FOR MORE INFORMATION

JOHNSON & BELL LTD.
Chicago, IL
www.johnsonandbell.com

Nicholas R. Lykins
lykinsn@jbltd.com

Robert J. Comfort
comfortr@jbltd.com

Illinois

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

Arbitration provisions are generally enforceable in Illinois pursuant to the Federal Arbitration Act and the Illinois Uniform Arbitration Act. Enforcement of arbitration clauses generally parallels contract law. Under Illinois law, arbitration clauses will not be enforced if:

> (1) If the clause is unconscionable (it unreasonably favors one party; it represents a disparity in bargaining power; or its terms are difficult to find and read);
>
> (2) If the clause was entered into by an agent of the party against whom it is being enforced, the principal must have knowledge of the agreement to arbitrate, must have acquiesced in the agreement, and the third party seeking to enforce the arbitration clause must have relied on the representation of an agreement to arbitrate;
>
> (3) If the authority granted to the agent is the wrong form of authority, i.e., some courts have held that Healthcare Powers of Attorney are not authorized to enter into arbitration agreements on behalf of a patient, it must be a Financial Power of Attorney; and,
>
> (4) If the arbitration agreement was obtained by fraud.[i]

Even absent an arbitration clause, mandatory arbitration will be ordered in municipal cases (cases seeking less than $30,000), and, in Cook County, in some law division cases of higher value at the judge's discretion. The law division arbitration program is not actually binding – the award can be rejected for a fee of $750. And if the litigant who rejects the award fails to obtain that amount at trial, he must pay the other side's attorney's fees for the arbitration. It is worth it to request or move for a referral to mandatory arbitration from the motion judge.

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

GIFT CARDS:

The Illinois Consumer Fraud and Deceptive Business Practices Act ("Act") provides protections in a wide variety of consumer transactions, from automobile purchases to animal cremation services.[ii] It also provides consumer protections to holders of certain types of gift certificates.

For any gift certificate or gift card issued on or after Jan. 1, 2008, the Illinois act prohibits a gift certificate from having: (i) an expiration date earlier than five years after the date of issuance, or (ii) a post-purchase fee, such as an inactivity fee.[iii] For gift cards sold prior to Jan. 1, 2008, and containing a post-purchase fee, it is required that they have the terms of the fee conspicuously printed on the certificate in a location that the consumer could see prior to the purchase.

For purposes of the Act, the following do not constitute gift certificates and are not subject to the above restrictions: prepaid calling cards; gift certificates usable with multiple sellers of goods or services; gift certificates distributed as part of an awards, loyalty or promotional program without money or anything of value given by the consumer; gift certificates sold below face value at a volume discount to employers or charitable organizations for fundraising purposes if the expiration is not more than 30 days; or gift certificates issued for a food product.[iv]

SUBSCRIPTIONS:

Businesses that allow customers to sign up for automatically renewing subscriptions must comply with a patchwork of state and federal regulations. The Federal Trade Commission ("FTC") recently issued an Enforcement Policy Statement Regarding Negative Option Marketing ("Enforcement Policy") that addresses recurring subscription programs. In 2022, Illinois amended its existing laws on recurring subscriptions.

As of January 1, 2022, businesses that allow customers to sign up for subscriptions online must offer "cost-effective, timely, and easy-to-use" mechanisms for Illinois customers to terminate their subscriptions. Illinois customers who sign up for subscriptions online must be allowed to cancel their subscriptions online. Additionally, Illinois businesses must provide notice, 30 to 60 days prior to an automatic renewal, including a toll-free phone number, email, postal address, or other cost-effective, timely, and easy-to-use mechanism for cancellation.

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

Illinois law provides several regulations to safeguard consumer credit card and other private data. These regulations are primarily set forth in the Illinois Personal Information Protection Act (PIPA), the Illinois Consumer Fraud and Deceptive Business Practices Act, and the Illinois Biometric Information Privacy Act (BIPA). See below for additional information on these acts as they relate to non-public financial information, generally.

PIPA is a key law that sets forth data breach notification obligations. It applies to entities that handle, collect, disseminate, or otherwise deal with nonpublic personal information. Personal information under this law includes an individual's first name or first initial and last name in combination with an individual's social security number, driver's license number or State identification card number, account number or credit or debit card number, or an account number or credit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account.

Under PIPA, data collectors are required to maintain reasonable security measures to protect consumer personal information from unauthorized access, acquisition, destruction, use, modification, or disclosure. In the event of a data breach, the data collector is required to provide timely notice to the affected parties. The Act was amended in 2017 to further require data collectors to implement and maintain reasonable security measures

to protect those records from unauthorized access, acquisition, destruction, use, modification, or disclosure. In addition to PIPA, the Illinois Consumer Fraud and Deceptive Business Practices Act sets forth regulations respecting a host of business practices including data collection. This law, along with contractual obligations, makes a company responsible for protecting the confidential information provided to it by its suppliers, partners, customers, and other third parties. The attorney general has the authority to promulgate rules and regulations as necessary to accomplish the objectives and carry out the duties prescribed by the Act. If in the public interest, the attorney general or a state's attorney may bring an action to enjoin a method, act, or practice declared by the Act to be unlawful. The court, in its discretion, may exercise all powers necessary, including but not limited to:

- Injunction
- Revocation, forfeiture, or suspension of any license, charter, franchise, certificate, or other evidence of authority of any person to do business in the state
- Appointment of a receiver
- Dissolution of domestic corporations or association suspension or termination of the right of foreign corporations or associations to do business in the state –and–
- Restitution.

