FOR MORE INFORMATION

MCDOWELL KNIGHT
ROEDDER & SLEDGE, L.L.C
Mobile, Alabama
www.mcdowellknight.com

Craig W. Hamilton
chamilton@mcdowellknight.com

Ransome R. Hare
rhare@mcdowellknight.com

Alabama

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

Yes, mandatory arbitration provisions are widely recognized and are generally enforceable in Alabama if there is a valid agreement to arbitrate and a party has not waived its right to arbitrate by litigation conduct. In determining whether the parties entered into a valid arbitration agreement, Alabama courts apply state contract law principles including whether there was offer and acceptance, consideration, and mutual assent to the terms essential to the contract.[i]

Even if there is a valid agreement to arbitrate, however, the party resisting arbitration may be able to show waiver if the party seeking arbitration substantially invoked the litigation process and the party resisting arbitration is substantially prejudiced by requiring it to arbitrate.[ii] A party seeking to prove the other party waived its right to arbitrate has a "heavy burden" and courts do not lightly infer a waiver of the right to arbitrate. [iii]

In terms of other potential limitations on the enforcement of arbitration provisions, an Alabama court may void an arbitration clause as a matter of public policy if it is based on consideration that is illegal under Alabama law, such as gambling[iv] or if the arbitration clause is found unconscionable because it has terms grossly favorable to a party that has overwhelming bargaining power.[v]

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

Gift certificates are presumed abandoned, other than those exempt under §35-12-73, three years after June 30 of the year in which the certificate was sold, but if redeemable in merchandise only, the amount abandoned is deemed to be 60 percent of the certificate's face value.[vi]

A gift certificate, gift card, or in-store merchandise credit issued or maintained by any person engaged primarily in the business of selling tangible personal property at retail is exempt from reporting under this article.[vii]

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

These matters are governed by the Alabama Data Breach Notification Act of 2018 (the "Act").[viii] The Act applies to any person or entity that "acquires or uses sensitive

©2022 ALFA International Global Legal Network, Inc. | All Rights Reserved.

personally identifying information," which, pursuant to the Act, includes a variety of personal information related to an individual, including, but not limited to SSNs, TINs, driver's license numbers, financial account information, medical information, and usernames and passwords.[ix]

The Act requires each covered entity and its third-party agents to implement and maintain reasonable security measures to protect the above types of information against a security breach.[x] "Reasonable security measures" means measures "practicable" for the covered entity to "implement and maintain, including consideration of all of the following:"

- Designation of an employee or employees to coordinate the covered entity's security measures to protect against a breach of security.
- Identification of internal and external risks of a breach of security.
- Adoption of appropriate information safeguards to address identified risks of a breach of security and assess the effectiveness of such safeguards.
- Retention of service providers, if any, that are contractually required to maintain appropriate safeguards for sensitive personally identifying information.
- Evaluation and adjustment of security measures to account for changes in circumstances affecting the security of sensitive personally identifying information.
- Keeping the management of the covered entity, including its board of directors, if any, appropriately informed of the overall status of its security measures.[xi]

In the case of a "breach" – defined as the "unauthorized acquisition of data in electronic form containing sensitive personally identifying information"[xii] – the Act requires covered entities to conduct a "good faith and prompt investigation" of the breach that includes:

- An assessment of the nature and scope of the breach.
- Identification of any sensitive personally identifying information that may have been involved in the breach and the identity of any individuals to whom that information relates.
- A determination of whether the sensitive personally identifying information has been acquired or is reasonably believed to have been acquired by an unauthorized person, and is reasonably likely to cause substantial harm to the individuals to whom the information relates.
- Identification and implementation of measures to restore the security and confidentiality of the systems compromised in the breach.[xiii]

Covered entities are also required to give direct notice of the breach to affected individuals within 45 days of notice or discovery of the breach.[xiv] The written notice should be sent to the individual(s) either via mail or email and include, at a minimum, all the following:

