2005 Mt. HB 732

Enacted, April 28, 2005

Reporter
2005 Mt. ALS 518; 2005 Mt. Laws 518; 2005 Mt. Ch. 518; 2005 Mt. HB 732

MONTANA ADVANCE LEGISLATIVE SERVICE > MONTANA 59TH REGULAR SESSION > CHAPTER NO. 518 > HOUSE BILL 732

Notice

[A> UPPERCASE TEXT WITHIN THESE SYMBOLS IS ADDED <A]

[D> Text within these symbols is deleted <D]

Synopsis

AN ACT ADOPTING AND REVISING LAWS TO IMPLEMENT INDIVIDUAL PRIVACY AND TO PREVENT IDENTITY THEFT; REQUIRING A CONSUMER REPORTING AGENCY TO BLOCK INFORMATION ON A REPORT THAT RESULTS FROM A THEFT OF IDENTITY; PROVIDING PRIVACY PROTECTION PROVISIONS FOR CREDIT CARD SOLICITATIONS AND RENEWALS AND TELEPHONE ACCOUNTS; PROVIDING PRIVACY PROTECTION FOR BUSINESS RECORDS BY REQUIRING DESTRUCTION OF RECORDS; REQUIRING BUSINESSES TO REPORT A BREACH OF COMPUTER SECURITY; PROVIDING PENALTIES FOR VIOLATIONS; AMENDING *SECTION 31-3-115, MCA*; AND PROVIDING EFFECTIVE DATES.

Text

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

Section 1. *Section 31-3-115, MCA*, is amended to read:

"*31-3-115*. Adverse information. [A> (1) <A] Whenever a consumer reporting agency prepares an investigative consumer report, [D> no <D] adverse information in the consumer report [A> , <A] [D> (<D] other than information [D> which <D] [A> THAT <A] is a matter of public record [D>) <D] [A> , <A] may [A> NOT <A] be included in a subsequent consumer report unless [D> such <D] [A> THE <A] adverse information has been verified in the process of making [D> such <D] [A> THE <A] subsequent consumer report.

[A> (2) A CONSUMER REPORTING AGENCY SHALL BLOCK THE REPORTING OF ANY INFORMATION IN THE FILE OF A CONSUMER THAT THE CONSUMER IDENTIFIES AS INFORMATION THAT RESULTED FROM AN ALLEGED IDENTITY THEFT, PURSUANT TO *15 U.S.C. 1681C-2.* <A] "

Section 2. Identity theft impediments -- credit cards -- definition. (1) A credit card issuer that mails an offer or solicitation to receive a credit card and, in response, receives a completed application for a credit card that lists an address that is different from the address on the offer or

solicitation shall verify the change of address by contacting the person to whom the solicitation or offer was mailed, as provided in [section 3].

(2) Notwithstanding any other provision of law, a person to whom an offer or solicitation to receive a credit card is made is not liable for the unauthorized use of a credit card issued in response to that offer or solicitation if the credit card issuer does not verify the change of address pursuant to subsection (1) prior to the issuance of the credit card unless the credit card issuer proves that this person actually incurred the charge on the credit card.

(3) When a credit card issuer receives a written or oral request for a change of the cardholder's billing address and then receives a written or oral request for an additional credit card within 10 days after the requested address change, the credit card issuer may not mail the requested additional credit card to the new address or, alternatively, activate the requested additional credit card unless the credit card issuer has verified the change of address.

(4) (a) Except as provided in subsections (4)(b) through (4)(d), a person, firm, partnership, association, corporation, or limited liability company that accepts credit cards for the transaction of business may not print more than the last five digits of the credit card account number or the expiration date upon any receipt provided to the cardholder.

(b) Subsection (4)(a) applies only to receipts that are electronically printed and does not apply to transactions in which the sole means of recording the person's credit card number is by handwriting or by an imprint or copy of the credit card.

(c) Subsection (4)(a) applies beginning January 1, 2008, with respect to any cash register or other machine or device that electronically prints receipts for credit card transactions that is in use before January 1, 2005.

(d) Subsection (4)(a) applies beginning January 1, 2006, with respect to any cash register or other machine or device that electronically prints receipts for credit card transactions that is first put into use on or after January 1, 2005.

