Contract Amendment No. 3 Page 1 of 1

Contract Number 16DH050 between the REGIONAL TRANSPORTATION DISTRICT and Masabi LLC dated May 31, 2017, as amended ("Contract"), is further amended pursuant to General Terms & Conditions Article 12, Change Orders and Contract Amendments, as set forth below:

1. Purpose: The purpose of this Amendment 3 is to allow RTD to sell RTD mobile tickets, through the Masabi interface, on compatible third-party applications. Additionally, this Amendment 3 serves to expand the Contract Statement of Work to include the integration of RTD mobile ticket sales onto the first third party application, the Uber transporation services application ("Uber App"). Masabi's costs and expenses related to the system setup or configuration of any third party application to the RTD Mobile Ticketing Service shall not be charged to RTD as part of its Fixed Fee Implementation Costs and such integrations and implementations shall be of no cost to RTD.

2. Exhibit 2 Insurance and Bond Requirements is hereby replaced in total by the revised Exhibit 2 attached.

3. Exhibit 3—SPECIAL PROVISIONS/ALTERATIONS is hereby replaced in total by the revised Exhibit 3 attached.

4. The Statement of Work to the Contract is hereby amended to include the performance of RTD ticket sales on the Uber App in accordance with the attached Mobile Ticketing Contract 16DH050 Amendment 3 Uber Statement of Work.

Except as provided herein, all other terms and conditions of the Contract remain unchanged and in full force and effect.

Approved as to Legal Form for the Regional Transportation District:

Name: DANA STEELE
Printed Name

By:
Legal Counsel

Date: 4/29/19

Regional Transportation District

By:
David A. Genova
General Manager and CEO

Date: 4.30.19

Contractor: Masabi LLC

By: SARA POULTON
S.V.P GLOBAL SERVICES

Date: 4-26-19

Updated 4/19/19

Regional Transportation District
Denver, CO

Mobile Ticketing
Contract16DH050
Amendment 3
Uber Statement of Work

Uber Mobile App
Ticket Integration with Justride Software Development Kit (SDK)

Statement of Work
4/18/2019

1. Executive Summary

The Regional Transportation District is looking to implement new products and innovative features in the RTD Mobile Ticketing App to provide innovative ways for our customers to purchase RTD products. The purpose of this amendment is to integrate RTD ticketing into the Uber transportation services application ("Uber App") using the Masabi Justride SDK. The Masabi Justride SDK and RTD's mobile ticketing app communicate with Masabi's back office platform for viewing and purchasing available fare products, processing payments and managing mobile tickets. All fees applicable to purchases in the Uber App are consistent with the Contract and only those stated in the Contract, and shall not include any deductions to cover additional expenses resulting from the integration or services. This integration will reflect positively on RTD's branding and service orientation, and RTD's role as a leading public transportation agency in one of the United States' fastest growing, most livable, and most tech-savvy metro regions.

2. Project Description

A. Scope of the Project

2.A.1. SDK Ticket Integration

The ticket integration shall be done by Masabi and Uber via the Justride software development kit ("SDK"). The SDK allows the core functionality of a branded Justride mobile app to be embedded within the Uber App. The Justride SDK shall manage the presentation of RTD mobile tickets to ensure a consistent display for customers, conductors, drivers and revenue protection staff, regardless of how the ticket was purchased. The SDK shall be used to extend sale and activation of RTD's mobile tickets in the Uber App.

Prior to making design and/or configuration changes to the SDK, which could change user experience in the Uber App, user experience in the Justride Hub, or any other aspects of the integration, Masabi shall share release notes to RTD for review, comment and approval prior to implementing changes.

2.A.2. Customer Service, Data and Remittances

The SDK shall allow consistent reporting and customer service interfaces so sales through the Uber App can be managed in-line with existing RTD business processes.

- RTD mobile tickets sold in the Uber App shall be available in RTD's Justride Hub to allow RTD Customer Care agents to service RTD customers. Sales generated through the Uber App shall be distinguishable in the Justride Hub.
- RTD shall have the ability to issue refunds and complimentary tickets to RTD customers who purchased tickets through the Uber App.
- The ticket wallet in the Uber App will not be the same ticket wallet that a customer has in the RTD Mobile Ticketing Application (RTD App).
- The customer shall authenticate an RTD ticket to the Justride SDK through the Uber App, providing a seamless ticket purchasing experience for customers.

Masabi shall provide the materially similar detailed data to RTD from the Uber App ticket sales as it provides to RTD from ticket sales on the Masabi platform for the purpose of identifying an account and its associated transactions, purchases and funding sources. This information shall include UserName, AccountID, Account Verification Flag, Device ID and App ID. RTD shall have the ability and option to test the data accuracy of the Justride Hub prior to release.

Masabi and Uber will provide access to a test build of the Uber / Masabi SDK integration that will be conducted by Uber personnel onsite in Denver, CO. RTD shall use the test version of the Uber app, under observation by an Uber and/or Masabi personnel in a managed test environment, to verify tickets purchased from the Uber app are accurately reflected in the Justride Hub. Up to five devices will be made available by Masabi for testing purposes.

RTD shall have the ability to generate Uber App channel sales reports directly out of the Justride Hub. Masabi shall provide the same type of documentation for credit card fee back-up, chargebacks, uncleared transactions, and related items from the Uber App channel as they do from the RTD Mobile Ticketing App. Masabi shall provide a remittance advice in accordance with the attached sample report, "Third Party App Ticket Integration Revenue Summary sample report". Masabi shall, at some time later, provide RTD with a single remittance advice for sales in the RTD App and the Uber App.

Masabi shall maintain accurate and complete books and records relating to sales of RTD tickets on the Uber App in accordance with the Contract, and such information shall be made available to RTD upon request. RTD has the right to an independent public accountant (the Auditor) examine Masabi's relevant books, records and accounts (including records contained in electronic format on computers or any electronic data storage device) for the purpose of verifying compliance with the Contract. An audit will be conducted no more than once in any twelve (12) month period, with at least thirty (30) days prior written notice. RTD will pay all fees and expenses of the Auditor for the examination; provided, however, that Masabi will bear any such expense if the review or audit results in a significant remedy in favor of RTD or shows Masabi's non-compliance with the Contract.

RTD and Masabi will negotiate in good faith, where feasible and allowed under our Contract, an additional Contract amendment to provide for specific regular data reporting to RTD of aggregate and anonymized user data available to Masabi such as click-thru rates in the RTD App. Masabi will cooperate with RTD, where feasible and allowed under our Contract, to negotiate with Uber for aggregate and anonymized user data for which RTD has a business need, such as click-thru rates in the Uber App.

2.A.3. Fare product appearance and ticket process/purchase flow

Fare Product Appearance

Every RTD fare product presented by the Uber App shall be recognizable as and provide information consistent with existing RTD fare media design, and is subject to review and approval by RTD prior to presentation on the Uber App. Masabi shall work with RTD staff to develop final graphics and information to be included on the visually validated tickets.

Each RTD fare product available on the Uber App shall be capable of being configured. The Universal Ticket shall contain descriptive information that may be used to provide further

information including service and eligibility criteria. Masabi and RTD shall work together to complete a product configuration sheet noting the details of each new product that RTD requests to activate on the Uber App. RTD and Masabi shall work together to finalize the graphic design and appearance of the activated RTD fare products prior to launch in the Uber App.

RTD fare products sold via the Uber App shall allow a customer to activate an RTD fare product only once. Verification of an RTD fare product shall not require any bus or rail on-board equipment. The Uber App shall appropriately handle RTD fare products that become invalid due to business rule changes, fare price increases, fare structure changes, etc. based upon RTD's direction.

