

Montana

Are mandatory arbitration provisions recognized in your state? If so, are there any limitations to its enforcement?

Yes, Montana recognizes mandatory arbitration provisions under its version of the Uniform Arbitration Act. Specifically,

- a written agreement to submit an existing controversy to arbitration is valid and enforceable except upon grounds that exist at law or in equity for the revocation of a contract.[i]
- a written agreement to submit to arbitration any controversy arising between the parties after the agreement is made is valid and enforceable except upon grounds that exist at law or in equity for the revocation of a contract.[ii]
- a written agreement between members of a trade or professional organization to submit to arbitration any controversies arising between members of the trade or professional organization after the agreement is made is valid and enforceable except upon grounds that exist at law or in equity for the revocation of a contract.[iii]

However, mandatory arbitration provisions are not enforceable for the following:

- (a) claims arising out of personal injury, whether based on contract or tort;
- (b) any contract by an individual for the acquisition of real or personal property, services, or money or credit when the total consideration to be paid or furnished by the individual is \$5,000 or less;
- (c) any agreement concerning or relating to insurance policies or annuity contracts except for those contracts between insurance companies; or
- (d) claims for workers' compensation.[iv]

Additionally, there are certain limitations to the enforceability of arbitration agreements relating to basic principles of contract law. To be enforceable, an arbitration agreement must contain the same elements as any enforceable contract (i.e., the agreement must contain the following elements: identifiable parties with the capacity to contract; the consent of the parties; a lawful object; and consideration). Limitations include equitable considerations and the usual contract defenses such as absence of consideration, illegality, and unconscionability.

What is your state's law, if any, regarding gift cards, subscription services and loyalty programs?

GIFT CARDS

Gift cards are included in Montana's Consumer Protection Act. A gift certificate is defined as a record, including a gift card or stored value card, that is provided for paid consideration and that indicates a promise by the issuer or seller of the record that goods or services will be provided to the possessor of the record for the value that is shown on the record or contained within the record by means of a microprocessor chip, magnetic stripe, bar code, or other electronic information storage device. The consideration provided for the gift certificate must be made in advance. The value of the gift certificate is reduced by the amount spent with each use. A gift certificate is considered trust property of the possessor if the issuer or seller of the gift certificate declares bankruptcy after issuing or selling the gift certificate. The value represented by the gift certificate belongs to the possessor, to the extent provided by law, and not to the issuer or seller.[v]

Despite this expansive definition, the law specifically excludes three situations which, for the purposes of the Montana Consumer Protection Act are not considered gift cards: prepaid telecommunications and technology cards, including but not limited to prepaid telephone calling cards, prepaid technical support cards, and prepaid internet disks that have been distributed to or purchased by a consumer; a coupon provided to a consumer pursuant to any award, loyalty, or promotion program without any money or consideration being given in exchange for the card; or a gift certificate usable with multiple sellers of goods or services. [vi]

Certain actions in relation to the sale/transaction of gift cards/certificates are prohibited under the Consumer Protection Act:

- (1) A gift certificate is valid until redemption and does not terminate. A gift certificate is considered trust property of the possessor if the issuer or seller of the gift certificate declares bankruptcy after issuing or selling the gift certificate
- (2) The value represented by the gift certificate belongs to the possessor and not to the issuer or seller. An issuer or seller may redeem a gift certificate presented by an individual whose name does not match the name on the gift certificate
- (3) A gift certificate may not be reduced in value by any fee, including a dormancy fee applied if a certificate is not used
- (4) If the original value of the gift certificate was more than \$5 and the remaining value is less than \$5 and the possessor requests cash for the remainder, the issuer or seller shall redeem the gift certificate for cash.[vii]

Under the Montana Uniform Unclaimed Property Act, gift cards can be considered abandoned property. This has little bearing on the obligation of the issuer or seller, since, as noted above, a gift card is valid until redemption and does not terminate. However, the statutory wording that an issuer or seller "may redeem a gift certificate presented by an individual whose name does not match the name on the gift certificate" implies that an issuer or seller may decline to redeem a gift certificate presented by such an individual. This could be relevant in the context of an abandoned gift card.

A gift card may be presumed to be abandoned property if unclaimed by the apparent owner by three years after December 31st of the year in which the gift card was sold. If redeemable in merchandise only, the amount abandoned is considered to be 60% of the certificate's face value. A gift certificate is not presumed abandoned if the gift certificate was sold by a person who in the past fiscal year sold no more than \$200,000 in gift certificates,

Montana

which amount must be adjusted by November of each year by the inflation factor. The amount considered abandoned for a person who sells more than the amount that triggers presumption of abandonment is the value of gift certificates greater than that trigger. [viii]

SUBSCRIPTION SERVICES/LOYALTY PROGRAMS

Montana does not currently have any specific legislation pertaining to subscription services. For example, some states have laws addressing automatic renewal in subscription-based services. Interestingly, Montana does have an automatic renewal provision within its administrative rules; however, it only relates to contracts for utilities. Among other requirements, under that rule, the utility provider must provide written notice prior to expiration of the service contract explaining whether there is an automatic renewal provision and if so, how it operates. Interestingly, despite the rule addressing “automatic renewal”, under the rule, the customer must still affirmatively renew to retain services. [ix]

In general, basic principles of contract law would be implicated in any legal question related to subscription services. Also potentially implicated would be the Montana Consumer Protection Act, which broadly prohibits unfair or deceptive trade practices. [x]

We could not identify any other state statute, case law, or regulation regarding subscription services.

LOYALTY PROGRAMS

Montana does not currently have any specific legislation pertaining to loyalty programs. However, Montana’s Data Privacy Protection Act (discussed later in this article) does address a consumer’s rights to have personal data deleted and to opt out of having their data processed for targeted advertising or sale. Accordingly, this could potentially implicate loyalty programs if the program includes the collection of private data for the purpose of advertising or sale. The Act specifically provides that a data controller is not required to provide a product or service that requires the personal data of a consumer that the controller does not collect or maintain and is not prohibited from offering a different price, rate, level, quality, or selection of goods or services to a consumer, including offering goods or services for no fee, if the consumer has exercised their right to opt out under the Act or the offering is in connection with a consumer’s voluntary participation in a bona fide loyalty, rewards, premium features, discounts, or club card program. [xi]

Recall from above the following exception to the definition of a gift card which is not subject to the Montana Consumer Protection Act: a coupon provided to a consumer pursuant to any award, loyalty, or promotion program without any money or consideration being given in exchange for the card.

With respect to casino gambling, Montana law permits licensed gambling operators to use a “player rewards system”. If the rewards system interfaces with a gambling machine, it must not affect play. Player data must remain confidential and may be used only for the purposes of player rewards, and is considered protected as confidential trade secrets of the operator, and cannot be shared between individual licensed premises. Player rewards data may be sold or passed from a licensed gambling operator to a party purchasing that same alcoholic beverage license or by the same licensed gambling operator if a new alcoholic license is purchased for use at the same individual licensed premises. [xii]

Interestingly, the Montana Department of Revenue submitted a rule for public comment on establishing a customer loyalty program for marijuana dispensaries; however, the proposed rule was withdrawn on September 9, 2022. [xiii]

We could not identify any other state statute, case law, or regulation regarding loyalty programs.

What is your state's law, if any, regarding safeguarding consumer credit card or other private data (i.e., cyber security)?

Montana enacted comprehensive legislation addressing consumer data in 2023 which became effective on October 1, 2024. The Consumer Data Privacy Act provides a variety of protections for the personal data of consumers and applies to persons that conduct business in this state or persons that produce products or services that are targeted to residents of Montana and (1) control or process the personal data of not less than 50,000 consumers, excluding personal data controlled or processed solely for the purpose of completing a payment transaction; or (2) control or process the personal data of not less than 25,000 consumers and derive more than 25% of gross revenue from the sale of personal data. [xiv]

The Act does generally does not apply to government entities, nonprofits, higher education institutions, entities covered by HIPAA or the Gramm-Leach-Bliley Act. Further, it broadly does not apply to certain types of data including medical records, scientific research, credit-reporting data, employment information, and data regulated by the Family Educational Rights and Privacy Act or federal Farm Credit Act. [xv]

The Act establishes certain rights for the consumer and obligations on the part of the entity collecting or holding the personal data.

A consumer must have the right to:

- (a) confirm whether a controller is processing the consumer's personal data and access the consumer's personal data, unless such confirmation or access would require the controller to reveal a trade secret;
- (b) correct inaccuracies in the consumer's personal data, considering the nature of the personal data and the purposes of the processing of the consumer's personal data;
- (c) delete personal data about the consumer;
- (d) obtain a copy of the consumer's personal data previously provided by the consumer to the controller in a portable and, to the extent technically feasible, readily usable format that allows the consumer to transmit the personal data to another controller without hindrance when the processing is carried out by automated means, provided the controller is not required to reveal any trade secret; and
- (e) opt out of the processing of the consumer's personal data for the purposes of: targeted advertising; the sale of the consumer's personal data, except as provided in 30-14-2812(2); or profiling in furtherance of solely automated decisions that produce legal or similarly significant effects concerning the consumer. [xvi]

