Biometric Data Privacy Policy

CN (the "Company")[1] may collect, store, and use Biometric Data for employment purposes, and it may disclose that Biometric Data in certain circumstances. This Policy explains what that means for you, and how you consent to CN's activities. This Policy is provided to employees before collection of any Biometric Data.

In signing the Acknowledgement attached to this Policy, you are providing consent for collection, storage, use, and disclosure of Biometric Data under federal, state, or local laws and regulations that apply to the collection, storage, use, and disclosure of Biometric Data.

What is Biometric Data?

Biometric Data is based on human features, such as eyes, fingerprints, or voice, that can identify a person. "Biometric Data" as used in this Policy includes both "Biometric Identifiers" and "Biometric Information."

- "Biometric Identifier" in this Policy means a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry or other physiological traits. Biometric Identifiers do not include writing samples, written signatures, photographs, human biological samples used for 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 healthcare information or information that is protected by the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

- "Biometric Information" in this Policy means any information, regardless of how it is captured, converted, stored, or shared, based on a Biometric Identifier.

How the Company Uses Biometric Data

The Company may collect, store, and use Biometric Data for several different reasons based on this Policy. Additionally, the Company may work with vendors, service providers, and/or software licensees to collect, store, and use Biometric Data. The Company and these vendors, service providers, and/or software licensees are collectively referred to as the "Company Group" in this Policy.

The Company Group will collect, store, and use Biometric Data for "Permissible Employment Uses."

A "Permissible Employment Use" is any use that is reasonably related to workplace and employee management. Permissible Employment Use includes, but is not limited to, time and attendance (for example, using biometric time clocks that use employees' fingerprints or finger scans as

[1] This term includes Illinois Central Railroad Company, Grand Trunk Western Railroad Company, Chicago Central & Pacific Railroad Company, Wisconsin Central, Ltd., Bessemer and Lake Erie Railroad Company, and Canadian National Railway Company (collectively referred to in the Policy as "CN" or the "Company").

identifiers), employee identification, fraud prevention, employee safety, worksite security, performance management, regulation of internal systems, and pre-employment hiring purposes. The Company will store, transmit, and protect from disclosure Biometric Data using a reasonable standard of care, in the same way it treats other confidential and sensitive information.

Members of the Company Group may disclose Biometric Data to other members of the Company Group. The Company will not give Biometric Data that it receives to anyone outside of the Company Group unless:

a. The employee agrees in writing that the Company can give their Biometric Data to a third party;

b. The employee approves a financial transaction that requires the Company to give their Biometric Data;

c. Federal, state, or local law requires the Company to give an employee's Biometric Data to a person or entity authorized by the law to receive it; or

d. The Company must give an employee's Biometric Data to a third party or a court because it is subject to a subpoena or court order.

How Long the Company Keeps Biometric Data

The Company will only keep Biometric Data until the first of the following happens:

- The Company Group's initial reason for collecting the Biometric Data is satisfied; or
- Within 3 years of an employee's last interaction with the Company.

Use of UKG Time Clocks

The Company uses time clocks provided and maintained by Ultimate Kronos Group ("UKG"). These time clocks scan employees' fingers and use a secure technology that generates an encoded mathematical representation of the finger scans. The data is stored on the time clocks and on a secure cloud server provided by Google, Inc.. The data cannot be used as or converted into actual fingerprints. To ensure functionality of the timekeeping system, UKG uses sub-processors (www.UKG.com/workforce-dimensions/agreement/subprocessors). UKG and its sub-processors have access to this data. UKG protects personal information, as outlined in its Privacy Policy available at www.UKG.com/privacy-policy, and its Security Policy available at: www.kronos.com/security. UKG, its subprocessors, and Google, Inc. are all members of the "Company Group" as defined in the Policy.

UKG time clocks are not the only technology that the Company and other members of the Company Group may utilize to collect, store, and use Biometric Data under this Policy, and the Company and other members of the Company Group may utilize additional types of technology not specifically itemized in this Policy.