Policy Statement

Ruan Transportation Management Systems, Inc. and its subsidiaries (together, the "Company") uses a DriveCam® camera, or similar technology, in most of its vehicles as part of its Video Safety Program (the "VSP") to assess and coach employees for the purpose of, among other things, enhancing road safety. The DriveCam® technology takes video of employees and may collect, capture, store, retain, and/or use "biometric identifiers" and "biometric information," as those terms are defined in the Illinois Biometric Information Privacy Act, 740 ILCS Sections 14/1, *et seq*. (the "Act"). This policy applies to routine operators of a truck, technicians, or other Company employees who may occasionally operate a truck or other Company vehicle (the "Driver").

The purpose of this Biometric Data Privacy Policy ("Policy") is to define the procedures for the collection, capture, use, safeguarding, storage, retention, disclosure, and destruction of biometric identifiers and biometric information. The Company's Policy is to protect, use, store, and delete biometric identifiers and biometric information in accordance with applicable law, including but not limited to, the Act.

1. Biometric Data Defined. "Biometric Data" includes "biometric identifiers" and "biometric information" as defined in the Act.

1.1 Biometric Identifier means a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry. Biometric identifiers do not include 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. Biometric identifiers do not include biological materials regulated under the Genetic Information Privacy Act. Biometric identifiers do not include 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. Biometric identifiers do not include an X-ray, roentgen process, computed tomography, MRI, PET scan, mammography, or other image or film of the human anatomy used to diagnose, prognose, or treat an illness or other medical condition or to further validate scientific testing or screening.

1.2 Biometric Information means any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual. Biometric information does not include information derived from items or procedures excluded under the definition of biometric identifiers.

2. Purpose for Collection of Biometric Data. The Company, its vendors, and/or Lytx, Inc. ("Licensor") collect, capture, store, use, retain, and share amongst them, the Biometric Data solely for the purposes of the VSP. The Company may pay its vendors and Licensor for products or services used by the Company that utilize such Biometric Data and Licensor may use the Biometric Data for product improvement and development. The Company, its vendors, and/or the Licensor will not sell, lease, trade, or otherwise profit from any Driver's Biometric Data.

3. Authorization. To the extent the Company, its vendors, or Licensor collect, capture, purchase, receive through trade, or otherwise obtain biometric data relating to any Driver, the Company once notified, shall as reasonably fast as possible:

3.1 Inform the Driver in writing that Biometric Data is being collected, captured, stored, used, or retained and that the Company is providing such Biometric Data to its vendors and Licensor;

3.2 Inform the Driver in writing of the specific purpose and length of time for which any Biometric Identifier or Biometric Information is being collected, captured, stored, and used; and,

3.3 Receive a written release signed by the Driver (or his or her legal representative) authorizing the Company, its vendors, and/or the Licensor to collect, capture, use, retain,

purchase, receive through trade, or otherwise obtain Biometric Data for the specific purpose disclosed by the Company, and for the Company to provide such Biometric Data to its vendors and Licensor.

4. Biometric Data Storage. The Company shall use a reasonable standard of care to store, transmit, and protect from disclosure all Biometric Data collected or possessed by the Company. The 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 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, unique identifier numbers to locate accounts or property, account numbers, PIN numbers, pass codes, driver's license numbers, or social security numbers.

5. Retention Schedule. The Company shall permanently destroy a Driver's Biometric Data, and shall request that its vendors and Licensor permanently destroy such data, when the first of the following occurs:

5.1 when the initial purpose for collecting or obtaining the Biometric Data has been satisfied, such as the Driver is no longer employed by the Company; or

5.2 within three (3) years of the Driver's last interaction with the Company;

unless the Company is required by a statute, rule, or other law to continue to retain such Biometric Data.

6. Disclosure. As part of this Policy, the Company will not disclose, redisclose, or otherwise disseminate a person's or a customer's biometric identifier or biometric information, other than its vendors and the Licensor providing products or services using the Biometric Data unless:

6.1 The Company obtains the Driver's prior consent to disclosure, redisclosure, or dissemination of the Driver's Biometric Data;

6.2 The disclosed Biometric Data completes a financial transaction request or authorized by the Driver whose Biometric Data is disclosed;

6.3 Disclosure is required by state or federal law or municipal ordinance; or

6.4 Disclosure is required pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction.