INVOICE

BILL TO:
COYOTE LOGISTICS LLC
2545 W. DIVERSEY AVENUE
CHICAGO, IL 60647

INVOICE DATE: 12/23/2024
INVOICE #: B70369
TERMS: NET 30
DUE DATE: 01/23/2025

DATE	CUSTOMER REF#	ORIGIN - DESTINATION	QUANTITY	RATE	AMOUNT
12/19/2024		15902 Main St, Gardena, CA 90248, USA - 3051 Lakeview Road (truck entrance), Lawrence, KS 66049			
		Freight Income	1	$4,600.00	$4,600.00

TOTAL
$4,600.00

PLEASE NOTE
The right to payment under this invoice has been assigned to Compass payment Solutions LLC (CFS) and all payments hereunder are to be directed to the assignee at the address noted below. Remittances to other than CFS do not constitute payment of this invoice. CFS must be given notification of any claims, agreements or merchandise returns which would affect the payment of all or part of this Invoice on the due date.
COMPASS FUNDING SOLUTIONS LLC
P.O.BOX 205154
DALLAS, TX 75320-5154
Tel: 844-899-8092

Rate Confirmation
Load 32592035

Send invoices to:
CarrierInvoices@coyote.com
960 Northpoint Parkway
Suite 150
Alpharetta, GA 30005

877-6COYOTE
(877-626-9683)

Cust Requirements

Equipment	Van, 53'
Pre Cooled Temp	None
Load Temp	None
Tarps	Undefined
Value	$100,000

Booked By

Jared Soderholm
Jared.Soderholm@coyote.com
Phone: +1 (773) 365 6497 x2228
Fax: +1 (773) 365 7804

Load Requirements

N/A

Equipment Requirements

N/A

Notes

All Van/Container loads MUST be sealed at origin either by shipper or driver with a seal number noted on bill of lading. The driver is responsible for re-sealing the trailer after each pickup/drop on a multi-stop shipment. In the event a shipment that was sealed at origin or after each additional pickup/drop arrives at the destination with a tampered seal or without the seal intact then (i) the Carrier shall be liable for any shortage or damage claims with respect to such shipment and (ii) the shipper shall have the right, in its sole discretion, to deem the entire shipment damaged, adulterated/contaminated and unsalvageable, without the need for any inspection and the Carrier shall be liable for the full value of the shipment. Carrier is required to weigh shipment within 50 miles of departing each shipper. If carrier fails to weigh shipment within 50 miles of departing each shipper, any citations/expenses incurred due to the equipment and/or shipment weight will be the carrier's sole responsibility. Carrier must meet and comply to shipper requirements at the facility. All drivers must wear masks or facial coverings to the extent required by laws or facilities. **Carrier must be in full compliance with the Food Safety Modernization Act (FSMA), if applicable. By accepting the shipment, Carrier agrees that the driver has consented to receiving text messages and/or phone calls from or on behalf of Coyote.**

Approval for payment of detention is contingent upon the following eligibility requirements:

1) Carrier must report facility departure time and total detention hours within 24 hours of shipment delivery at the final facility.
2) Carrier must provide proof of the on time arrival and departure times in the form of a BOL or other shipping document with arrival and departure times notated by facility within 24 hours of shipment delivery at final facility.

Route Directions

Carrier acknowledges that any routing instructions from the shipper herein are being provided for convenience only, and the Carrier may choose the route.

Signature Line

By signing below, BRZ agrees to the terms and conditions set forth below and provided herewith, if any.

Rate Confirmation

Load 32592035

Stop 1: Pick Up

Pick Up Numbers: EGLV090400222236

Confirmation Numbers: None

Facility: CARTAGE WEST

Address: 15902 S MAIN ST
Gardena, CA 90248-2551

Contact: Miguel Lopez

Phone: +1 (971) 295 4762

Pickup On
Thu 12/19/2024
PLEASE CALL COYOTE TO SCHEDULE AN APPOINTMENT

Driver Work
No Touch

SLIC
N/A

Facility Notes
PICKUP AT DOCK A

Stop 1 Requirements

N/A

Commodity	Packaging	Load On	MinWt	Exp Wt	Pallets
Coffee products	Pallet	Pallets	44,000 Lbs	44,000 Lbs	27

Stop 2: Delivery

Delivery Numbers: LAW-001595

Confirmation Numbers: None

Facility: Transform Innovel - W2G

Address: 3051 Lakeview Road (truck entrance)
Lawrence, KS 66049

Contact: shawn/drew/kurt

Phone: +1 (785) 842 9600 x281

Appointment Scheduled For
Mon 12/23/2024
at 08:00

Driver Work
No Touch

SLIC
N/A

Facility Notes

Stop 2 Requirements

N/A

Commodity	Packaging	Load On	MinWt	Exp Wt	Pallets
Coffee products	Pallet	Pallets	44,000 Lbs	44,000 Lbs	25

Charges

Description	Units	Per	Amount
Fuel Surcharge	1591.00	$0.410	$652.31
Flat Rate	1.00	$3,947.690	$3,947.69

Contact

Send invoices to:
960 Northpoint Parkway
Suite 150
Alpharetta, GA 30005

Please contact Coyote at 877-626-9683 if the charges are incorrect.

[Load Number - 32592035]
[Carrier Legal Name - Riki Transportation Inc]
[Carrier USDOT - 3119062]

Rate Confirmation

Load 32592035

Total	USD $4,600.00

Agreement

Carrier	Riki Transportation Inc
USDOT	3119062
Phone	None
Email	steve@rtbrz.com
Fax	None

Broker	Coyote Logistics, LLC
Rep	Jared Soderholm
Title	Sales Rep
Phone	+1 (773) 365 6497 x2228
Fax	+1 (773) 365 7804
Date	12/19/2024 10:39

By signing below, BRZ agrees to the terms and conditions set forth below and provided herewith, if any.

Name and Title (Print)

Signature

Date

PLEASE SIGN THIS AGREEMENT AND EMAIL TO Jared.Soderholm@coyote.com

Coyote Logistics, LLC is an Equal Opportunity Employer

Rate Confirmation Load 32592035

Terms and Conditions

The Broker-Carrier Agreement or Carrier Agreement (in each case, the “Agreement”) between Coyote Logistics, LLC, a Licensed Property Broker - USDOT # 2236410, and BRZ is amended by the verbal agreement between Jared Soderholm of Coyote Logistics, LLC hereafter referred to as BROKER, and Steve Tatum of BRZ hereafter referred to as CARRIER, dated 12/19/2024.

This confirmation is subject to the terms of the Agreement and this document constitutes an amendment thereto. If the CARRIER has not signed the Agreement, then the rate shown above is the agreed individually negotiated rate and no other rate shall apply including any carrier tariff rate or terms.