At a minimum, the following RTD fare products must be sold via the SDK integration:

Service Level	Fare Product	Fare Level	Estimated Timeframe
Local	3-Hour Pass	Full Fare	May 1, 2019
Local	3-Hour Pass	Discount	May 1, 2019
Local	3-Hour Pass	Youth	May 1, 2019
Regional	3-Hour Pass	Full Fare	May 1, 2019
Regional	3-Hour Pass	Discount	May 1, 2019
Regional	3-Hour Pass	Youth	May 1, 2019
Regional/Airport	Day Pass	Full Fare	May 1, 2019
Regional/Airport	Day Pass	Discount	May 1, 2019
Regional/Airport	Day Pass	Youth	May 1, 2019

RTD and Masabi will negotiate further fare products and changes to existing fare products on a case by case basis as they become generally available in the RTD Fare Tariff Configuration within its own native Justride App.

RTD shall have the opportunity to review and provide feedback to the ticket process/purchase flow in the Uber App and related transactions in the Justride Hub prior to initial launch as well as prior to any changes to that process/purchase flow. Masabi shall facilitate review by providing screen shots or a Click Through prototype of the process flow.

The Uber App purchase flow shall include providing each customer that is purchasing an RTD ticket through the Uber App with a prompt to RTD's Mobile Ticketing Terms and Conditions. The link to the RTD Mobile Ticketing Terms and Conditions must be made available at least the first time each customer purchases an RTD ticket.

2.A.4. Wind Down Period and Termination

Upon RTD's request, Masabi shall remove a fare product from the Uber App within 5 working days of such request. Upon RTD's request, Masabi shall remove the mobile ticketing purchasing capabilities upon written notice and with a wind-down provision to satisfy the use of previously purchased tickets for up to 60 days from the notification date. During the wind down period, no new RTD tickets may be sold, but RTD tickets purchased in the Uber App will continue to function as valid tickets in the RTD Mobile Ticketing App

Upon confirmation of a data or security breach identified by Masabi, RTD or authorized third-party, Masabi shall block the Uber SDK integration from processing ticket purchases, within 48 hours, or less.

2.A.5 Security and Compliance

Masabi shall provide a copy of their PCI-DSS Attestation of Compliance (AOC) and/or SOC2 Type 2 audit report to RTD on an annual basis. Masabi shall be responsible for validating Uber's PCI compliance, reporting such status to RTD in writing on an annual basis. In the event of non-compliance, Masabi shall work with RTD in good faith to resolve the non-compliance issue to RTD's satisfaction.

Masabi shall provide RTD with written notification of incidents impacting service to RTD ticket sales in the Uber App or RTD data transmitted to Uber via the SDK integration.

Upon discovery, Masabi shall provide RTD with written notification of any known data breach by Uber which may impact RTD customer information in accordance with RTD security requirements, which notification shall include proposed measures for appropriate and timely support for forensic analysis in the event of a data security breach.

All RTD passenger card data shall remain in the RTD card data environment hosted at Masabi. There shall be no substantive changes to the RTD Card Data Environment with the implementation of the SDK.

The Masabi Justride SDK shall ensure any and all data used/ gathered for the purpose of a sale of a RTD mobile ticket is secure. Only data necessary to issue RTD tickets in the Uber App and data necessary for revenue reconciliation shall be made available to Uber.

Wherever cardholder data is processed, Masabi must comply with RTD's Cardholder Data Environments requirements.

3. Performance Measures

A. Verification and Testing

Masabi and the Uber App developer, Uber, shall conduct a comprehensive testing and quality assurance program that demonstrates, to the satisfaction of RTD, that system functionality has materially been provided, that tickets and revenue are accurately processed, that the system design

has been satisfied, that the system is properly configured, and that the system is stable and ready for use prior to launch of RTD ticket sales in the Uber App. Demonstrated evidence of properly conducted comprehensive testing and quality assurance may include test results and/or a demonstration of the Uber App integration. RTD shall have the option to conduct audits and testing, at RTD's discretion before and/or after the ticket integration.

B. Project Milestones

#	Milestone	Description	Delivery Date	Cost Estimate
1	Uber App Integration	Integrate with the Uber App using the Justride SDK to sell RTD tickets.	May 1st, 2019	$0
2	Masabi's PCI-DSS Attestation of Compliance	Attestation of compliance for PCI-DSS that includes the Uber integration/SDK	Prior to May 1, 2019 or the integration launch date.	$0

4. Cost

Any costs associated with this implementation and any further work related thereto shall be borne by Masabi and shall not be passed through to RTD. All fees applicable to purchases in the Uber App are consistent with and only those stated in the contract which shall not include any deductions to cover additional expenses resulting from the integration or services.

5. Appendix Materials

The following appendix materials are included for Contractor review and are incorporated into this Statement of Work:

