Are changes needed to address ID Theft?

Does the definition of "state agency" need to be revised to include those local government entities that contract with a state agency?

2-17-506. Definitions. In this part, unless the context requires otherwise, the following definitions apply:

(1) "Board" means the information technology board established in 2-15-1021.

(2) "Central computer center" means any stand-alone or shared computer and associated equipment, software, facilities, and services administered by the department for use by state agencies.

(3) "Chief information officer" means a person appointed by the director of the department to carry out the duties and responsibilities of the department relating to information technology.

(4) "Data" means any information stored on information technology resources.

(5) "Department" means the department of administration established in 2-15-1001.

(6) "Electronic access system" means a system capable of making data accessible by means of an information technology facility in a voice, video, or electronic data form, including but not limited to the internet.

(7) "Information technology" means hardware, software, and associated services and infrastructure used to store or transmit information in any form, including voice, video, and electronic data.

(8) "State agency" means any entity of the executive branch, including the university system.

(9) "Statewide telecommunications network" means any telecommunications facilities, circuits, equipment, software, and associated contracted services administered by the department for the transmission of voice, video, or electronic data from one device to another.

Under the penalty section (2) – should this remain linked to values of $1,000 or be expanded to incorporate identity theft?

45-6-311. Unlawful use of a computer. (1) A person commits the offense of unlawful use of a computer if the person knowingly or purposely:

(a) obtains the use of any computer, computer system, or computer network without consent of the owner;

(b) alters or destroys or causes another to alter or destroy a computer program or computer software without consent of the owner; or

(c) obtains the use of or alters or destroys a computer, computer system, computer network, or any part thereof as part of a deception for the purpose of obtaining money, property, or computer services from the owner of the computer, computer system, computer network, or part thereof or from any other person.

(2) A person convicted of the offense of unlawful use of a computer involving property not exceeding $1,000 in value shall be fined not to exceed $1,000 or be imprisoned in the county jail for a term not to exceed 6 months, or both. A person convicted of the offense of unlawful use of a computer involving property exceeding $1,000 in value shall be fined not more than 2 1/2

times the value of the property used, altered, destroyed, or obtained or be imprisoned in the state prison for a term not to exceed 10 years, or both.

40-4-105 MCA--- Does the requirement "at the request of a person subject to …" need to be removed in subsection (6)?

40-4-105. Procedure -- commencement -- pleadings -- abolition of existing defenses. (1) The verified petition in a proceeding for dissolution of marriage or legal separation must allege that the marriage is irretrievably broken and must set forth:

(a) the age, occupation, and residence of each party and the party's length of residence in this state;

(b) the date of the marriage and the place at which it was registered;

(c) that the jurisdictional requirements of 40-4-104 exist and that the marriage is irretrievably broken in that either:

(i) the parties have lived separate and apart for a period of more than 180 days preceding the commencement of this proceeding; or

(ii) there is serious marital discord that adversely affects the attitude of one or both of the parties towards the marriage, and there is no reasonable prospect of reconciliation;

(d) the names, ages, and addresses of all living children of the marriage and whether the wife is pregnant;

(e) any arrangements as to support of the children and maintenance of a spouse;

(f) a proposed parenting plan, if applicable; and

(g) the relief sought.

(2) Either or both parties to the marriage may initiate the proceeding.

(3) If a proceeding is commenced by one of the parties, the other party must be served in the manner provided by the Montana Rules of Civil Procedure and may within 20 days after the date of service file a verified response. A decree may not be entered until 20 days after the date of service.

(4) Previously existing defenses to divorce and legal separation, including but not limited to condonation, connivance, collusion, recrimination, insanity, and lapse of time, are abolished.

(5) The court may join additional parties proper for the exercise of its authority to implement this chapter.

[(6) The social security number, if known, of a person subject to a decree of dissolution or a support order must be recorded in the records relating to the matter. At the request of a person subject to a decree of dissolution or a support order, the recordkeeper shall keep the social security number from this source confidential, except that the number may be provided to the department of public health and human services for use in administering Title IV-D of the Social Security Act.] (Bracketed language terminates on occurrence of contingency--sec. 1, Ch. 27, L. 1999.)

What penalty would adhere to governments if Title 30, chapter 14, part 17 were to be expanded to include government under the requirements for record disposal, computer security breach?

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

History: En. Sec. 6, Ch. 518, L. 2005.

30-14-1704. (Effective March 1, 2006) 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 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 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.

History: En. Sec. 7, Ch. 518, L. 2005.

30-14-1705. (Effective March 1, 2006) Department to restrain unlawful acts -- penalty. (1) Whenever the department has reason to believe that 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 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 person pursuant to 30-14-111(2).

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

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

History: En. Sec. 8, Ch. 518, L. 2005.