THIS LOAD SHALL NOT BE DOUBLE BROKERED. No additional charges not listed above may be added by the CARRIER. Any additional charges must appear on a revised confirmation sheet signed by the BROKER. CARRIER must include signed copy of the shipper's bill of lading and any other proof of delivery with invoice to BROKER. Rates, except as specifically designated above, are inclusive of any fuel surcharge. CARRIER certifies that it is in compliance with all requirements of the California Air Resources Board (CARB) that are applicable to the scope of CARRIER’s operations, including, but not limited to: Statewide Truck and Bus Regulations, Transport Refrigeration Unit (TRU) Regulations, Tractor-Trailer Greenhouse (GHG) Gas Regulations, and Drayage Truck Regulations. CARRIER also warrants that it is in compliance with any comparable requirements of the Environmental Protection Agency (EPA) and other states, where applicable. CARRIER shall be responsible for any fines imposed on BROKER and/or shipper resulting from noncompliance.

CARRIER hereby confirms that it maintains applicable and valid insurance without exclusions that would prevent coverage for the items listed above. CARRIER has at least $100,000.00 in cargo insurance and $1,000,000.00 in automobile liability coverage. CARRIER further confirms that in transporting the shipment described hereinabove, it will comply with all U.S. DOT and FDA regulations applicable to its operations while transporting said shipment, including, but not limited to drivers' hours of service, and the Food Safety Modernization Act (FSMA), if applicable. CARRIER agrees to the attached requirements from the shipper, if any.

ALL LOADS ARE SUBJECT TO ELECTRONIC TRACKING

By accepting this shipment, CARRIER agrees that it has obtained a written agreement from each driver transporting a shipment tendered by BROKER to CARRIER pursuant to the Agreement in which each driver provides all necessary consents to (i) receiving text messages and/or phone calls from or on behalf of BROKER and (ii) allowing BROKER or its vendor to track such driver’s location while transporting such shipment. CARRIER shall comply with all applicable laws relating to the collection, use, storage, retention, disclosure, and disposal of any information CARRIER provides to BROKER, including information regarding the drivers transporting shipments. CARRIER shall indemnify, defend, and hold BROKER and its affiliates harmless from and against any and all claims, damages, liabilities, losses, actions and expenses (including attorneys’ fees) arising out of or in connection with CARRIER’s breach of this Section. This Section shall survive the expiration or termination of the Agreement between BROKER and CARRIER.

Operating Parameters
United Parcel Service

Carrier ("Vendor") shall adhere to the following customer requirements:

Carrier shall in no event or in any circumstances whatsoever, without the express written consent of Broker/UPS, cause, suffer or permit the transfer, sale or disposal of any Customer freight, whether as salvage or otherwise. Carrier shall notify Coyote who shall (A) promptly notify UPS in writing if any or all of any shipment is damaged, lost, destroyed or rejected, (B) hold such load(s) until further notice from Broker/UPS, and (C) comply with Brokers/UPS's or the applicable Customer's written instructions regarding the transfer, sale or disposal of such load(s).

Equipment; Materials. Carrier shall cause any freight transported only on, in or with equipment owned by such Carrier or leased to such Carrier for more than thirty (30) days, operating under such Carrier's operating authorities, except to the extent that such Carrier uses the services of "owner/operators" in the course of conducting its regular operations. Carrier shall maintain all materials, equipment and supplies in safe condition and good working order, free of any defects and contaminants, and upgrade and/or replace materials, equipment or supplies due to, among other things, age and condition as may be required to ensure all such materials, equipment or supplies perform at the levels or specifications required and applicable Laws. Carrier shall ensure that none of the equipment used to provide the Carrier Services has been used for the transportation of any waste of any kind, garbage, hazardous waste materials or any other commodity that might adulterate or contaminate the freight that UPS may tender.

Sanitation and Operation Policies. Carrier shall comply with all of UPS's reasonable sanitation and operation policies, and all instructions and specifications on each bill of lading issued hereunder and any related documents provided to Carrier, including any refrigeration, pre-cooling, or other temperature control requirements.

California Air Resources Board (CARB). To the extent that any shipments are transported within the State of California, the Carriers shall certify that it is in and shall maintain, compliance with all requirements of the California Air Resources Board (CARB) that are applicable to the scope of Carrier's operations, including, but not limited to, Statewide Truck and Buses Regulations, Transport Refrigeration Unit (TRU) Regulations, Tractor-Trailer Greenhouse (GHG) Gas Regulations, and Drayage Truck Regulations. Carrier shall also warrant that it complies with, and shall continue to comply with, any comparable requirements of the Environmental Protection Agency (EPA) and other states, where applicable. Carrier shall be responsible for any fines, penalties or any other liability imposed on Coyote and\or shipping resulting from Carrier's noncompliance with the requirements.

Safety Precautions. Carrier shall take and ensure reasonable safety precautions, and follow customary transportation practices in the loading, unloading, transport, and handling of Customers' freight. Carrier shall ensure that no freight transported shall become, or shall be deemed to be, adulterated or misbranded within the meaning of applicable Laws because such freight was transported in or with Carrier, or because of any of Carrier's activities in connection with such transport.

Safety Ratings. Carrier shall agree that, at all times while providing Services hereunder, it shall obtain or maintain no less than a "satisfactory" USDOT safety rating or a comparable rating issued by any applicable authority, including the FMCSA. If Carrier receives a less than "satisfactory" safety rating, it shall immediately (but, in any event within thirty-six (36) hours) notify Coyote in writing. Coyote shall have the right to suspend or terminate the Carrier Contract if the Carrier's safety rating is determined to be conditional, unsatisfactory, unfit, marginal or a similar designation. For purposes of clarity, an "unrated" safety rating shall not be considered less than "satisfactory."

Anti-Corruption Laws. Carrier and its employees, officers, directors, contractors, Subcontractors, agents and other representatives shall comply with all applicable anti-corruption Laws, including, without limitation, the U.S. Foreign Corrupt Practices Act, the U.K. Bribery Act of 2010 and the Canada Corruption of Foreign Public Officials Act, and neither Carrier, nor any of its employees, officers, directors, contractors, Subcontractors, agents or other representatives, have made any payments in connection with the Services which could violate any applicable anti- corruption Laws.

EQUAL OPPORTUNITY. Carrier shall comply with the Equal Opportunity provisions in accordance with FAR 52.222-26.

MARKETING. Carrier shall not display UPS's trade name, trademark(s), logo(s), and/or company and product descriptions and similar information and designations (collectively the "**UPS Marks**"), including, without limitation, on web pages, in advertisements, brochures, exhibits and other marketing and promotional material of Carrier (collectively "**Carrier Collateral**"), except with UPS's prior written approval. Nothing stated herein shall constitute a grant or other transfer to Carrier of any right, title or interest in or to any UPS Marks.