(5) (a) As used in this section, "credit card" means any card, plate, coupon book, or other single credit device existing for the purpose of being used from time to time upon presentation to obtain money, property, labor, or services on credit.

(b) "Credit card" does not mean any of the following:

(i) any single credit device used to obtain telephone property, labor, or services in any transaction with an entity under regulation as a public utility;

(ii) any device that may be used to obtain credit pursuant to an electronic fund transfer, but only if the credit is obtained under an agreement between a consumer and a financial institution to extend credit when the consumer's asset account is overdrawn or to maintain a specified minimum balance in the consumer's asset account;

(iii) any key or card key used at an automated dispensing outlet to obtain or purchase petroleum products that will be used primarily for business rather than personal or family purposes.

Section 3. Identity theft impediments -- credit card renewal -- telephone accounts. (1) A credit card issuer that receives a change of address request, other than for a correction of a typographical error, from a cardholder who orders a replacement credit card within 60 days before or after that request is received shall send to that cardholder a change of address notification that is addressed to the cardholder at the cardholder's previous address of record. If the replacement credit card is requested prior to the effective date of the change of address, the notification must be sent within 30 days of the change of address request. If the replacement credit card is requested after the effective date of the change of address, the notification must be sent within 30 days of the request for the replacement credit card.

(2) Any business entity that provides telephone accounts that receives a change of address request, other than for a correction of a typographical error, from an account holder who orders new service shall send to that account holder a change of address notification that is addressed to the account holder at the account holder's previous address of record. The notification must be sent within 30 days of the request for new service.

(3) The notice required pursuant to subsection (1) or (2) may be given by telephone or electronic mail communication if the credit card issuer or business entity that provides telephone accounts reasonably believes that it has the current telephone number or electronic mail address for the account holder or cardholder who has requested a change of address. If the notification is in writing, it may not contain the consumer's account number, social security number, or other personal identifying information but may contain the consumer's name, previous address, and new address of record. For business entities described in subsection (2), the notification may also contain the account holder's telephone number.

(4) A credit card issuer or a business entity that provides telephone accounts is not required to send a change of address notification when a change of address request is made in person by a consumer who has presented valid identification or is made by telephone and the requester has provided a unique alphanumeric password.

(5) As used in this section, the following definitions apply:

(a) "Credit card" has the meaning provided in [section 2].

(b) "Telephone account" means an account with a telecommunications carrier, as defined in *69-3-803*.

Section 4. Purpose. The purpose of [sections 4 through 8] is to enhance the protection of individual privacy and to impede identity theft as prohibited by *45-6-332*.

Section 5. Definitions. As used in [sections 4 through 8], 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 of 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) "Individual" means a natural person.

(4) "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) (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 an individual has voluntarily consented to have publicly disseminated or listed, such as name, address, or telephone number.

Section 6. 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.

Section 7. 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.

Section 8. Department to restrain unlawful acts -- penalty. (1) Whenever the department has reason to believe that a person has violated [sections 2 through 8] 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 [sections 2 through 8].

(3) A violation of [sections 2 through 8] is a violation of *30-14-103*, and the penalties for a violation of [sections 2 through 8] are as provided in *30-14-142*.

Section 9. 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) 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 or state identification 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.

Section 10. Codification instruction. (1) [Sections 2 through 8] are intended to be codified as an integral part of Title 30, chapter 14, and the provisions of Title 30, chapter 14, apply to [sections 2 through 8].

(2) [Section 9] is intended to be codified as an integral part of Title 33, chapter 19, part 3, and the provisions of Title 33, chapter 19, part 3, apply to [section 9].

Section 11. Severability. If a part of [this act] is invalid, all valid parts that are severable from the invalid part remain in effect. If a part of [this act] is invalid in one or more of its applications, the part remains in effect in all valid applications that are severable from the invalid applications.

Section 12. Effective date. (1) Except as provided in subsection (2), [this act] is effective March 1, 2006.

(2) [Sections 1, 10, and 11 and this section] are effective on passage and approval.

History

Approved by the Governor April 28, 2005

Sponsor

Roberts

End of Document