

30-14-1701. Purpose. The purpose of [30-14-1701](#) through [30-14-1705](#), [30-14-1712](#), and [30-14-1713](#) is to enhance the protection of individual privacy and to impede identity theft as prohibited by [45-6-332](#).

History: En. Sec. 4, Ch. 518, L. 2005; amd. Sec. 3, Ch. 276, L. 2007.

30-14-1702. Definitions. As used in [30-14-1701](#) through [30-14-1705](#), [30-14-1712](#), and [30-14-1713](#), unless the context requires otherwise, the following definitions apply:

(1) (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) "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) "Electronic mail message" means a message sent to a unique destination, commonly expressed as a string of characters, consisting of a unique user name or electronic mailbox and a reference to an internet domain, whether or not displayed, to which an electronic message can be sent or delivered.

(4) "Individual" means a natural person.

(5) "Internet" has the meaning provided in [2-17-551](#).

(6) "Internet services provider" has the meaning provided in [2-17-602](#).

(7) "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.

(8) (a) "Records" means any material, regardless of the 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.

(9) "Website" means an electronic location that has a single uniform resource locator or other single location with respect to the internet.

History: En. Sec. 5, Ch. 518, L. 2005; amd. Sec. 4, Ch. 276, L. 2007.

30-14-1703. 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. 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.

(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; amd. Sec. 3, Ch. 180, L. 2007.

30-14-1712. Fraudulent electronic misrepresentation -- penalties -- exemption. (1)

An individual or business that, by means of a website, an electronic mail message, or otherwise through the internet, solicits, requests, or takes an action to induce another individual or business to provide personal information by purporting to be a third-party individual or a business without the authority or approval of the third-party individual or business is guilty of a theft of identity, as provided in [45-6-332\(1\)](#). This crime of fraudulent electronic misrepresentation is commonly known as "phishing".

(2) An individual or a business that is adversely affected by a violation of subsection (1) has a private right of action, as provided in [30-14-1713](#).

(3) The attorney general or a county attorney in a county where the violation under subsection (1) is reported may bring a criminal action against an individual or a business accused of engaging in a pattern and practice of violating subsection (1) and, in addition to bringing a criminal action, may request a court of competent jurisdiction to issue a temporary injunction against the continued use of a website, an electronic mail message, or the internet by the individual or business served with the injunction.

(4) An internet services provider may not be held liable for identifying, removing, or disabling access to an internet website or other online location if the internet services

provider believes that the internet website or other online location is being used to engage in a violation of this section.

30-14-1713. Remedies for fraudulent electronic misrepresentation. (1) A business, including the owner of a website or the owner of a trademark, that is adversely affected by a violation of [30-14-1712\(1\)](#) may bring an action to recover the greater of actual damages or \$500,000.

(2) An individual who is adversely affected by a violation of [30-14-1712\(1\)](#) may bring an action against an individual or a business that has directly violated [30-14-1712\(1\)](#) for the greater of three times actual damages or \$5,000 for each violation.