



Transit Software Solution RFP No.54-12008772-CM

State of North Carolina Department of Transportation
June 19, 2023

spare

810-815 West Hastings St
Vancouver, BC V6C 1B4
Canada

STATE OF NORTH CAROLINA Department of Transportation	REQUEST FOR PROPOSAL NO. 54-12008772-CM	
	Offers will be publicly opened: June 19, 2023	
	Issue Date: April 4, 2023	
Refer <u>ALL</u> inquiries regarding this RFP to: Christie Murphy clmurphy1@ncdot.gov 919-707-4848	Commodity Number: 81162000	
	Description: Transit Software Solution	
	Purchasing Agency: Department of Transportation	
	Requisition No.: 12008772	

OFFER

The Purchasing Agency solicits offers for Services and/or goods described in this solicitation. All offers and responses received shall be treated as Offers to contract as defined in 9 NCAC 06A.0102(12).

EXECUTION

In compliance with this Request for Proposal, and subject to all the conditions herein, the undersigned offers and agrees to furnish any or all Services or goods upon which prices are offered, at the price(s) offered herein, within the time specified herein.

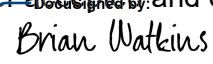
Failure to execute/sign offer prior to submittal shall render offer invalid. Late offers are not acceptable.

OFFEROR: Spare Labs Inc		
STREET ADDRESS: 815 W Hastings St, STE 810	P.O. BOX:	ZIP:
CITY, STATE & ZIP: Vancouver, British Columbia, V6C1B4	TELEPHONE NUMBER: +1 (855) 551-0585	TOLL FREE TEL. NO
PRINT NAME & TITLE OF PERSON SIGNING: Kristoffer Vik Hansen , CEO	FAX NUMBER:	
AUTHORIZED SIGNATURE: 	DATE: 06 / 14 / 2023	E-MAIL: kristoffer@sparelabs.com

Offer valid for ninety (90) days from date of offer opening unless otherwise stated here: ____ days

ACCEPTANCE OF OFFER

If any or all parts of this offer are accepted, an authorized representative of Department of Transportation shall affix its signature hereto and any subsequent Request for Best and Final Offer, if issued. Acceptance shall create a contract having an order of precedence as follows: Best and Final Offers, if any, Special terms and conditions specific to this RFP, Specifications of the RFP, the Department of Information Technology Terms and Conditions (Attachment B), the NCDOT Agency Terms and Conditions (Attachment C), and the agreed portion of the awarded Vendor's Offer. A copy of this acceptance will be forwarded to the awarded Vendor(s).

FOR PURCHASING AGENCY USE ONLY		02/13/2025
Offer accepted and contract awarded this date _____, as indicated on attached certification,		
by 	(Authorized representative of Department of Transportation).	

Brian Watkins

Brian Watkins

Table of Contents

Cover Letter	2
Attachment D: Description of Offeror	2
Vendor Response to Specifications and Requirements	4
Statewide Information Security Manual	4
Project Understanding	4
Spare Platform	6
1. Project Management	7
a. Project Manager and Key Staff	7
b. Project Meetings	11
c. Project Management Deliverables	12
2. Common Design Specifications	20
a. Application Programming Interface (APIs)	20
3. Demand Response Software	22
a. Demand Response General Specifications	22
b. Client Management	26
c. Reservations	29
d. Scheduling	32
e. Dispatching	36
f. Driver Display Functionality	39
g. Billing and Invoicing	40
4. Customer Applications	41
a. Mobile Applications	41
b. Customer Website	43
c. Phone Notification	44
5. Reporting	46
a. General Reporting	46
b. Performance Monitoring and Analytics	49
6. Implementation	50
a. System Design Reviews	50
b. Testing	51
c. Training and Manuals	54
7. Ongoing System Operations and Maintenance	58
a. System Maintenance Agreement (SMA)	58
b. Service Level Agreement (SLA) and Key Performance Indicators (KPIs)	60
c. Issue Resolution and Remedies	61
8. Priced Options	62
a. Hardware (Option)	62
b. Payment Hardware (Option)	63
c. Onboard Hardware, Data Communications, and Installation (Option)	64
d. On-Demand Trips (Option)	65

