PURPOSE

Bally's Chicago Operating Company, LLC (the "Company" or "Bally's") has instituted the following Biometric Information Privacy Policy ("Policy"):

POLICY

The Company uses equipment and software that scans employees' hands, fingers or faces (a "Biometric Identifier")[1] to create a template associated with employees ("Biometric Information")[2] for purposes of identifying employees as well as recording and tracking access to the Company's sensitive keys.

The Policy defines the Company's policy and procedures for collection, use, safeguarding, storage, retention, and destruction of Biometric Identifiers and Biometric Information in accordance with the applicable laws, including, but not limited to, the Illinois Biometric Information Privacy Act ("BIPA"), 740 ILCS § 14/1, et seq.

An employee's Biometric Identifier or Biometric Information will not be collected or otherwise obtained by the Company without prior written consent and release by the employee. The Company will inform the employee of the reason his or her biometric information is being collected and the length of time the data will be stored.

From time to time, the Company may change the specific device, software or vendor utilized to collect Biometric Identifiers or Biometric Information. A list of the vendors and software and equipment providers who may collect, retain, use, or disclose Biometric Identifiers or Biometric information is available by request from Human Resources.

DISCLOSURE

To the extent that the Company, its vendors, and/or software or equipment providers collect, capture, or otherwise obtain Biometric Identifiers or Biometric Information from an employee, the Company will first:

- Inform the employee in writing that the Company, its vendors, and/or software or equipment providers are collecting, capturing, or otherwise obtaining the employee's Biometric Identifier or Biometric Information, and that the Company is providing such data to its vendors or software providers;

---

[1] Biometric Identifiers do not include: (1) writing samples, written signatures, photographs, human biological samples used for valid scientific testing or screening, demographic data, tattoo descriptions, or physical descriptions such as height, weight, hair color, or eye color; or (2) information captured from a patient in a health care setting or information collected, used, or stored for health care treatment, payment, or operations under the federal Health Insurance Portability and Accountability Act of 1996.

[2] Biometric Information does not include information derived from items or procedures excluded under the definition of biometric identifiers.

- Inform the employee in writing of the specific purpose and length of time for which his or her Biometric Identifier or Biometric Information is being collected, stored, and used; and
- Receive a written release signed by the employee (or his or her legally authorized representative) authorizing the Company, its vendors, and/or its software or equipment providers to collect, store, and use the employee's Biometric Identifiers or Biometric Information for the specific purposes disclosed by the Company, and for the Company to provide such data to its vendors and software and equipment providers.

The Company, its vendors, and/or software and equipment providers will not sell, lease, trade, or otherwise profit from an employee's Biometric Identifiers or Biometric Information; provided, however, that the Company's vendors and software providers may be paid for products or services used by the Company that utilize such data.

The Company will not disclose or disseminate any Biometric Identifiers or Biometric Information to anyone other than its vendors and software providers without/unless:

- First obtaining written employee consent to such disclosure or dissemination;
- The disclosed data completes a financial transaction requested or authorized by the employee;
- Disclosure is required by state or federal law or municipal ordinance; or
- Disclosure is required pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction.

RETENTION SCHEDULE

The Company shall retain employee Biometric Identifiers or Biometric Information only until, and shall request that its vendors and software and equipment providers permanently destroy such data when, the first of the following occurs:

- The initial purpose for collecting or obtaining such biometric data has been satisfied; or
- Within three (3) years of the employee's last interaction with the Company.

Should the Company or one of its vendors or software or equipment providers receive a valid warrant or subpoena issued by a court of competent jurisdiction, this retention and destruction schedule may be suspended.

DATA STORAGE

The Company shall use a reasonable standard of care to store, transmit and protect from disclosure any paper or electronic Biometric Identifier or Biometric Information collected. Such storage, transmission, and protection from disclosure shall be performed in a manner that is the same as or more protective than the manner in which the Company stores, transmits and protects from disclosure other confidential and sensitive information, including personal information that can be used to uniquely identify an individual or an individual's account or property, such as genetic markers, genetic testing information, account numbers, PINs, driver's license numbers, and social security numbers.

CONSENT FORM

Each employee as a condition of employment and/or continued employment must execute a copy of the Consent Form attached to this Policy.