UPS INFORMATION SECURITY

1. **GENERAL**

(a) This UPS Information Security Exhibit (the "Exhibit") outlines the logical and physical security requirements that Vendor will maintain as part of the Services ("Security Requirements"). The Security Requirements are applicable to the Information Security Programs of the Vendor, as well as all Vendor Controlled facilities, that contain UPS Data and/or access UPS Systems, and/or support UPS Information Technology Services or products. Capitalized terms used in this Exhibit without a definition will have the meaning ascribed to them in the Master Agreement. Vendor will comply with the obligations contained herein consistent with applicable Industry Standards and in a commercially reasonable manner.

(b) Definitions:

(i) "Affiliate" means an entity that a party controls or is controlled by, or with which a party is under common control. For purposes of this definition, "control" means ownership of more than fifty (50%) percent of the voting stock or equivalent ownership interest in an entity.

(ii) "Applicable Law" means all applicable laws (including those arising under common law), statutes, codes, rules, regulations, reporting or licensing requirements, ordinances, and other pronouncements, as interpreted or enforced by relevant governmental or regulatory authorities.

(iii) "Confidential UPS Data" means the data deemed "Confidential Information" under the Agreement and any Personal Information as defined in the DPA, including but not limited to, Sensitive Personal Information.

(iv) "Industry Standards" means security measures that are commercially reasonable in the information technology industry and designed to ensure the security, integrity, and confidentiality of sensitive data and to protect against a compromise of security.

(v) "Personal Information" means UPS Data that identifies or relates to an identifiable individual (i.e., a person who can be identified, directly or indirectly, including, by reference to an identification number, location data, an online identifier or to one or more factors specific to the person's physical, physiological, mental, economic, cultural, or social identity) and such similar data regulated under Applicable Law.

(vi) "Privileged Users" means any users of Vendor who have enhanced authority to access and configure network systems that contain and/or access UPS Data, including but not limited to system administrators and "super users" who can provision, install, upgrade, or modify credentials, operating systems, source code, applications, and other network systems.

(vii) "Secured" means physical and logical, as applicable, methods of security designed to protect against unauthorized access, acquisition, modification, theft, misuse, or destruction of information. These methods may incorporate recommendations in specific publications of the National Institute of Standards and Technology ("NIST"), the International Organization for Standardization ("ISO") and the International Electrotechnical Commission ("IEC"), Federal Information Processing Standards ("FIPS"), or the Internet Engineering Task Force ("IETF") and specific protocols such as Transport Layer Security ("TLS"), or the Advanced Encryption Standard ("AES").

(viii) "Sensitive Personal Information" means UPS Data that contains a financial account number, such as a bank account number, credit card number or debit card number, a Social Security Number or other national insurance number, a driver's license number or other government identification number, a date of birth, an email address or username in combination with a password or security code for an online account, a private key or digital

signature, biometric data of a specific person, precise geolocation data, or credit history or eligibility information that is identifiable to a specific person; or information that reveals racial or ethnic origin, political opinions, religious or spiritual beliefs, criminal history, or labor union membership of an identifiable person or that relates to a specific person's health or sex life and such similar information regulated under Applicable Law.

(ix) "Services" as used in this Exhibit shall mean the services, goods, or work provided by the Vendor in the Agreement and has the same meaning as the term "Work," "Services," "Goods," or "Deliverables" if used in the Agreement.

(x) "UPS" as used in this Exhibit means the UPS entity to the Agreement and has the same meaning as the term "Owner," "UPS," or "Purchaser" if used in the Agreement.

(xi) "UPS Data" means any data transmitted by UPS or its Affiliates to Vendor or accessed or acquired by Vendor in connection with the provision of Services.

(xii) "UPS Systems" means, collectively, the systems of UPS and its Affiliates, managed by UPS and accessed or hosted by Vendor in connection with the provision of Services, including computer systems, software, and networks, including technology and data, stored on or accessible through utilization of such systems, software, and networks.

(xiii) "Vendor" as used in this Exhibit means the third party contracted carrier or has the same meaning as the term "Supplier," "Seller," "Provider," "Contractor," or "Consultant".

(xiv) "Vendor Personnel" means the officers, directors, employees, agents, contractors, consultants, vendors, invitees, and representatives of Carrier and of Carrier's Affiliates performing Services or otherwise accessing any UPS Data or UPS Systems.

(c) Vendor will (i) implement and maintain a comprehensive written information security program; (ii) update and/or review such program, as necessary, on no less than an annual basis or upon a material change in the provision of Services; and (iii) ensure such program

(1) complies with Applicable Law and applicable industry standards, examples of relevant industry standards that may be applicable include:

- ISO/IEC 27001:2013
- ISO/27002:2013/2022
- ISO27017
- ISO27018
- Payment Card Industry Data Security Standard (PCI DSS)
- US NIST Cybersecurity Framework
- US NIST 800-53
- US NIST800-171
- Committee of Sponsoring Organizations (COSO)

(2) includes appropriate administrative, logical, technical, and physical safeguards that comply with this Exhibit and

(3) is designed to achieve the following objectives:

(A) To ensure the security and the confidentiality, integrity, and availability of UPS Data;

(B) To protect against any threats or hazards to the security and integrity or availability of UPS Systems; and

(C) To prevent unauthorized or accidental access, acquisition, destruction, loss, deletion, disclosure, or alteration or use of UPS Data or UPS System

(d) Any expenses related to the implementation and maintenance of the Vendor's Information Security program, and the requirements and obligations set forth in this exhibit, are the sole responsibility of the Vendor.

(e) Where Applicable Law sets forth more stringent requirements than those set forth in this Exhibit, Vendor will comply with Applicable Law.

(f) The provisions of this Exhibit will control in the event of a conflict between the Agreement (including any attachments, exhibits or schedules) and this Exhibit.

(g) Upon reasonable written request, Vendor will disclose to UPS any shared third-party hosting facilities that will hold UPS Data, and Vendor will take reasonable measures to require such third parties materially comply with the applicable terms of this Exhibit.

(h) For the avoidance of doubt, and in addition to the confidentiality obligations, when making any authorized transfer of UPS Data hereunder, Vendor will comply with Applicable Law and this Exhibit.

(i) If the underlying agreement involves Personal Information, Vendor will execute the UPS Data Processing Exhibit (DPE). The Data Transfer Addendum (DTA) and Transfer Impact Assessment (TIA) are also needed where personal data is transferred out of or accessed from outside of the European Economic Area (EEA) or the UK. Vendor will execute any additional privacy documentation where required by Applicable Laws.

2. POLICIES, AWARENESS AND TRAINING

(a) Vendor will maintain, publish, recertify, enforce, and make available to UPS upon reasonable advance written request, written policies addressing core information security concepts including, but not limited to, "acceptable use," "encryption," "password management," "security incident and data breach response," "physical security," "disaster recovery," and "background checks."