☐ Third Party App Ticket Integration Revenue Summary sample report

☐ RTD Release and Change Management Vendor Process_SOW_rev6

☐ RTD Data Protection

☐ RTD System Security

☐ RTD Custom Software Development

☐ Cardholder Data Environment

Revenues Summary
UBER - EXAMPLE
December 2018

FOR ILLUSTRATION PURPOSES ONLY

masabi

JUSTRIDE HUB									PAYMENT GATEWAY									
	Transactions (#)		Amount (USD)						Amount (USD)									
Date	Purchases	Refunds	Purchases		Refunds		Total		Purchases		Refunds		CB Received		CB Represented		Total	
Sat-01-Dec	132	-	USD	1,508.75	USD	-	USD	1,508.75	USD	1,489.75	USD	-	USD	-	USD	-	USD	1,489.75
Sun-02-Dec	86	-	USD	946.25	USD	-	USD	946.25	USD	965.25	USD	-	USD	-	USD	-	USD	965.25
Mon-03-Dec	140	-	USD	1,331.00	USD	-	USD	1,331.00	USD	1,331.00	USD	-	USD	-	USD	-	USD	1,331.00
Tue-04-Dec	133	2	USD	1,170.25	USD	(11.25)	USD	1,159.00	USD	1,170.25	USD	(11.25)	USD	-	USD	-	USD	1,159.00
Wed-05-Dec	168	-	USD	1,386.50	USD	-	USD	1,386.50	USD	1,386.50	USD	-	USD	-	USD	-	USD	1,386.50
Thu-06-Dec	158	-	USD	1,290.75	USD	-	USD	1,290.75	USD	1,290.75	USD	-	USD	-	USD	-	USD	1,290.75
Fri-07-Dec	219	-	USD	2,051.50	USD	-	USD	2,051.50	USD	2,051.50	USD	-	USD	-	USD	-	USD	2,051.50
Sat-08-Dec	133	-	USD	1,440.00	USD	-	USD	1,440.00	USD	1,440.00	USD	-	USD	-	USD	-	USD	1,440.00
Sun-09-Dec	94	-	USD	1,988.25	USD	-	USD	1,988.25	USD	1,988.25	USD	-	USD	-	USD	-	USD	1,988.25
Mon-10-Dec	157	-	USD	1,358.00	USD	-	USD	1,358.00	USD	1,358.00	USD	-	USD	-	USD	-	USD	1,358.00
Tue-11-Dec	168	-	USD	1,440.75	USD	-	USD	1,440.75	USD	1,440.75	USD	-	USD	-	USD	-	USD	1,440.75
Wed-12-Dec	155	-	USD	1,269.75	USD	-	USD	1,269.75	USD	1,269.75	USD	-	USD	-	USD	-	USD	1,269.75
Thu-13-Dec	187	-	USD	1,502.50	USD	-	USD	1,502.50	USD	1,502.50	USD	-	USD	-	USD	-	USD	1,502.50
Fri-14-Dec	189	5	USD	1,682.25	USD	(37.50)	USD	1,644.75	USD	1,682.25	USD	(37.50)	USD	-	USD	-	USD	1,644.75
Sat-15-Dec	105	-	USD	1,262.25	USD	-	USD	1,262.25	USD	1,262.25	USD	-	USD	-	USD	-	USD	1,262.25
Sun-16-Dec	80	-	USD	1,057.50	USD	-	USD	1,057.50	USD	1,057.50	USD	-	USD	-	USD	-	USD	1,057.50
Mon-17-Dec	147	-	USD	1,444.00	USD	-	USD	1,444.00	USD	1,444.00	USD	-	USD	-	USD	-	USD	1,444.00
Tue-18-Dec	158	-	USD	1,329.25	USD	-	USD	1,329.25	USD	1,329.25	USD	-	USD	-	USD	-	USD	1,329.25
Wed-19-Dec	158	-	USD	1,470.00	USD	-	USD	1,470.00	USD	1,470.00	USD	-	USD	-	USD	-	USD	1,470.00
Thu-20-Dec	179	-	USD	1,869.50	USD	-	USD	1,869.50	USD	1,869.50	USD	-	USD	-	USD	-	USD	1,869.50
Fri-21-Dec	150	2	USD	1,554.75	USD	(11.00)	USD	1,543.75	USD	1,554.75	USD	(11.00)	USD	-	USD	-	USD	1,543.75
Sat-22-Dec	96	-	USD	1,199.25	USD	-	USD	1,199.25	USD	1,199.25	USD	-	USD	-	USD	-	USD	1,199.25
Sun-23-Dec	93	-	USD	1,254.25	USD	-	USD	1,254.25	USD	1,254.25	USD	-	USD	-	USD	-	USD	1,254.25
Mon-24-Dec	61	-	USD	698.75	USD	-	USD	698.75	USD	698.75	USD	-	USD	-	USD	-	USD	698.75
Tue-25-Dec	40	-	USD	429.00	USD	-	USD	429.00	USD	429.00	USD	-	USD	-	USD	-	USD	429.00
Wed-26-Dec	147	-	USD	2,268.50	USD	-	USD	2,268.50	USD	2,268.50	USD	-	USD	-	USD	-	USD	2,268.50
Thu-27-Dec	206	-	USD	2,811.50	USD	-	USD	2,811.50	USD	2,811.50	USD	-	USD	-	USD	-	USD	2,811.50
Fri-28-Dec	194	-	USD	2,788.50	USD	-	USD	2,788.50	USD	2,788.50	USD	-	USD	-	USD	-	USD	2,788.50
Sat-29-Dec	164	-	USD	3,418.25	USD	-	USD	3,418.25	USD	3,418.25	USD	-	USD	-	USD	-	USD	3,418.25
Sun-30-Dec	133	-	USD	2,619.50	USD	-	USD	2,619.50	USD	2,619.50	USD	-	USD	-	USD	-	USD	2,619.50
Mon-31-Dec	148	-	USD	1,918.25	USD	-	USD	1,918.25	USD	1,918.25	USD	-	USD	-	USD	-	USD	1,918.25
Total Fare Receipts:	**4,378**	**9**	**USD**	**49,759.50**	**USD**	**(59.75)**	**USD**	**49,699.75**	**USD**	**49,759.50**	**USD**	**(59.75)**	**USD**	**-**	**USD**	**-**	**USD**	**49,699.75**

RTD IT Release and Change Management Process for Vendors

The purpose of this document is to ensure that Vendors shall follow the methods and processes in the RTD IT Change Management Internal Work Instructions. Doing so will facilitate the efficient and prompt handling of all changes and releases and the maintenance of service level objectives. The approval process will serve to maintain the balance between the need for change and the potential detrimental impact of changes. The following are supplementary to the RTD IT Change Management Internal Work Instructions and apply specifically to Vendors:

- Non-Emergency change and release requests for test environments, user acceptance testing environments, or production environments shall be submitted 10 calendar days in advance.
    - Requests shall be reviewed and, if accepted, approved in the monthly CAB (Change Advisory Board) which will consist of the CIO, IT Managers, IT Service Delivery Team, and the Vendor.
- Vendor must provide test scripts, test results, risk analysis, release notes, data flow, and process flow related to the particular change *before* installing into testing environments and user acceptance testing environments.
- Emergency change and release requests for production must be submitted as soon as possible prior to release.
    - Requests shall be reviewed by an eCAB (Emergency Change Advisory Board) and, if accepted, approved for production deployment.
    - The eCAB shall be held as soon as possible after receipt of the emergency change/release request.
- All releases to test environments, user acceptance testing environments, or production environments shall minimally require the following:
    - infrastructure or application documentation (i.e. data flow and process flow)
    - risk or impact analysis for the affected application(s)
    - test plan including type of testing to be performed
    - installation or release plan (change plan)
    - back out plan
- RTD shall review and, if accepted, approve all results before moving a release forward to the next test environment, user acceptance testing environment, or production environment.
- RTD uses a number of tools and processes in regards to the Release and Change Management Process, which the Vendor shall utilize as needed and as instructed by the Release/Change Manager.

RTD Access to Vendor Environments

- RTD shall be provided access into the Vendor test environments, user acceptance testing environments, and production environments to evaluate, test, and accept projects prior to production deployment for Vendor hosted applications and systems.

Fully Outsourced Services that will Affect RTD Business Processes

- Changes that affect RTD's ability to conduct business will go through the RTD's change process.
- Non-Emergency change and release requests shall be submitted 10 calendar days in advance.
    - Requests shall be reviewed and must be approved by the CAB.
- The Vendor shall notify RTD in writing before commencing any work effort on internal or external hardware, software, or business process changes that will affect RTD's ability to conduct business.
    - Changes shall not commence before the request is reviewed and approved by RTD in order to allow RTD to first plan, review, and implement the necessary internal and external changes to accommodate the Vendor's request.
- *RTD must be notified in writing of any changes impacting outsourced services provided to the Vendor by third party vendors*, when such changes could affect RTD's ability to conduct business.

Vendor Access to RTD Environments

- RTD shall provide the Vendor with remote and unique access to the individuals logging into environments for auditing purposes if deemed necessary for a project.

RTD Release and Change Management Point of Contact

- The Release/Change Manager shall be the point of contact for RTD in regards to all Change and Release Management activities.

Data Protection

"**RTD Data**" means all information processed or stored on computers or other electronic media by RTD or on RTD's behalf, or provided to Contractor for such processing or storage, as well as information derived from such information. RTD Data includes, without limitation: (i) information on paper or other non-electronic media provided to Contractor for computer processing or storage, or information formerly on electronic media; (ii) information provided to Contractor by RTD customers, users, employees, or other third parties; and (iii) Sensitive RTD Data as that term is defined below.

"**Sensitive RTD Data**" means data that poses a risk to RTD, its employees, customers, and the public if improperly disclosed or accessed, including without limitation personally identifiable information, financial information, protected health information, proprietary information, critical infrastructure information, and other confidential information.

1. **Contractor's Access and Use of RTD Data.** Unless it receives RTD's prior written consent, Contractor shall not: (i) access, process, or otherwise use RTD Data other than as necessary to facilitate the work under this Agreement; (ii) give any of its employees access to RTD Data except to the extent that such individual needs access to facilitate performance under this Agreement; (iii) give any third party access to RTD Data, including without limitation Contractor's other customers, except Contractor's subcontractors as set forth in subsection (D) below; and (iv) sell RTD Data to any third parties. Notwithstanding the foregoing, Contractor may disclose RTD Data as required by applicable law or by proper legal or governmental authority. Contractor shall give RTD prompt notice of any such legal or governmental demand and reasonably cooperate with RTD in any effort to seek a protective order or otherwise to contest such required disclosure, at RTD's expense.
2. **Ownership of RTD Data**. RTD possesses and retains all rights, title, and interest in and to RTD Data, and Contractor's use and possession thereof is solely on RTD's behalf. RTD may access and copy any RTD Data in Contractor's possession at any time, at no cost to RTD. Contractor shall reasonably facilitate such access after receiving RTD's request.
3. **Retention and Deletion of Data.** Contractor shall follow any commercially reasonable written instructions from RTD regarding retention and erasure of RTD Data, provided however, Contractor shall not retain any RTD Data beyond thirty (30) days after termination of this Agreement unless otherwise requested and approved by RTD. RTD Data shall be available to RTD to retrieve at any time and at no additional charge throughout the term of this Agreement and for no more than thirty (30) days after expiration or termination of this Agreement for any reason. Upon written request, promptly after erasure of RTD Data or any copy thereof, Contractor shall certify such erasure to RTD in writing. In purging or erasing RTD Data as required by this Agreement, Contractor shall leave no data recoverable on its computers or other media, to the maximum extent commercially feasible.
4. **Subcontractors.** Contractor shall not permit any subcontractor to access RTD Data unless such subcontractor is subject to a written contract with Contractor agreeing to protect the data, with terms and conditions reasonably consistent with those of this provision. Contractor shall exercise reasonable efforts to ensure that each subcontractor complies with all of the terms of this Agreement related to RTD Data.
5. **Applicable Law.** Contractor shall comply with all applicable laws and regulations governing the handling of RTD Data and shall not engage in any activity related to RTD Data that would place RTD in violation of any applicable law, regulation, government request, or judicial process.
6. **Data Breach.** Contractor shall exercise commercially reasonable efforts to prevent unauthorized exposure or disclosure of RTD Data. In the event of a confirmed data breach or unauthorized

disclosure, Contractor shall (i) notify RTD by telephone within 24 hours of discovery of the breach or unauthorized disclosure; and (ii) cooperate with RTD and law enforcement agencies, where applicable, to investigate and resolve the matter, including without limitation notifying injured third parties. Contractor shall give RTD prompt access to such records related to a data breach or unauthorized disclosure as RTD may reasonably request, provided that Contractor shall not be required to provide RTD with records belonging to, or compromising the security of, Contractor's other customers. In the event of a confirmed data breach or unauthorized disclosure caused solely by the act or omission of the Contractor or any of its agents, employees, or subcontractors, to the extent required by applicable law, the Contractor shall pay or reimburse RTD for any costs incurred with respect to: (i) notification to all affected individuals using a reasonable method (e.g., email or standard regular mail; overnight courier is not reasonable); (ii) one year of credit monitoring for all affected individuals; and (iii) any other penalties and fines related to the breach or unauthorized disclosure as required by applicable law. The provisions of this Subsection (F) do not limit RTD's other rights and remedies, if any, resulting from a data breach or unauthorized disclosure.

7. **Disaster Recovery and Business Continuity.** Contractor shall maintain and implement a disaster recovery plan to ensure the recovery of data lost due to operator error, system error or other unforeseen circumstances. Upon written request, Contractor shall provide RTD with a copy of its current disaster recovery plan and all updates to these plans during the term of this Agreement. In addition, Contractor shall maintain and implement a business continuity plan for the term of this Agreement. Upon RTD's written request, Contractor will issue to RTD a summary statement on the design of the business continuity management framework. The Business Continuity Plan is confidential and Contractor will not provide actual plans nor will it allow customers to participate in business continuity activities.
8. **Multi-Tenancy.** Should RTD Data be processed or stored on multi-tenancy servers, security controls shall be in place to ensure that a tenant with weak security settings cannot affect or interfere with the security of RTD Data as well as to ensure that data is not co-mingled within the server or stack.
9. **Security Control Non-Disclosure.** The Contractor shall not publish or disclose in any manner the details of any safeguards designed to protect RTD Data without prior consent of RTD.

System Security

1. **Control Activities.** At RTD's request, Contractor shall provide RTD the opportunity to review the design and execution of the control activities performed by the Contractor as relates to the support and security of RTD's operations and the data, systems, networks, or facilities that are relevant to providing services to RTD (as applicable to the scope of services).
2. **Disaster Recovery and Business Continuity.** Contractor shall maintain and implement a disaster recovery plan to ensure continuity of the services provided to RTD pursuant to this Agreement and the recovery of any data or functionality lost due to operator error, system error or other unforeseen circumstances. Upon written request, Contractor shall provide RTD with a copy of its current disaster recovery plan and all updates to these plans during the term of this Agreement. In addition, Contractor shall maintain and implement a business continuity plan for the term of this Agreement. Upon RTD's written request, Contractor will issue to RTD a summary statement on the design of the business continuity management framework. The Business Continuity Plan is confidential and Contractor will not provide actual plans nor will it allow customers to participate in business continuity activities.
3. **On Premises Systems.** Should the Contractor require the installation of an on-premises system to support the services, either (a) at minimum, RTD must have read-only administrative access to the system to verify security controls, or (b) the system must be separated from the RTD internal network using, at minimum, logical access controls to restrict the system to the least necessary access to perform services under the Agreement. Any system placed on the RTD network must be capable of conforming to RTD's security policies and standards and architectural standards, including but not specifically limited to the following requirements: must have a supported operating system or firmware version; must be patched or updated to close security vulnerabilities; must support access controls that maintain user least-privilege; must be able to undergo configuration hardening; must be capable of running antimalware software (endpoints only).
4. **Multi-Tenancy.** Should a multi-tenancy architecture be used, Contractor shall implement and maintain access controls to adequately separate the functions of each environment such that actions taken in or for another customer do not affect the security of RTD's data or operations on the same architecture.
5. **SOC 2 Type 2 Report.** Fourteen calendar days after receipt of the NTP, Contractor shall provide to RTD their most recent Service Organization Control (SOC) 2 Type 2 report pertaining to the scope of services provided to RTD. Thereafter for the term of this Agreement, the Contractor shall provide an updated SOC 2 Type 2 report to RTD on an annual basis. If Contractor fails to provide an updated SOC 2 Type 2 report, then Contractor will notify RTD in writing of a date when the SOC 2 Type 2 report will be made available to RTD, except that the updated SOC 2 Type 2 report must be made available to RTD no later than 18 months after the last report was produced. If Contractor's SOC 2 Type 2 report is qualified, then Contractor will provide a written Plan of Actions and Milestones to notify RTD of what actions they are taking to correct any findings and the expected resolution date for those corrections. Should a SOC 2 Type 2 not be performed or available, an alternative third-party control audit report may be acceptable to RTD with prior notice, sufficiency of criteria review, and approval from RTD.
6. **Risk Assessment.** Contractor must perform a risk assessment prior to any major system change or installation that impacts the storage, collection, transmission or processing of RTD Data, including but not specifically limited to the addition of new systems, removal of systems, major upgrades, changes in data flows affecting RTD Data, or changes in security controls related to RTD Data. Identified risks and mitigation plans must be reviewed with RTD prior to change

implementation. Risks that cannot be mitigated must be presented to RTD for review and acceptance prior to change implementation.

Custom Application Development

"Custom application" means any code that is not generally commercially available, but was created for RTD, that is used to create, modify, integrate, or support computer functions for end users.

1. **Risk Assessment.** Contractor must perform a risk assessment prior to any major development effort that will impact the storage, collection, transmission, or processing of RTD Data, including but not limited to the implementation of a new application, implementation or major changes to components that collect more or different data, changes that allow the application to use, process, or retain data in significantly different ways, major changes to the data flow throughout the system, or changes in security controls related to data management.
2. **Design Specifications.** Application design documents, requirements, or specifications must include a description of all custom-developed or integrated application features that are designed to address data security and privacy risks. Contractors shall not publish or disclose in any manner, without written consent of an RTD attorney and the Manager of Cybersecurity, the details of any safeguards designed, or developed by the contractor. The developed or integrated security features must, at minimum, complement those risks uncovered in the risk assessment and meet RTD's design requirements in the following areas:
    a. **Logging.** The product must support or facilitate logging and forwarding of application security events for operational failure, security incident, and security monitoring purposes.
    b. **Access Control and Authority.** The product must contain features that allow administrators to control user and system access to functions, features, or system components a need-to-know basis. The product must be able to operate with user level authority, and must not require that a user be logged in as an administrator in order to operate properly. Access control functions must validate a user's identity before access can be established or changed (for example, by sending an expiring token to a side channel). Users and administrators of the product must be able to self-manage their credentials (for example, establish a password and perform password resets).
    c. **Compatibility with Security Functions and Products.** The product must be capable of operating concurrent with well-known industry security products, such as antimalware programs, log collection and monitoring agents, and web application firewalls. The product must tolerate periodic vulnerability scanning, operating system patching and upgrades, and basic system hardening (for example, changing of default passwords and disabling unnecessary services). Products that require an out-of-support operating system or do not tolerate operating system patching for at least three years from the date of purchase will be considered out of compliance with the Minimum Viable Use requirement.
    d. **Data Security.** Products that are intended for the storage, processing, or transfer of sensitive data must support strong encryption at rest. Products that communicate over the Internet, for example, for authentication, maintenance purposes, or remote management, must use unbroken encrypted communication methods. Products that store sensitive data must tolerate and/or enforce purging data that RTD determines no longer has a business need to be retained.
3. **Separation of Duties.** Development, test, and production software instances must be kept strictly separate through physically separate computer systems or separate directories or libraries with strictly enforced access controls. Separate staff must perform development (programming tasks) and staging and operations tasks. Workers who have been involved in the development of the application must not be involved in the formal validation of the application.

4. **Contractor Staffing.** RTD reserves the final right of approval for all contracted developers performing application development on behalf of RTD. External contractors involved in the development of RTD applications must read and abide by RTD's application security requirements (as described in this document). Contractors who fail to abide by or cannot understand the requirements are subject to immediate dismissal.
5. **Secure Coding.** All source code must be developed using industry-recognized secure coding practices (for example, OWASP Secure Coding Practices or SEI CERT from Carnegie Mellon University) by developers who are certified in such practices or receive training no less than annually. Secure coding practices must include, at minimum, (a) input validation, (b) proper password handling, (c) manual and/or automated code reviews that address the OWASP Top 10 vulnerabilities.
6. **Source Code Management.** Source code created under this Contract is considered "RTD Data" under RTD's Data Protection requirements and is solely owned by RTD. Also in accordance with RTD's Data Protection requirements, source code that facilitates sensitive business functions such that, if released, could lead to harm to RTD's employees, patrons, or ability to provide service, must be access controlled. Public-facing non-compiled source code (for example, when used in web application programming) must be obfuscated to hide the business logic behind the application. Source code must otherwise be stored in an access-controlled code management repository to prevent unauthorized changes.
7. **Documentation.** All features and functions of the developed application must be fully revealed in the documentation provided to RTD. Covert software features or functions are incompatible with RTD's business practices. All specification, design, coding, and testing documentation used to develop RTD applications must be provided to RTD as necessary to facilitate review and implementation of the application, with final, "as-built" versions of the documentation to be provided at the conclusion of the development project.
8. **Open Source and Third Party Components.** All open source and external software packages and versions used within the application must be documented. These include but are not limited to linked libraries, database applications, and encryption packages. Contractors shall provide proof of license for all licensed software used to perform application development and all third-party libraries included within the application. The use of public domain, shareware, or freeware software is subject to RTD's review and written approval.
9. **Test Data.** Contractors may never use real (i.e. production) data to perform testing of applications that are designed to collect, process, store, or transmit sensitive data. Test data sets may be fabricated, or may be produced from sanitized production data. Contractor must ensure that the sanitization process has completely removed and/or replaced all details that may be valuable, critical, sensitive, or private before sanitized production data is used for testing.
10. **Security Testing.** Contractor must conduct initial vulnerability analysis and penetration testing prior to the release of the application. Should the contractor not have a relationship or resources to perform such testing, or should such testing be excluded from the Scope of Work, the contractor must collaborate with RTD and RTD's agents (if applicable) to perform security testing prior to launch of the custom application.
11. **Vulnerability Remediation.** Contractor must support the remediation of exploitable security vulnerabilities discovered in the application by the Contractor, RTD, or an external party during security testing, security incident reporting, or in the normal course of operations for a period of no less than three years from the first day that the custom application was used in production. Critical or high-risk exploitable vulnerabilities (categorized by the Common Vulnerability Scoring System) must be repaired and re-tested to confirm repair within thirty (30) days of when the vulnerability was first reported to the Contractor. The Contractor must produce a plan of actions and milestones to repair medium or lower-rated vulnerabilities on a timetable agreed by RTD, but

in no greater than 180 days from the date the vulnerability was reported to the Contractor. Repair plans may consist of a custom code adjustment (version), patch, or upgrade.

12. **Product Ownership.** RTD shall retain ownership and the unlimited right to use, transfer, or modify all finished materials, components, and proposed concepts associated with the custom application.

Cardholder Data Environments

"Cardholder Data (CHD)" means the full magnetic stripe contents of a credit card plus any of the following: cardholder name, expiration date, service code.

"Cardholder Data Environment (CDE)" means an area of a computer system or network that possesses cardholder data or sensitive authentication data (related to cards) and those systems that directly attach to such environments or otherwise support cardholder processing, storage, or transmission.