The data controller must provide and explain in its privacy notice a secure and reliable means by which the consumer can exercise these rights. The controller must respond to consumer requests in relation to these rights without undue delay, but not later than 45 days after receipt of the request, though an additional 45-day extension is allowed when reasonably necessary and notice of the extension is provided. Within that same timeframe if the controller declines to act regarding the request, it must notify the consumer and explain its justification for declining to act and provide instructions for how to appeal the decision by the controller's established appeal process. [xvii]

Additionally, the data controller must:

- (1) (a) limit the collection of personal data to what is adequate, relevant, and reasonably necessary in relation to the purposes for which the personal data is processed, as disclosed to the consumer;
- (b) establish, implement, and maintain reasonable administrative, technical, and physical data security practices to protect the confidentiality, integrity, and accessibility of personal data appropriate to the volume and nature of the personal data at issue; and
- (c) provide an effective mechanism for a consumer to revoke the consumer's consent under this section that is at least as easy as the mechanism by which the consumer provided the consumer's consent and, on revocation of the consent, cease to process the personal data as soon as practicable, but not later than 45 days after the receipt of the request.
- (4) If a controller sells personal data to third parties or processes personal data for targeted advertising, the controller shall clearly and conspicuously disclose the processing, as well as the way a consumer may exercise the right to opt out of the processing.
- (5) A controller shall provide consumers with a reasonably accessible, clear, and meaningful privacy notice that includes:
 - (a) the categories of personal data processed by the controller;
 - (b) the purpose for processing personal data;
 - (c) the categories of personal data that the controller shares with third parties, if any;
 - (d) the categories of third parties, if any, with which the controller shares personal data; and
 - (e) an active e-mail address or other mechanism that the consumer may use to contact the controller; and
 - (f) how consumers may exercise their consumer rights, including how a consumer may appeal a controller's decision regarding the consumer's request.
- (6) (a) A controller shall establish and describe in a privacy notice one or more secure and reliable means for consumers to submit a request to exercise their consumer rights pursuant to this part considering the ways in which consumers normally interact with the controller, the need for secure and reliable communication of consumer requests, and the ability of the controller to verify the identity of the consumer making the request.
- (b) A controller may not require a consumer to create a new account to exercise consumer rights but may require a consumer to use an existing account. [xviii]

Additionally, data controllers are required to conduct and document a data protection assessment for each of its processing activities that present a heightened risk of harm to a consumer. Such activities include:

- (a) the processing of personal data for the purposes of targeted advertising;
- (b) the sale of personal data;
- (c) the processing of personal data for the purposes of profiling in which the profiling presents a reasonably foreseeable risk of: unfair or deceptive treatment of or unlawful disparate impact on consumers; financial, physical, or reputational injury to consumers; a physical or other form of intrusion on the solitude or seclusion or the private affairs or concerns of consumers in which the intrusion would be offensive to a reasonable person; or other substantial injury to consumers; and
- (d) the processing of sensitive data. [xix]

A controller may not:

- (a) except as otherwise provided in the Act, process personal data for purposes that are not reasonably necessary to or compatible with the disclosed purposes for which the personal data is processed as disclosed to the consumer unless the controller obtains the consumer's consent;

(b) process sensitive data concerning a consumer without obtaining the consumer's consent or, in the case of the processing of sensitive data concerning a known child, without processing the sensitive data in accordance with the Children's Online Privacy Protection Act of 1998, 15 U.S.C. 6501, et seq.;

(c) process personal data in violation of the laws of this state and federal laws that prohibit unlawful discrimination against consumers;

(d) process the personal data of a consumer for the purposes of targeted advertising or sell the consumer's personal data without the consumer's consent under circumstances in which a controller has actual knowledge that the consumer is at least 13 years of age but younger than 16 years of age; or

(e) discriminate against a consumer for exercising any of the consumer rights under the Act, including denying goods or services, charging different prices or rates for goods or services, or providing a different level of quality of goods or services to the consumer. [xx]

Under a separate set of laws related to the prevention of identity theft, cyber security breaches must be promptly reported to those impacted by the breach.

The requirements differ based on whether the compromised data is owned by the entity suffering the 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, 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. [xxi]

The collecting entity has a duty to take adequate precautions to protect the data it collects. Following a breach, those impacted may have causes of action against the collecting entity under various legal theories including negligence, negligence per se, invasion of privacy, breach of confidence, breach of contract, and others. [xxii] However, The Consumer Data Privacy Act explicitly disclaims that it does not provide a basis for a private right of action for violations of the Act, which instead fall under the exclusive control of the Montana Attorney General. [xxiii]

What is your state's law, if any, regarding the collection and handling of financial information?

See previous discussion on Montana's laws pertaining to consumer/personal data. We could not identify any other state statute, case law, or regulation specifically regarding the collection and handling of financial information.