- The date, estimated date, or estimated date range of the breach.
- A description of the sensitive personally identifying information that was acquired by an unauthorized person as part of the breach.
- A general description of the actions taken by a covered entity to restore the security and confidentiality of the personal information involved in the breach.
- A general description of steps an affected individual can take to protect himself or herself from identity theft.
- Information that the individual can use to contact the covered entity to inquire about the breach.[xv]

Covered entities may substitute direct notice for other forms of notice in certain circumstances where direct notice

would not be feasible.[xvi] In addition to notifying affected individuals, covered entities must also notify the Alabama Attorney General and consumer reporting agencies where the number of individuals affected by a breach exceeds 1,000.[xvii]

The Act does not create a private cause of action in favor of consumers, but failure to adhere to the Act's notice requirements constitutes unlawful trade practice under the Alabama Deceptive Trade Practices Act and may result in an action for civil penalties by the Attorney General.[xviii] Civil penalties shall not exceed $500,000 per breach, nor more than $5,000 per day for each consecutive day the covered entity fails to take reasonable action to comply with the Act's notice provisions.[xix]

Certain entities may be exempt from the Act's notice requirements where they are already subject to and in compliance with federal laws of the same nature, or state laws that "are at least as thorough."[xx]

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

The Alabama Data Breach Notification Act of 2018 discussed above includes certain financial information in the class of protected "sensitive personally identifying information." This includes "a financial account number, including a bank account number, credit card number, or debit card number, in combination with any security code, access code, password, expiration date, or PIN, that is necessary to access the financial account or to conduct a transaction that will credit or debit the financial account."[xxi] As such, the Data Breach Notification Act has financial implications that covered entities should be sure to consider.

Additionally, there are certain Alabama regulatory provisions which govern the treatment of "nonpublic personal financial information" in the insurance industry. However, these regulations are limited to information obtained by "licensees of the Alabama Department of Insurance."[xxii] Otherwise, the only other Alabama statute regarding the handling of financial information is Ala. Code § 5-5A-43, which provides that a bank should only "disclose financial records of its customers pursuant to a lawful subpoena, summons, warrant or court order issued by or at the request of any state agency, political subdivision, instrumentality, or officer or employee thereof and served upon the bank."

---

[i] *See,* Baptist Health Sys., Inc. v. Mack, 860 So. 2d 1265, 1273 (Ala. 2003)
[ii] *See, Ocwen* Loan Servicing, LLC v. Washington, 939 So. 2d 6, 14 (Ala. 2006); Aurora Healthcare, Inc. v. Ramsey, 83 So. 3d 495, 500 (Ala. 2011)
[iii] *See,* Paragon Ltd., Inc. v. Boles, 987 So. 2d 561, 564 (Ala. 2007) (quoting Mutual Assurance, Inc. v. Wilson, 716 So. 2d 1160, 1164 (Ala. 1998))
[iv] *See*, Macon County Greyhound Park v. Hoffman, 226 So. 3d 152, 167 (Ala. 2016)
[v] *See,* Anderson v. Ashby, 873 So. 2d 168, 174 (Ala. 2003)
[vi] Ala. Code §35-12-72(a)(17)
[vii] Ala. Code §35-12-73(b)(1)
[viii] Ala. Code § 8-38-1
[ix] Ala. Code § 8-38-2(2), (6)
[x] Ala. Code § 8-38-3(a)
[xi] Ala. Code § 8-38-3(b)
[xii] Ala. Code § 8-38-2(1)
[xiii] Ala. Code § 8-38-4(a)
[xiv] Ala. Code § 8-38-5(a), (b)
[xv] Ala. Code § 8-38-5(a), (b), (d)

[xvi] Ala. Code § 8-38-5(e)(1)
[xvii] Ala. Code §§ 8-38-6, 7
[xviii] Ala. Code § 8-38-9(a)(1)
[xix] Ala. Code § 8-38-9(a)(2), (b)(1)
[xx] Ala. Code §§ 8-38-11, 12
[xxi] Ala. Code § 8-38-2(6)a.3.
[xxii] Ala. Admin. Code r. 482-1-122-.02