii) (A) The penalty for a violation of this part by an agency may be a civil fine of not less than \$50 or more than \$10,000 for a computer breach incident regardless of the number of individuals whose personal identifying information was disclosed by the breach.

(B) Except as provided in subsection (4) (b) (ii) (C), in an action filed under this subsection, the court may assess the costs and attorney fees against the person bringing the charges

Unofficial Draft Copy

As of: June 19, 2006 (5:19pm)

LC8800

if the court determines that a violation did not occur or against the agency if the court determines that a violation did occur.

(C) If the Lewis and Clark County Attorney brings charges against the department of justice and the court determines that a violation did not occur, the Lewis and Clark County Attorney may not be assessed court costs and attorney fees for the action.

(D) The agency may take disciplinary action against an employee for a violation of this part."

{ Internal References to 30-14-1705:
30-14-1701 30-14-1702 }

- END -

{ Name : Pat Murdo
Title : Legislative Research Analyst
Agency : Legislative Services Division
Phone : 444-3594
E-Mail : pmurdo@state.mt.us }