(b) Vendor will provide training on a general range of information security topics, including, but not limited to phishing and social engineering, strong passwords, and removable media to all existing Vendor Personnel on an annual basis, and to new Vendor Personnel upon hire, to educate such Vendor Personnel about information security industry standards and best practices, and emerging threats and trends. Vendor will provide copies of training materials to UPS upon request.

3. ASSET MANAGEMENT

(a) Vendor will maintain sufficient technology and capability to apply information classification schemes and storage requirements across the organization (On-premises and in the Cloud) according to legal or regulatory requirements, business value, and sensitivity to unauthorized disclosure or modification.

(b) Vendor will implement replacement or mitigation strategies for end of life and legacy infrastructure, networks, operating systems, software applications.

4. ACCESS MANAGEMENT AND IDENTIFICATION; AUTHENTICATION

(a) Vendor will permit only those Vendor Personnel and third parties who are authorized pursuant to the Services to access UPS Data or UPS Systems. Authorized Vendor Personnel and authorized third parties will use UPS Data or UPS Systems only as necessary to perform their obligations and this Exhibit.

(b) Vendor will follow Applicable Law and applicable Industry Standards and accounting rules to authenticate and authorize users. Vendor will not use shared or generic identification credentials to access UPS Data or UPS Systems. Passwords must contain a minimum of eight (8) characters and include at least one alpha character and one numeric character. In addition, passwords must expire every ninety (90) days or less and user IDs must be deactivated after no more than ten (10) failed log-in attempts.

(c) Vendor will identify to UPS any Vendor Personnel requiring access to UPS Systems. UPS will issue multi-factor authentication technology, if applicable, to Vendor Personnel. Vendor will promptly notify UPS when Vendor Personnel no longer requires access to UPS Systems.

(d) Vendor will maintain a documented centralized repository of all identification credentials used to access Vendor's network and /or systems where UPS Data or UPS Systems reside. Vendor will immediately revoke access from Vendor Personnel and authorized third parties who no longer require access to UPS Data or Systems.

(e) Vendor will periodically review and revoke access rights of users, as needed, and will log, monitor, and provide to UPS, upon request, reports on identification credentials used to access UPS Data or UPS Systems.

(f) Authentication to Vendor's network resources, platforms, devices, servers, workstations, applications, and devices will not be allowed with default passwords and, if available, will use role-based access control, single sign-on (SSO) and federated identity management (FIM). Multi-factor authentication will be used for (i) Vendor's Privileged Users, (ii) remote access to Vendor's network, (iii) regulated environment and (iv) access to UPS Confidential Data.

(g) All access to UPS Data and UPS Systems, if applicable, will be via a Secured connection between Vendor's service locations (including access through any of Vendor's cloud service providers) and UPS.

(h) Vendor will ensure secure external network connections to Vendor's network occur via a Virtual Private Network (VPN).

5. PRIVILEGED ACCESS

Vendor will assert that Vendor's security program adheres to the following, or substantially similar, principles:

(a) Maintaining an inventory of all privileged accounts including domains and local accounts to ensure only authorized and approved individuals have privileged access to systems and resources.

(b) Provide specific Privileged User role training to persons with privileged access.

(c) Ensure privileged access is only granted on least privileged basis and without violating the separation of duties principle.

(d) Performance of periodic (quarterly) reviews and recertification of privileged access to ensure privileges are appropriately assigned to users based on their job responsibilities.

(e) Defining and implementing a privileged access request process to ensure privileged access roles and rights are granted for a time limited period and implement procedures to prevent the culmination of segregated privileged access.

(f) Implementing Multi-Factor Authentication (MFA) and encrypted login channels for all privileged account access.

(g) Use of dedicated or secondary account/systems for elevated, privileged functions.

(h) Configuration of the privilege account systems to log and alert on key changes such as added or removed accounts, unsuccessful logins, or similar activities.

6. SECURE DATA HANDLING

(a) Vendor will encrypt Confidential UPS Data in transit, and in use via AES minimum 128-bit encryption and 1024-bit cipher key length.

(b) Prior to being backed up, all UPS Data will be encrypted or equivalently Secured.

(c) Any encryption products used by Vendor must be FIPS 140-2 or 140-3 certified, or at least meet FIPS 140-2 or 1403 applicable standards. Vendor must use TLS or equivalent with the highest feasible encryption available when transferring UPS Data over the Internet.

(d) Symmetric encryption keys and asymmetric private keys will be encrypted in transit and storage, protected from unauthorized access, and secured. Cryptographic key management and rotation procedures must be documented. Access to encryption keys must be restricted to named administrators. Vendor will follow industry standards, such as NIST 800-57 or ISO

recommendations, to generate, store, and manage cryptographic keys used to encrypt UPS Data.

(e) Vendor will maintain secure data disposal procedures, including but not limited to using secure erase commands, degaussing, and "crypto shredding" when needed. Vendor's procedures will follow industry standards, such as NIST 800-88 or ISO recommendations.

(f) The vendor must have a capability and process at the end of the contracted term to securely return and securely delete or destroy UPS Data from Vendor's environment. Upon UPS's written request, Vendor will provide evidence or authorized attestation of such deletion or destruction. Notwithstanding the above, Vendor may retain archival copies of the UPS Data, as required by applicable law or its data retention policies, provided that all such copies remain subject to the restrictions herein for so long as they are retained.

(g) Vendor will have the capability to perform a remote wipe on any Vendor Personnel mobile device, including, but not limited to a smartphone, tablet, and laptop ("Mobile Device"). If any Mobile Device contains or has access to UPS Data, Vendor will have a capability to wipe the Mobile Device upon a remote command after (i) multiple failed attempts to authenticate the user of the Mobile Device or (ii) the Mobile Device has been lost or stolen.

(h) To the extent practicable, Vendor will deploy Data Loss Prevention (DLP) technology, processes, and/or solutions to protect and prevent against exfiltration of UPS data or transfer of UPS data to non-authorized assets or networks.

7. PHYSICAL AND ENVIRONMENTAL SECURITY

(a) Vendor's facilities, if any must maintain appropriate physical and environmental controls such as access restriction, detective monitoring controls, fire detection and suppression, climate control and monitoring, power and backup power solutions, and water damage detection.

(b) Vendor will implement appropriate physical access controls such as user authentication badge access and/or appropriate sign-in procedures and appropriate access logs for facilities that contain systems with access to UPS Systems and UPS Data.

8. ENDPOINT & NETWORK SECURITY

(a) Vendor will install, configure, and maintain perimeter and network security controls to prevent unauthorized access to UPS Data and UPS Systems and/or Vendor's network and systems. Examples of security controls include, but are not limited to, firewalls, switches, routers, wireless access points, intrusion detection systems ("IDS"), intrusion prevention systems ("IPS"), antimalware software, and access control lists.

(b) Vendor will maintain and configure endpoint security software and hardware on servers, desktops, laptops, mobile, and portable digital media devices, including but not limited to updated anti-virus software. Other endpoint protections may include encryption software, intrusion detection systems, intrusion prevention systems, anti-malware software, in accordance with Industry Standards. Vendor will require such configurations generate alerts to Vendor and logs accessible by Vendor and will provide to UPS upon request.

(c) Vendor will have a security operations center ("SOC"), or a team performing a similar function, responsible for, at a minimum, security information and event management ("SIEM"), security logging, continuous security monitoring, and secure network security configurations.

(d) Vendor will implement and maintain security and hardening standards for network devices, including, but not limited to, baseline configurations, patching, passwords, access control, and multi-factor authentication with automatic system logout after 15 minutes of inactivity.

(e) Vendor will use defense-in-depth techniques, which may include any of the following: deep packet analysis, traffic throttling, and packet black-holing, for the detection of and timely response to network-based attacks associated with anomalous ingress or egress traffic patterns

(e.g., MAC spoofing and ARP poisoning attacks) and/or distributed denial-of-service (DDoS) attacks.

(f) Vendor will follow its documented change management procedures.

(g) Vendor will reasonably protect workstations from intrusion by implementing automatic screen savers, locking devices, privacy screens, and/or similar controls.

9. APPLICATION SECURITY

(a) Vendor will follow secure software development life cycle ("SDLC") secure coding practices, in accordance with the most current guidance, which may include any of the following (i) the Open Web Application Security Project ("OWASP") found at https://owasp.org/Top10/ https://www.owasp.org/, (ii)Common Weakness Enumeration ("CWE") found at , (https://cwe.mitre.org/top25/archive/2021/2021_cwe_top25.html) and (iii) SANS guidance Most Dangerous Software Errors (found at https://www.sans.org),to ensure harmful code is not delivered and best practices are followed. Coding practices will include (i) separate development, test, and production environments; (ii) regular security code reviews; (iii) static and dynamic scanning of all software and/or applications storing, processing, and/or transmitting UPS Data.

(b) Vendor will maintain proper segmentation of data environments (Development, Test, and Production). Segregation/Segmentation must be employed such that production data will not be used in development and testing environments.

(c) Vendor has reviewed the requirements outlined herein and has confirmed that the Vendor's application Security practices/requirements materially comply with the requirements set forth in this Exhibit. Where a conflict of specific technical requirements exists between this Agreement and this Exhibit, this Exhibit prevails.

10. RISK MANAGEMENT; THIRD PARTY/VENDOR ASSURANCE

(a) Vendor will maintain a third-party risk management program. This will include (i) maintenance of information security agreements to ensure that Vendor's third parties are bound to the terms of this Exhibit or substantially similar terms; and (ii) monitoring and auditing (at least annually) of Vendor's third parties. Vendor will make available to UPS upon written request, executive summaries of audit and monitoring reports, information security agreements, and other artifacts of Vendor's third parties to the extent not prohibited by confidentiality requirements.

(b) Risk management will include remediation by Vendor of any identified findings commensurate with risk and evidence of completion.

(c) Vendor will maintain a risk assessment program, which will define roles and responsibilities for performing risk assessment and responding to results. Vendor will perform an annual risk assessment to verify the design of controls that protect business operations and information technology.

(d) Vendor will maintain a risk assessment remediation plan, which will include the use of issue tracking to completion that measures remediation progress regularly against target dates. Vendor will assign an owner (active Vendor Personnel) to each remediation plan. For risk acceptance, Vendor management will provide clear acknowledgement and a description of the risk. The risk acceptance must include a business justification.

11. VULNERABILITY AND PATCH MANAGEMENT

(a) Vendor will conduct security vulnerability scans of Vendor's systems and networks that access or store UPS Data.

(b) Vendor will perform routine (at least quarterly) network and application-level scans for vulnerabilities, intrusions, and unauthorized changes to UPS Data or UPS Systems (each a "Vulnerability Scan").

(c) At least once every year, Vendor will hire an independent third-party cybersecurity firm to test a potential unauthorized user's ability to penetrate Vendor's network (a "Penetration Test").

(d) Vendor will provide to UPS, upon UPS's reasonable written request, an executive summary of the results of Vendor's then most recent Penetration Tests.

(e) Vendor will identify, triage, document, and remediate vulnerabilities and threats to UPS Data and UPS Systems, including those identified by anti-virus scans, firewall reports, IPS or IDS alerts, vulnerability scans, penetration tests, or other security data. Vendor will determine the severity of each vulnerability or threat in accordance with the NIST National Vulnerability Database's ("NVD") Common Vulnerability Scoring System ("CVSS"), version 3.0 or higher (found at https://nvd.nist.gov).

(f) Vendor will apply security patches and system updates to Vendor's network, systems, software, applications, appliances, and operating systems in the Vendor's environment in a reasonable time frame based on the criticality of an identified vulnerability, availability of the patch, and sensitivity of the underlying data, but at a minimum, Vendor will use commercially reasonable efforts to test and apply patches upon their availability based on Vendor's policies and procedures regarding security patches.

(g) Where the Vendor solely supplies UPS with commercial software or cloud software or hardware services, Vendor will supply, deliver, or apply security patches and system updates to vendor-managed and/or supplied software and applications, appliances, devices, and operating systems. Vendor will use commercially reasonable efforts to supply or apply the updates and patches will be supplied or applied upon the general release date based on the criticality of the vulnerability, availability of the patch, and sensitivity of the underlying data based on Vendor's policies and procedures regarding security patches.

12. BUSINESS CONTINUITY, RESILIENCE and DISASTER RECOVERY

(a) Vendor will maintain a documented and operational Business Continuity and Disaster Recovery (BC&DR) Program. Vendor will exercise and update its BC&DR plans at least annually.

(b) Vendor will document and upon written request, provide to UPS a high-level executive summary of Vendor's contingency and incidence planning procedures relevant to the goods, software or services used by UPS in connection with the Services, or used by the vendor to produce or support the said goods, software, or services.

(c) Vendor will conduct business impact analysis on critical assets to determine the acceptable Recovery Time Objective (RTO) /Recovery Point Objective (RPO) of the assets relevant to the goods, software or services provided to UPS and which may impact UPS.

(d) Vendor will periodically backup data per UPS business requirement and ensure that controls are in place to support the confidentiality, integrity, and availability of the backups, snapshot images and other recovery media.

(e) Vendor will monitor and test system backups to ensure the integrity of the backup for successful data restoration according to the Vendor's backup schedule and should be at minimum yearly.

(f) Vendor will verify data restoration and integrity from backups, snapshot images and other recovery media at a minimum yearly.