1. **PCI-DSS Compliance.** Cardholder Data Environments shall comply with all requirements of the current effective version of the Payment Card Industry Data Security Standard (PCI-DSS) for Level 2 merchants throughout the lifecycle of the environment.
2. **Scope.** If applicable and necessary under the scope of services, RTD shall disclose to the Contractor where cardholder data is stored in the target architecture such that it can be protected per the requirements below.
3. **CDE Boundary Controls.** To limit the scope of PCI controls, Contractor shall separate systems that collect, store, process, or transmit cardholder data from those that do not using network security control methods that are (a) deemed sufficient under the PCI-DSS standard and (b) validated for sufficiency to the frequency required in the PCI-DSS.
4. **Multi-Tenancy.** It is preferred that CDEs be separated by function and by customer. Should any of the CDEs be combined (across RTD, or across RTD and multiple customers, ex. multi-tenancy), in accordance with the PCI-DSS, Contractor shall implement and maintain access controls to adequately separate the functions of each environment such that actions taken in or for one CDE do not affect the security of other CDEs on the same architecture.
5. **Supporting Systems Compliance.** Contractor shall maintain all systems that do not contain cardholder data but provide supporting services to those systems that do (for example, to provide support, reporting functions, or similar) in a manner consistent with PCI-DSS requirements.
6. **Control Responsibilities.** Contractor shall participate with RTD in developing and reviewing a compliance scope matrix to document responsibility for the design and execution of PCI-compliant controls.
7. **Attestation of Compliance.** Contractor shall provide to RTD on request, and otherwise no less than annually, an Attestation of Compliance signed by a qualified or internal security assessor (QSA or ISA) as validation of the controls under vendor's scope.
8. **Compliance Auditing.** Contractor shall permit RTD to test, inspect, or audit Contractor systems assigned to RTD or data residing on Contractor hosted systems in order to support RTD's compliance responsibilities.
9. **Corrective Actions.** Should defects in security or PCI compliance be discovered by Contractor or by RTD, Contractor shall provide a Plan of Actions and Milestones that details the actions and timeline to resolve. Contractor shall resolve security and compliance defects in scope of the Contractor's supported services at no additional charge to RTD.
10. **Compliance Impact Assessments.** A Compliance Impact Assessment must be performed for any major changes to Cardholder Data Environment, including but not specifically limited to the addition of new systems, removal of systems, major upgrades, changes in data flows affecting cardholder data, or changes in security controls related to cardholder data. Identified risks and mitigation plans must be reviewed with RTD prior to change implementation. Risks that cannot be mitigated must be presented to RTD for review and acceptance prior to change implementation.

EXHIBIT 2

INSURANCE AND BOND REQUIREMENTS

INSURANCE REQUIREMENTS

General

Contractor shall procure and maintain, and shall require that its **Subcontractors** purchase and continuously maintain in full force and effect for the Contract period specified herein, all insurance policies specified in this Exhibit. The Contractor shall forward updated certificates of insurance and endorsement(s) when policies are renewed or changed.

The insurance required hereunder shall not be interpreted to relieve the **Contractor** of any obligations under the Contract and liability of **Contractor and Subcontractors** under this Exhibit shall not be limited to coverage provided under said insurance policies. The **Contractor and Subcontractors** shall remain solely and fully liable for all deductibles / Self Insured Retentions (SIR's) and amounts in excess of the coverage actually realized.

Commercial General Liability Insurance

The **Contractor and Subcontractors** shall provide and maintain Commercial General Liability Insurance (broad form coverage) insuring against claims for bodily injury, property damage, personal injury and advertising injury. By its terms or appropriate endorsements such insurance shall include the following coverage: Bodily Injury, Property Damage, Fire Legal Liability (not less than the replacement value of the portion of the premises occupied), Personal Injury, Blanket Contractual, Independent Contractors, Premises Operations, Products and Completed Operations.

If Commercial General Liability Insurance or other form with a general aggregate limit is used, either the aggregate limits shall apply separately to this project/location, or the general aggregate limit will be twice the required occurrence limit.

Amount of Coverage:	$1,000,000 per occurrence $2,000,000 aggregate

Automobile Liability Insurance

The Contractor and Subcontractors shall provide Automobile Liability Insurance insuring against claims for bodily injury, property damage, and physical damage, including Comprehensive and Collision, arising out of the ownership, maintenance or use of all owned/leased as well as hired and non-owned vehicles (Symbols 1, 8 and 9) used in the performance of the Work.

Amount of Coverage:	$1,000,000 combined single limit

Workers' Compensation and Employer Liability Insurance

The **Contractor and Subcontractors** shall provide Workers' Compensation Insurance sufficient to meet its statutory obligations to provide benefits for employees with claims of bodily injury or occupational disease (including resulting death).

The **Contractor and Subcontractors** shall provide Employer Liability Insurance covering its legal obligation to pay damages because of bodily injury or occupational disease (including resulting death) sustained by an employee.

Amount of Coverage:	$1,000,000 bodily injury by accident $1,000,000 bodily injury by disease $1,000,000 policy limit

Umbrella/Excess Liability

The **Contractor and Subcontractors** shall provide Umbrella/Excess Liability insurance limits as follows:

(Contracts $5,000,000 and under)	
Amount of Coverage:	$5,000,000 per occurrence $5,000,000 aggregate
(Contracts above $5,000,000)	
Amount of Coverage:	$10,000,000 per occurrence $10,000,000 aggregate

This excess insurance shall be at least as broad as the **Contractor's and Subcontractors'** primary Commercial General Liability, Commercial Auto Liability and Employer Liability insurance.

Professional Liability

This insurance requirement applies when a supplier has a professional designation or license and/or is providing professional services. The minimum limit for architects and engineers is $5,000,000 per occurrence and in the aggregate and may be increased depending upon the nature of the services to be provided to RTD.

The **Contractor and Subcontractors** shall provide Professional Liability Insurance covering liability arising out of any negligent act, error, mistake or omission in the performance of Contractor's services under this Contract. This insurance is to be maintained for the duration of the Contract and for a minimum of two (2) years following completion of this Contract.

(Contracts $1,000,000 and under)	
Amount of Coverage:	$2,000,000 per occurrence $2,000,000 aggregate
(Contracts above $1,000,000)	
Amount of Coverage:	$5,000,000 per occurrence $5,000,000 aggregate

Cyber Risk Insurance

This insurance requirement applies when a third party will be using, storing or accessing private, confidential or protected information on behalf of RTD. This insurance shall be maintained for the duration of the Contract and a minimum of two years following its termination.

Amount of Coverage:	$2,000,000 per occurrence $2,000,000 aggregate

Coverage to include:

Network Security & Privacy
Media Liability
Regulatory Defense & Penalties
Privacy Breach Costs
PCI Fines and Penalties
Data Restoration
Network Business Interruption
Cyber Extortion

Endorsements, Waivers and Related Requirements

Prior to performing any Work, the **Contractor** agrees to furnish RTD with a certificate of insurance for each of the Contractor's and its **Subcontractors'** policy(s). All insurance companies shall provide RTD with 30 days' advance notice of cancellation of policy(s) by Registered or Certified mail. Certificates of insurance shall be provided to the Contract Administrator designated for Notices on the Contract Award and Signature page.

All insurance policies required hereunder shall contain or be endorsed to contain the following provisions:

1. For the insurance specified herein, RTD and its members, directors, officers, employees and agents shall be named as an additional insured (except Workers' Compensation).
2. For claims covered by the insurance specified herein, said insurance coverage shall be primary and non-contributory insurance with respect to the additional insured parties, and their respective members, directors, officers, employees and agents.
3. The insurance specified herein shall contain a waiver of subrogation in favor of RTD as set forth below:

   All policies of insurance carried by the **Contractor or Subcontractors** pursuant to this Contract shall expressly waive any right on the part of their insurer(s) against RTD and its members, directors, officers, employees and agents, which right, is hereby expressly waived to the full extent permitted by law.
4. The insurance shall apply separately to each insured and additional insured party against whom a claim is made or suit is brought, except with respect to the limits of the insurer's liability.
5. The amount of insurance must be "at least" equal to the limits of liability shown herein.

Acceptable Insurance Company

The insurance company providing any of the insurance coverage required herein shall have at a minimum an AM Best Key Rating of A, with a Financial Strength of VII or higher, (i.e., A VII, A VIII, A IX, A X, etc.) or equivalent from similar rating agency and shall be subject

to approval by **RTD**. Each insurance company's rating as shown in the latest AM Best Key Rating Guide shall be fully disclosed and entered on the required certificate of insurance.