BIPA regulates the collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and information. Among other requirements, a private entity that wishes to collect and use individuals' biometric information must secure informed consent from the individual or his legally authorized representative before collecting and storing the data. The entity must also publicly provide a written policy governing the retention and permanent destruction of biometric information, inform the subject in writing of the specific purpose and length of time for which his or her biometric information is being stored and used, and obtain his or her written consent.
In conclusion, entities that handle, collect, disseminate, or otherwise deal with nonpublic personal information, including credit card and biometric data, are required to maintain reasonable security measures, provide timely notice in the event of a data breach, and secure informed consent before collecting and storing credit card and non-public personal information.

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

Illinois law also provides a comprehensive framework for the collection and handling of financial information, based largely on the same regulations that safeguard consumer credit card information as referenced above. The Illinois Personal Information Protection Act (PIPA), sets forth data breach notification obligations and regulates the actions of "data collectors," which include entities that handle, collect, disseminate, or otherwise deal with nonpublic personal information, including financial information.

Data security requirements are governed by a data security statute[v], which is contained the PIPA[vi]. Illinois's data security statute applies to data collectors and persons to whom such collectors disclose personal information pursuant to contract.[vii] "Data collector" may include, but is not limited to:

- Government agencies
- Public and private universities
- Privately and publicly held corporations

- Financial institutions
- Retail operators –and–
- Any other entity that, for any purpose, handles, collects, disseminates, or otherwise deals with nonpublic personal information.[viii]

In Illinois, the data security statute applies to "personal information," which includes either of the following:

- 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 or redacted or are encrypted or redacted but the keys to unencrypt or unredact or otherwise read the name or data elements have been acquired without authorization through the breach of security:
    - Social security number
    - Driver's license number or state identification card number
    - Account number or credit or debit card number, or an account number or credit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account
    - Medical information
    - Health insurance information
    - Unique biometric data generated from measurements or technical analysis of human body characteristics used by the owner or licensee to authenticate an individual, such as a fingerprint, retina or iris image, or other unique physical representation or digital representation of biometric data.
- Username or email address, in combination with a password or security question and answer that would permit access to an online account, when either the username or email address or password or security question and answer are not encrypted or redacted or are encrypted or redacted but the keys to unencrypt or unredact or otherwise read the data elements have been obtained through the breach of security.

"Personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records[ix].

The Illinois's data security statute requires implementation and maintenance of reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification, or disclosure.[x] While the Illinois's statutes do not set forth penalties specifically for violations of the data security provisions, the statutes provide that a violation of PIPA constitutes an unlawful practice under the Consumer Fraud and Deceptive Business Practices Act.[xi] If in the public interest, the attorney general or a state's attorney may bring an action to enjoin a method, act, or practice declared by the Act to be unlawful. The court, in its discretion, may exercise all powers necessary, including but not limited to:

- Injunction
- Revocation, forfeiture, or suspension of any license, charter, franchise, certificate, or other evidence of authority of any person to do business in the state

- Appointment of a receiver
- Dissolution of domestic corporations or association suspension or termination of the right of foreign corporations or associations to do business in the state –and–
- Restitution.[xii]

In addition, the attorney general or state's attorney may seek a civil penalty up to $50,000 against any person found by the court to have engaged in any method, act, or practice declared unlawful under the Act. In the event the court finds the unlawful act was done with fraudulent intent, the court has the authority to impose a civil penalty up to $50,000 per violation.[xiii]

In terms of financial records, Illinois law allows for the disclosure of financial records or information as necessary to effect, administer, or enforce a transaction requested or authorized by the customer, or in connection with servicing or processing a financial product or service requested or authorized by the customer. However, the sale of the financial records or information of a customer without the customer's consent is not authorized.[xiv]

In conclusion, Illinois law provides a robust framework for the collection and handling of financial information, with various statutes and regulations in place to protect the privacy and confidentiality of such information. The penalties can be severe as provided through application of the Consumer Fraud and Deceptive Business Practices Act, and entities need to take extra precaution to ensure they are in compliance with PIPA and the data security statute contained therein.

---

[i] 710 ILCS 5
[ii] 815 ILSC 505
[iii] *Id*
[iv] *Id*
[v] 815 Ill. Comp. Stat. Ann. 530/45
[vi] 815 Ill. Comp. Stat. Ann. 530/1 through 530/50
[vii] 815 Ill. Comp. Stat. Ann. 530/45(a), (b)
[viii] 815 Ill. Comp. Stat. Ann. 530/5
[ix] *Id.*
[x] 815 Ill. Comp. Stat. Ann. 530/45(a)
[xi] 815 Ill. Comp. Stat. Ann. 505/1 et seq. 815 Ill. Comp. Stat. Ann. 530/20
[xii] 815 Ill. Comp. Stat. Ann. 505/7(a)
[xiii] 815 Ill. Comp. Stat. Ann. 505/7(b).
[xiv] 205 ILCS 5/48.1 Customer financial records; confidentiality.