13. SECURITY BREACH

(a) Vendor will maintain and annually update a documented data breach action and response plan.

(b) If Vendor discovers or is notified of a breach of security, which results in unauthorized access, acquisition, disclosure, or use relating to any UPS Data or UPS Systems or any violation of these Security Requirements ("Data Breach"), upon validation or verification of the Data Breach,

Vendor will promptly at its expense: (i) notify UPS via UPS email addresses soc@ups.com and globalprivacy@ups.com of the Data Breach without undue delay, but no later than 72 hours of becoming aware of the Data Breach; (ii) investigate the Data Breach; (iii) mitigate the effects of the Data Breach; and (iv) perform post-incident assessments, including those reasonably requested by UPS, and report on the results of such assessment(s) to UPS.

(c) For any Data Breach caused by Vendor or any of its subcontractors, Vendor will be solely responsible for the costs of responding to the Data Breach, including, but not limited to, the costs to: (i) hire external counsel or litigate related claims; (ii) hire technical experts; and (iii) provide any notices and credit services to third parties, and all associated support to such third parties (e.g., call center support) and any services to third parties as required by Applicable Law.

14. REPORTING AND RIGHT TO AUDIT

(a) Vendor will perform continuous monitoring, logging, review, and mitigation of attempted and successful access, and security event logs for vulnerabilities, intrusions, and unauthorized changes on endpoints, network devices, and server systems that contain UPS Data or UPS Systems. All logs must be protected from unauthorized access or modification and be configured so as not to capture and record Confidential UPS Information and shall be provided to UPS upon written request.

(b) Vendor will reasonably cooperate with UPS in any investigations of confirmed or reasonably likely fraudulent or unauthorized use of or access to UPS Data or UPS Systems by Vendor's employees or third parties.

(c) UPS reserves the right to perform information security assurance audits, with Vendor's reasonable cooperation, annually upon at least thirty (30) prior written request. The audit may be on-site at Vendor's facility, via questionnaire, or through a third party (who signed a confidentiality agreement with Vendor). UPS will provide Vendor with 30 days' written notice prior to the audit. Vendor will endeavor respond to all questionnaires and resulting recommendations within 30 days or as otherwise agreed by the parties. At no time will UPS have access to Vendor's systems.

(d) Vendor agrees as part of the above-referenced audit, to discuss any non-privileged findings with UPS, and to provide related evidence of capabilities, remediation, and compliance activities out outlined herein.

UPS DATA PROCESSING

This UPS Data Processing Exhibit (the "Exhibit") contains requirements for Carrier ("Vendor") with respect to the privacy and protection of Personal Information (as defined below) that, as part of the Agreement or any related statement of work (collectively, the "Agreement"), Vendor accesses or acquires from UPS or its Affiliates, that UPS or its Affiliates provide to Vendor, or that Vendor collects or acquires on behalf of UPS or its Affiliates. Capitalized terms used without definition in this Exhibit are defined in Section 4 (Definitions) of this Exhibit.

1. PROCESSING OF PERSONAL DATA

(a) General Obligations. Vendor will Process Personal Data in compliance with Applicable Law at all times and will provide at least the same level of privacy protection for all Personal Data as required by Applicable Law. Vendor will not disclose Personal Data to any third party without first obtaining UPS's written consent or in accordance with the Agreement. Vendor shall ensure that, at all relevant times during the term of the Agreement, all Vendor personnel engaged in the Processing of Personal Data are subject to enforceable obligations to maintain the confidentiality of the Personal Data and to comply with the relevant terms and conditions of this Exhibit.

(b) Processing Only on Instructions from UPS. Vendor will Process Personal Data solely on behalf of UPS for the purpose of performing the Services and in accordance with UPS's reasonable instructions as issued from time to time in writing. Vendor acknowledges that, with respect to the Personal Data, Vendor will act only as a data processor as defined under Applicable Law. The duration of Vendor's Processing of Personal Data will be the term of the Agreement, except as provided otherwise in the Agreement, and subject to Section 1(e) (Retention and Deletion) of this Exhibit. Vendor will Process only such Personal Data during the course of performing the Services as is strictly necessary for Vendor to perform the Services. Other than as outlined in the Agreement, Vendor shall not combine or commingle Personal Data with Personal Information that Vendor receives from or on behalf of any third party or collects from Vendor's own interactions with Data Subjects, except to the extent necessary to Process the Personal Data in accordance with the Agreement and/or this Exhibit. If Applicable Law requires Vendor (or, for avoidance of doubt, any subcontractor) to conduct Processing that is or could be construed as inconsistent with UPS's instructions, then Vendor shall notify UPS promptly and prior to commencing the Processing. If Vendor believes that any instruction from UPS is in violation of, or would result in Processing in violation of, Applicable Law, then Vendor shall notify UPS immediately.

(i) The Personal Data to be Processed by the Vendor consists of the following categories of information: names, physical addresses, and email addresses related to shipments arranged by Vendor for UPS.

(ii) The Personal Data to be Processed by the Vendor involves the following categories of Data Subjects: shippers / consignees and package recipients / customers of UPS and its Affiliates / contractors, supplier and vendors.

(c) Subcontractors. Vendor may subcontract the Processing of Personal Data only with prior written consent of UPS. For any proposed subcontractor, Vendor will disclose to UPS the geographic location(s) at which the proposed subcontractor will perform the Processing. All Processing by subcontractors must be subject to a written agreement between Vendor and the subcontractor that requires the subcontractor to comply with substantially similar limitations, restrictions and other terms and conditions as provided in this Exhibit, including express guarantees by the subcontractor to implement technical and organizational measures to ensure that Processing satisfies all requirements of Applicable Law. Vendor shall remain responsible for the Processing of the Personal Data by Vendor's subcontractors and for any acts and omissions of such subcontractors while performing the Services under the Agreement or otherwise in connection with such subcontractor's Processing of Personal Data to the same extent as if such acts or omissions were performed by Vendor.

(d) Cooperation to Facilitate Data Subject Requests.

(i) Vendor will at no additional charge reasonably cooperate with UPS with respect to, and reasonably facilitate UPS's authentication, recording, investigation, processing, execution and resolution of, all enquiries, complaints, requests and claims of Data Subjects relating to access, rectification, portability, restriction, erasure, objection or any other rights available to Data Subjects under Applicable Law with respect to Personal Data collected, stored or otherwise processed by Vendor under the Agreement.

(ii) Vendor will notify UPS promptly if it receives any enquiry, complaint, request or claim from a Data Subject relating to Personal Data or Vendor's Processing thereof under or in connection with the Agreement or the Services. Vendor will not respond to any such Data Subject request without UPS's prior written consent except to the extent required by Applicable Law or necessary to confirm the request relates to

UPS.