Premiums, Deductibles and Self-Insured Retentions

The **Contractor and Subcontractors** shall be responsible for payment of premiums for all of the insurance coverages required hereunder. The **Contractor** further agrees that for each claim, suit or action made against insurance provided hereunder, with respect to all matters for which the **Contractor or Subcontractors** are responsible hereunder, the **Contractor** shall be solely responsible for all deductibles and self-insured retentions. Any deductibles or self-insured retentions over $25,000 in the **Contractor's and Subcontractors'** insurance must be declared and approved in writing by **RTD**. To apply for approval for a level of retention in excess of $25,000 the **Contractor or Subcontractor** shall notify RTD of the level of retention and provide a current financial statement, if not previously submitted, documenting the ability to pay claims falling within the stated self-insured retention. If RTD does not approve the Contractor's or Subcontractors' self-insured retention, the Contractor or Subcontractor shall, at the option of RTD, either: (i) cause the insurer to reduce or eliminate such self-insured retention as respects this contract with RTD; or (ii) procure a bond guaranteeing payment of losses and related investigations, claims administration and defense expenses.

Certificate of Insurance

The **Contractor** will deliver to RTD a certificate of insurance with respect to each required policy to be provided by the **Contractor and Subcontractors**. The required certificates must be signed by the authorized broker or agent representative of the insurance company shown on the certificate and authorized to bind the named underwriter(s) and their company to the coverage, limits and termination provisions shown thereon. All endorsements shall be attached to the certificates of insurance when submitted to **RTD**. A certified, true and exact copy of each insurance policy (including renewal policies) required under this contract shall be provided to **RTD** if so requested.

Renewal Policies

The **Contractor** shall promptly deliver to RTD a certificate of insurance with respect to each renewal policy, as necessary to demonstrate the maintenance of the required insurance coverage for the terms specified herein. Such certificate shall be delivered to **RTD** not less than 30 calendar days prior to the expiration date of any policy.

Cancellation and Modification of Insurance Coverages

The **Contractor** shall be responsible to immediately notify RTD in writing of any changes or cancelations of its insurance, or may be found in breach of the Contract and the Contract could be terminated. This notice requirement does not waive the insurance requirements contained herein.

No Recourse

There shall be no recourse against **RTD** for the payment of premiums or other amounts with respect to the insurance required from the **Contractor**.

Failure to Provide or Maintain Insurance Coverages

The **Contractor's and Subcontractor's** failure to provide or maintain any of the insurance coverage required herein shall constitute a breach of the Contract. In addition to the remedies that **RTD** may have under the insurance specified herein, **RTD** may take whatever action is necessary to maintain the current policies in effect (including the payment of any premiums that may be due and owing by the **Contractor and Subcontractors**) or procure substitute insurance. The **Contractor** is responsible for any costs incurred by **RTD** in maintaining the current insurance coverage in effect, or providing substitute insurance, and such costs may be deducted from any sums due and owing the **Contractor and Subcontractors**.

BOND REQUIREMENTS

EXHIBIT 3—SPECIAL PROVISIONS/ALTERATIONS

SPECIAL TERMS

The following provisions from Section III, General Terms and Conditions, have been specifically negotiated for this Contract and these provisions, as added or altered, shall supersede to the extent that they conflict with corresponding provisions contained in Section III, General Terms and Conditions and any other conflicting specification required by the Contract Documents.

The following articles are added or altered accordingly:

ARTICLE 49. DATA MANAGEMENT

"RTD Data" shall mean all information processed or stored on computers or other electronic media by RTD or on RTD's behalf, or provided to Contractor for such processing or storage, as well as information derived from such information. RTD Data includes, without limitation: (i) information on paper or other non-electronic media provided to Contractor for computer processing or storage, or information formerly on electronic media; (ii) information provided to Contractor by RTD customers, users, employees, or other third parties; and (iii) sensitive customer information, including without limitation personally identifiable information and financial information. Contractor shall ensure that all third parties hosting an interface for RTD Mobile Ticketing comply with RTD's Mobile Ticketing Privacy Policy and the provisions set forth in Article 49, Data Management.

A. **Access and Use of RTD Data**. Unless it receives RTD's prior written consent, Contractor shall not: (i) access, process, or otherwise use RTD Data other than as necessary to facilitate the Work; (ii) give any of its employees access to RTD Data except to the extent that such individual needs access to facilitate performance under this Contract; (iii) give any third party access to RTD Data, including without limitation Contractor's other customers, except Contractor's subcontractors subject to subsection (d) below; and (iv) sell RTD Data to any third parties. Notwithstanding the foregoing, Contractor may disclose RTD Data as required by applicable law or by proper legal or governmental authority. Contractor shall give RTD prompt notice of any such legal or governmental demand and reasonably cooperate with RTD in any effort to seek a protective order or otherwise to contest such required disclosure, at RTD's expense.

B. **Ownership of RTD Data**. RTD possesses and retains all rights, title, and interest in and to RTD Data, and Contractor's use and possession thereof is solely on RTD's behalf.

C. **Retention and Deletion of Data.** Contractor shall not erase RTD Data, or any copy thereof, without RTD's prior written consent and shall follow any written instructions from RTD regarding retention and erasure of RTD Data. Unless

prohibited by applicable law, Contractor shall purge all systems under its control of all RTD Data as such time as RTD may request. Promptly after erasure of RTD Data or any copy thereof, Contractor shall certify such erasure to RTD in writing. In purging or erasing RTD Data as required by this Contract, Contractor shall leave no data recoverable on its computers or other media, to the maximum extent commercially feasible.

D. **Subcontractors.** Contractor shall not permit any subcontractor to access RTD Data unless such subcontractor is subject to a written contract with Contractor agreeing to protect the data, with terms and conditions reasonably consistent with those of this Article 52. Contractor shall exercise reasonable efforts to ensure that each subcontractor complies with all of the terms of this Contract related to RTD Data.

E. **Applicable Law.** Contractor shall comply with all applicable laws and regulations governing the handling of RTD Data and shall not engage in any activity related to RTD Data that would place RTD in violation of any applicable law, regulation, government request, or judicial process.

F. Data Security and Breach. Contractor shall exercise commercially reasonable efforts to prevent unauthorized exposure or disclosure of RTD Data. In the event of a data breach or suspected data breach, Contractor shall (i) notify RTD within 24 hours of discovery of the breach or suspected breach; and (ii) cooperate with RTD and law enforcement agencies, where applicable, to investigate and resolve the data breach, including without limitation notifying injured third parties. Contractor shall give RTD prompt access to such records related to a data breach or suspected data breach as RTD may reasonably request, provided that Contractor shall not be required to provide RTD with records belonging to, or compromising the security of, Contractor's other customers. In the event of a data breach or unauthorized disclosure caused by the act or omission of the Contractor or any of its agents, employees, or subcontractors, the Contractor shall pay for or reimburse RTD for payment of: (i) notification to all affected individuals; (ii) repayment of lost funds; (iii) repair of damaged credit; (iv) credit monitoring for all affected individuals; and (v) any other penalties and fines related to the breach or unauthorized disclosure.

ARTICLE 21. HOLD HARMLESS

A. The Contractor shall indemnify, defend, and hold harmless RTD, its employees, and agents against any and all claims, damages, liability and court awards including costs, expenses and reasonable attorneys' fees, to the extent such claims are caused by any act or omission of, or breach of Contract by the Contractor, its employees, agents, subcontractors or assignees pursuant to the terms of this Contract, but not to the extent such claims are caused by any act or omission of, or breach of Contract by RTD, its employees, agents, other contractors or assignees, or other parties not under the control of or responsible to the Contractor.