(e) Retention and Deletion. Vendor may retain Personal Data only for the period of time required for Vendor to perform the Services, or such longer period required by Applicable Law, required pursuant to the Agreement or requested in writing by UPS. Vendor will permanently delete all copies of Personal Data in its possession or control at the expiration of such time period in accordance with any standards provided for deletion of data in the main body of the Agreement or in the Security Exhibit or, if the Agreement does not provide such standards, then in accordance with applicable industry standards for secure deletion of Personal Data.

(f) Cross-Border Transfers.

(i) Vendor may only transfer Personal Data across national borders upon the prior written consent of UPS and in compliance with Applicable Law.

(ii) Vendor will follow UPS's written instructions with respect to any transfer of Personal Data across national borders to adduce adequate safeguards for the privacy of all relevant Data Subjects and will require any applicable subcontractors to do the same. Without limiting the generality of the foregoing, transfers by Vendor (if any) of Personal Data from the European Economic Area, Switzerland or the United Kingdom to another location must be: (A) to a country providing adequate protection of privacy rights (as deemed by the European Commission, the UK Information Commissioner's Office or the Swiss Federal Data Protection and Information Commissioner, as applicable, from time to time); (B) pursuant to Standard Contractual Clauses issued or approved by the European Commission, the UK Information Commissioner's Office or the Swiss Federal Data Protection and Information Commissioner, as applicable, and which remain valid for use for transfers of Personal Data from the applicable jurisdiction at the time of the transfer, provided Vendor has secured any necessary approvals for the transfer from applicable governmental authorities; or (C) authorized by all applicable governmental authorities in the European Economic Area, Switzerland or the United Kingdom, as the case may be, such as through Binding Corporate Rules approved by all applicable governmental authorities.

2. TECHNICAL AND ORGANIZATIONAL SECURITY MEASURES

(a) Standards. Vendor will take appropriate technical and organizational security measures against the unauthorized or unlawful processing of Personal Data and against the loss, alteration or destruction of, or damage to, Personal Data. Such technical and organizational measures will include at a minimum: (i) compliance with the Security Exhibit or, if the Agreement does not include a Security Exhibit, (ii) compliance with applicable industry standards for information security. Vendor acknowledges that its duty to take security measures under this Section 2(a) is in addition to, and does not limit, Vendor's obligations to take appropriate technical and organizational security measures pursuant to Applicable Law.

(b) Privacy Breaches.

(i) For the avoidance of doubt, Vendor agrees that any Privacy Breach that impacts UPS's Personal Data will constitute a Data Breach as defined in the Security Exhibit. In the event of a Privacy Breach, Vendor will therefore comply with all requirements of the Security Exhibit that arise from or relate to a Data Breach.

(ii) If the Agreement does not require Vendor to notify UPS of a Privacy Breach, then Vendor will comply with this Section 2(b)(ii).

(A) Vendor will maintain a documented Privacy Breach action and response plan. If Vendor discovers or is notified of a Privacy Breach that impacts UPS's Personal Data, then Vendor will, once such a Privacy Breach is

confirmed, at its expense: (1) notify UPS without undue delay, but no later than 72 hours of confirming the Privacy Breach; (2) investigate the Privacy Breach; (3) mitigate the effects of the Privacy Breach; and (4) perform post-incident assessments, including those reasonably requested in writing by UPS, and report on the results of such assessment(s) to UPS via an executive level summary.

(B) Subject to Vendor's confidentiality obligations to other customers of Vendor, Vendor will promptly provide UPS with, at a minimum, information to assist UPS in its own reporting obligations relating to the Privacy Breach, including descriptions of the following: (1) the steps taken by Vendor to remedy the Privacy Breach; (2) when the investigation and mitigation has been completed, as well as material progress related to the foregoing; and (3) the details of the Privacy Breach.

(C) For any Privacy Breach, Vendor will be solely responsible for the costs incurred by UPS:

(1) to remedy any such Privacy Breach; (2) to notify all affected Data Subjects of the Privacy Breach; (3) to provide commercially reasonable identity theft protection services to affected Data Subjects, which may include establishing and operating (directly or through a third party) a call center and other support resources to provide information to Data Subjects inquiring about the Privacy Breach.

(iii) Vendor agrees that, in addition to applicable requirements provided in the Security Exhibit or in Section 2(b)(ii):

(A) Vendor's notice to UPS of a Privacy Breach must contain the following: (1) a description of the categories and approximate number of Data Subjects, as well as the categories and approximate number of Personal Data records affected by the Privacy Breach; (2) the name and contact details of any Data Protection Officer appointed by Vendor; and (3) Vendor's assessment, developed through reasonable diligence, of the likely consequences of the Privacy Breach with respect to the affected Personal Data and Data Subjects.

(B) If UPS determines that under Applicable Law any Privacy Breach must be disclosed to a third party, including Data Subjects or governmental authorities (including, but not limited to, any data protection authorities in the European Economic Area), then Vendor shall fully cooperate with and assist UPS in fulfilling UPS's reporting and disclosure obligations.

(C) Vendor shall not disclose the occurrence of any Privacy Breach to any third party without first obtaining UPS's written consent to do so, except to the extent Vendor is required by Applicable Law to make such disclosure prior to obtaining UPS's written consent. Vendor agrees that UPS has the sole right to determine: (1) whether to provide notice of the Privacy Breach to any individuals, regulators, consumer reporting agencies or other third parties; and (2) the contents of such notice, whether any type of remediation may be offered to affected Data Subjects, and the nature and extent of any such remediation.

3. AUDITS AND OVERSIGHT.

(a) Audits. Upon at least thirty (30) days written notice, Vendor will provide to UPS, its auditors (including internal audit staff and external auditors), inspectors, regulators and other representatives who have executed an appropriate confidentiality agreement access to any Vendor owned or managed facility or part of a Vendor owned or managed

facility at which Vendor is providing the Services, to relevant Vendor personnel, and data and records relating to the Services for the purpose of performing audits of Vendor or any of its subcontractors to verify Vendor's compliance with this Exhibit. At no time will UPS have access to Vendor's systems. Vendor will provide commercially reasonable cooperation to UPS and its representatives in connection with any such audit. UPS may perform such audits no more than once in any calendar year unless UPS has confirmation of or a bona fide reasonable suspicion of a Privacy Breach, in which event UPS may perform an audit on a more frequent basis. Vendor will respond in writing within thirty (30) days to all reasonable recommendations UPS provides that result from such audits. Vendor will comply with all reasonable recommendations from UPS that result from such audits relating to Vendor's compliance with this Exhibit.

(b) Documentation and Requests for Information. Vendor will:

(i) Document and provide to UPS upon written request copies of all records of Personal Data Processing activities required to be maintained under Applicable Law;

(ii) Provide to UPS a high-level executive summary of Vendor's then-most recent audit report or review that relates to any Processing of Personal Data received in connection with the Agreement, as conducted by Vendor's external auditors; and

(iii) Provide to UPS a high-level executive summary of the non-privileged reports resulting from any audits performed by Vendor's internal personnel related to Vendor's Processing of Personal Data received in connection with the Agreement.

(c) Cooperation.

(i) If UPS determines that Applicable Law requires an assessment of the privacy impacts of any Processing of Personal Data by Vendor, then Vendor will reasonably cooperate with and facilitate UPS's conduct of the assessment.

(ii) If UPS determines that Applicable Law requires UPS to notify, seek guidance from or consult with a third party, including any governmental authority or representative labor body, concerning Vendor's Processing of Personal Data received in connection with the Agreement, then Vendor will reasonably cooperate with UPS in connection with such advisory request or consultation.

(iii) Vendor will notify UPS promptly if Vendor becomes the subject of, any claim, investigation, audit, suit or enforcement proceeding arising from or relating to Vendor's Processing of Personal Data received in connection with the Agreement; and will reasonably cooperate with UPS and assist UPS with any such claim, investigation, audit, suit or enforcement proceeding arising from or relating to Vendor's Processing of Personal Data received in connection with the Agreement.

(iv) Vendor will cooperate with any reasonable and appropriate steps UPS takes, pursuant to Section 3(d) (Compliance with Exhibit), to stop and remediate any unauthorized use of Personal Data received under the Agreement.

(v) Vendor's cooperation pursuant to this Section 3(c) must include providing access to relevant information, records and personnel.

(d) Compliance with Exhibit. Vendor certifies that Vendor understands the restrictions in this Exhibit and will comply with them. Vendor must notify UPS promptly if Vendor determines it can no longer meet its obligations under this Exhibit. Any failure of Vendor to comply with this Exhibit constitutes a material breach of the Agreement. In such event, UPS may terminate the Agreement or the applicable Processing, effective immediately, at its sole option upon written notice to Vendor without liability or further obligation to Vendor and without prejudice to any other remedies under this Agreement, at law or in equity, and may take other reasonable and appropriate steps to stop and remediate any unauthorized use of Personal Data.

4. DEFINITIONS

(a) "Affiliate" means an entity that a party controls or is controlled by, or with which a party is under common control. For purposes of this definition, "control" means ownership of more than fifty (50%) percent of the voting stock or equivalent ownership interest in an entity.

(b) "Agreement" means the contract between UPS and Vendor that references this Exhibit, including all Schedules, Exhibits, Appendices and other attachments to the contract.

(c) "Applicable Law" means all applicable laws (including those arising under common law), statutes, cases, ordinances, constitutions, regulations, treaties, rules, codes, reporting or licensing requirements, ordinances and other pronouncement having the effect of law of the United States, any foreign country or any domestic or foreign state, county, city or other political subdivision, including those promulgated, interpreted or enforced by any governmental authority. References to "Applicable Law" mean the Applicable Law as may be amended, modified, supplemented, or restated.

(d) "Data Subject" means an identified or identifiable natural person to whom the Personal Data relates.

(e) "Personal Information" means UPS Data (as defined in this Exhibit or the Agreement) that identifies or relates to an identifiable individual (i.e., a person who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to the person physical, physiological, mental, economic, cultural or social identity) or such person's computer system or mobile device, and other similar information regulated by Applicable Law.

(f) "Personal Data" means Personal Information that Vendor accesses or acquires in connection with the Agreement, from UPS or its Affiliates, that UPS or its Affiliates provide to Vendor, or that Vendor collects or acquires on behalf of UPS or its Affiliates.

(g) "Privacy Breach" means any incident involving the accidental, unlawful or unauthorized destruction, loss, alteration, disclosure of or access to Personal Data in Vendor's or its agents' possession or control.

(h) "Process" means any operation or set of operations which is performed by or on behalf of Vendor upon Personal Data received in connection with the Agreement, whether by automatic or manual means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

(i) "Security Exhibit" means the UPS Information Security Agreement for Vendors or such other exhibit, schedule or appendix to the Agreement or provisions set forth within the main body of the Agreement that set forth information security standards for Vendor.

(j) "Services" means the services Vendor is obligated to perform pursuant to the Agreement.

COYOTE→

Load Date: 12/19/2024

BOL NO: 32592035

BILL OF LADING

BRZ

Shipment #: EGLV090400222236

PU#: EGLV090400222236

DEL#: LAW-001595

Pro #:

Shipper

CARTAGE WEST

15902 S MAIN ST

Gardena, CA 90248-2551

P: 1 (971) 295-4762 Name: Miguel Lopez

Consignee

Transform Innovel - W2G

3051 Lakeview Road (truck entrance)

Lawrence, KS 66049

P: 1 (785) 842-9600 281 Name: shawn/drew/kurt

Transformco Appt # LAW-001595 Officer DW

Carrier BRZ W47035

Arrival Date 12/23 Time 0753 Seal K

Unload Date Time

Rec'd 26 plts Exceptions

Rec'd by

3rd Party Freight Charges Bill To

Coyote Logistics (prepaid/third party)

960 North Point Parkway, Suite 150

Alpharetta, GA 30005

SPECIAL INSTRUCTIONS:

Freight Terms:

Prepaid: ___
Collect: ___
3rd Party: X

Qty	Type	Weight	HM(X)	Commodity	LTL Class
~~27~~	PLT	44,000		Coffee products	
				Dimensions: 0.00 x 0.00 x 0.00	
~~27~~	**PLT**	**44,000**		GRAND TOTALS	

26 plts

Where the rate is dependent on value, shippers are required to state specifically in writing the agreed or declared value of the property as follows: "The agreed declared value of the property is specifically stated by the shipper to be not exceeding _____ per _____."

Remit COD to:

Collect:_____ Prepaid:_____ Customer Check Acceptable:_____ COD Amount: $

Note: Liability limitation for loss or damage in this shipment may be applicable. See 49 USC 14706(c)(1)(A) and (B).

Received, subject to individually determined rates or contracts that have been agreed upon in writing between the carrier and shipper, if applicable, otherwise to the rates, classifications and rules that have been established by the carrier and are available to the shipper, on request, and to all applicable state and federal regulations.

Trailer Loaded:
__ by Shipper
__ by Driver

Freight Counted:
__ by Shipper
__ by Driver

The carrier shall not make delivery of this shipment without payment of and all other lawful charges.

Shipper:_____

Shipper Signature / Date:

This is to certify that the above named materials are properly classified, packaged, marked and labeled, and are in proper condition for transportation according to the applicable regulations of the Department of Transportation.

Carrier Signature / Pickup Date:

Carrier acknowledges receipt of packages and required placards. Carrier certifies emergency response information was made available and/or carrier has the Department of Transportation emergency response guidebook or equivalent documentation in vehi Property described above is received in good order, except as noted.