B. The Contractor shall indemnify, defend, and hold harmless RTD, its employees and agents against any and all claims, damages, liability and court awards including costs, expenses and reasonable attorneys' fees, to the extent such claims are caused by any act or omission of a third party interface host, its employees, agents, subcontractors or assignees pursuant to the RTD Mobile Ticketing System and any third party interface, but not to the extent such claims are caused by any act or omission of, or breach of contract by RTD, its employees, agents, other contractors or assignees, or other parties not under the control of or responsible to the Contractor.

C. The Contractor shall indemnify, defend, and hold harmless RTD, its employees, and agents against any and all claims, including willful violations, damages, liability and court awards including costs, expenses and reasonable attorneys' fees, to the extent such claims against RTD arise out of or are in any way connected with a claim that the Product(s) or any third party integration partner's product infringes on or misappropriates a third party's Intellectual Property Rights.

D. In respect to the indemnities given at Subsections A, B and C of this Article, RTD shall give the Contractor prompt notice and control of any claim. If the Contractor fails to promptly indemnify, defend or hold RTD harmless, then the Contractor shall reimburse RTD's legal expenses. The rights granted in this Article shall survive any termination or expiration of this Contract or of Contractor's engagement with RTD.

E. The Contractor shall give RTD immediate notice of any suit or action filed or prompt notice of any claim made against the Contractor or any third party integration partner arising out of the performance of this Contract. The Contractor shall immediately furnish to RTD copies of all pertinent papers received by the Contractor. If the amount of the liability claimed exceeds the amount of insurance coverage, the Contractor may authorize representatives of RTD to collaborate with counsel for the insurance carrier, if any, in settling or defending such claim.

ARTICLE 22. TERMINATION

A. For Convenience. RTD may, by giving at least 14 days' written notice to the Contractor, terminate this Contract, or suspend performance hereunder, in whole or in part and at any time for RTD's convenience. The Contractor shall be compensated solely for Work satisfactorily performed prior to the effective date and time of termination or suspension. The Contractor shall have no right to recover lost profits on the balance of the Work, or any other measure of damages.

B. For Default. RTD may declare default in the Contractor's performance of any term of this Contract by giving seven days' written notice to the Contractor specifying with particularity the basis for such default. The Contractor shall deliver a response in writing to RTD within five days of Contractor's receipt of RTD's

default notice setting forth a reasonable proposal to cure or to prevent repetition of the default. If the Contractor fails to timely respond to the notice of default, fails to cure the default, or if the default occurs again on any Work performed (or which should have been performed) during the remainder of the Contract term (including options), RTD shall have the right to terminate this Contract for default by written notice. RTD is not required to provide subsequent written notices of default for recurring instances of default already brought to the attention of the Contractor in a written notice. In the event of such termination for default, the Contractor shall be compensated solely for Work satisfactorily performed prior to the effective date and time of termination. RTD may proceed with the Work by contract or otherwise and the additional cost to RTD of completing the Work shall be deducted from any sum due the Contractor. If after termination for default it is determined that the Contractor was not in default, the rights and obligations of the parties shall be the same as if the termination had been issued for RTD's convenience. The foregoing shall be in addition to any other legal or equitable remedies available to RTD.

C. Suspension of Work. RTD may suspend the performance of the Contractor by giving the Contractor seven days' written notice. Upon Contractor's receipt of notice of suspension of Work, the Contractor shall perform no further Work and RTD will not be required to reimburse the Contractor for any costs incurred subsequent to Contractor's receipt of notice of suspension and prior to notice to resume Work, if any. Suspension of Work may be in whole or in part, as specified by RTD. The Contractor shall continue to submit invoices for Work performed. If after six months of suspension, RTD has not given the Contractor notice to resume Work, the Contractor is entitled to request in writing that RTD either (1) amend the Statement of Contract Cost or (2) terminate the Contract pursuant to "Termination for Convenience." If suspension for more than six months is not due in any part to the fault of the Contractor, RTD shall be required to amend or terminate the Contract. No amendment to the Statement of Contract Cost shall be made under this Article if suspension, delay, or interruption is due to the fault or negligence of the Contractor, or for which an equitable adjustment is provided for or excluded under any other term or condition of this Contract.

D. Termination of Third Party Interface. Upon written notice, RTD may direct the Contractor to terminate any third party interface according to the wind-down schedule included in the contract statement of work for that third party.

ARTICLE 50. INTELLECTUAL PROPERTY REPRESENTATIONS AND WARRANTIES

"Intellectual Property Rights" means copyright, rights related to or affording protection similar to copyright, database rights, patents and rights in inventions, semi-conductor topography rights, trade and service marks, logos, rights in internet domain names and website addresses and other rights in trade or business names, design rights (whether registerable or otherwise) and registered designs, know-how, trade secrets and moral rights and other similar proprietary rights or obligations, together with applications for registration and the right to apply for registration, and all other proprietary rights whether registerable or not having equivalent or similar

effect in any country or jurisdiction and the right to sue for passing off in each case which may subsist or come into existence from time to time.

"Product" means the goods or supplies, and any related services provided to RTD by the Contractor under this Contract, including but not limited to: software, hardware, technology applications or systems, and associated documentation.

Contractor represents and warrants that it is the owner of the Product(s) and of each and every component, or the Contractor is the recipient of a valid license, and that it has and will maintain the full power and authority to grant the Intellectual Property Rights provided to RTD under this Contract without the further consent of any third party.

Excluding the following lawsuit, Bytemark, Inc. v. Masabi Ltd. (2:16-cv-00543-JRG-RSP), Contractor represents and warrants that it is not aware of any pending or threatened litigation that would have a material impact on the Contractor's ability to perform its obligations or grant the Intellectual Property Rights pursuant to this Contract.

ARTICLE 51. INTELLECTUAL PROPERTY OWNERSHIP RIGHTS.

All Intellectual Property Rights created by the Contractor in the course of any Work performed under the Contract or in carrying out the obligations under this Contract shall belong to the Contractor. All Intellectual Property Rights created by RTD in the course of the performance of its obligations or exercise of its rights under this Contract shall belong to RTD.

ARTICLE 52. RTD REMEDIES FOR INTELLECTUAL PROPERTY INFRINGEMENT.

Notwithstanding Contractor's obligations pursuant to Article 21 (Hold Harmless), in the event of a bona fide claim of infringement or misappropriation of a third-party's Intellectual Property Rights against RTD or a temporary or permanent injunction is granted by a court which prohibits RTD from using the Product(s) in whole or part, the Contractor, at its own expense and at RTD's sole option, shall: (1) procure for RTD the licensing rights necessary to continue use of the Product(s); (2) replace the Product(s) with a non-infringing product(s) acceptable to RTD; or (3) refund RTD for all fees paid to the Contractor under this Contract for the last twelve months, in which case RTD will return to the Contractor all Product(s) and cease use of the Product(s).

The rights and remedies of RTD provided in this Article are in addition to and do not limit any rights and remedies available to RTD. The rights granted in this Article shall survive any termination or expiration of this Contract or of Contractor's engagement with RTD.

DELETED ARTICLES

The following provisions have been deleted in their entirety from Section III, General Terms and Conditions:

I. **Article 19 Duty to Protect Critical Infrastructure and Security Sensitive Information** is hereby deleted in its entirety.

II. **Article 30, Prohibition Against Employment of Illegal Aliens.** This Contract is not a "Public Contract for Services" under C.R.S. § 8-17.5-101 and this Article is hereby deleted in its entirety.