e. Fixed Route Scheduling (Option)	68
f. CCTV (Option)	68
9. Project Management Specifications	69
a. Project Deliverables Specifications	69
Security Vendor Readiness Assessment Report (VRAR)	70
Architecture Diagrams	70
Cost of Vendor's Offer (Attachment E)	70
Schedule of Offered Solution	150
Signed Vendor Certification Form (Attachment F)	155
Location of Workers Utilized by Vendor Form (Attachment G)	155
References (Attachment H)	155
Financial Statements (Attachment I)	166
Errata and Exceptions	166
Vendor's License, Maintenance, and Service Level Agreements	166
Supporting Material	166
Other Supporting Materials	167
Description of Vendor Submitting Offer Form	199
All Pages Solicitation Document	201
Appendix A - Signed Addendum #1	
Appendix B - Project Deliverables Specifications	
Appendix C - Standard Master Agreement	
Appendix D - Other Supporting Materials	
Appendix E - Remaining Attachments	

Cover Letter

June 19, 2023

State of North Carolina
Department of Transportation
1 S Wilmington Street
Raleigh, NC 27601, United States

Attention: Christie Murphy

RFP No.54-12008772-CM | Transit Software Solution

As transit evolves at an increasing pace, transit agencies are seeking a new approach to more innovative, customer-focused, future-proof transit services. To help the 98 Demand Response Operators (DROs) within the State of North Carolina effectively purchase and obtain demand response scheduling software that fits their needs, the State of North Carolina Department of Transportation (NCDOT) is looking to evaluate qualified vendors through this proposal response.

Spare Labs Inc.'s (Spare) user-friendly, demand response software solution can seamlessly be scaled and customized to meet the DROs' current and future needs. Our innovative technology for route and fleet optimization gives DROs the freedom to respond to fluctuating demand in their demand response network. DROs have the ability to set their own service hours, zones and route parameters to give them the flexibility to expand and include new communities, serviced by their own fleet or complemented by non-dedicated providers.

Spare's cloud based architecture and open API give DROs the flexibility to interact and integrate with third party apps for booking, payment or trip brokering to third party parties. Our software automates booking, scheduling, routing, communications and reporting using superior machine learning algorithms—eliminating the time consuming, manual tasks around scheduling, bookings and communications.

Throughout our proposal you will find information about our technology and the value-driven outcomes it provides. Here are just a few of the advantages we'd like to highlight.

A powerful algorithm to boost passenger per vehicle hour (PPVH). The Spare Engine algorithm powers efficient, self-serve dispatching by optimizing across multiple duties in a DROs' service area and combines scheduled and same-day trips to enable the most efficient ride at all times.

Customer focused software for an easy rider experience. The Spare Rider app and Spare Web Booker gives the DROs' customers all the information they need at their fingertips to book and manage their rides which reduces the burden on the DROs call centers.

Automated scheduling to save time. For in-progress vehicles, Spare Engine's Global Optimization for Live Duties (GOLD) feature automatically assesses the entire DROs' service zone to see if the assignment of rides to runs can be reorganized in a more optimal configuration, saving time, boosting PPVH, and eliminating human error and manual processes by automating the dispatch process.

Easy to use reporting. Spare provides fully exportable reports in Excel format that provides microtransit and ADA paratransit passenger trip data, including important billing reports and vital NTD reports — saving time and providing accurate, up-to-to-date data.

We look forward to speaking with you further about this exciting opportunity and answering any questions you may have about Spare and our software solution.

Kind regards,



Josh Bethel, Growth Manager
josh.bethel@sparelabs.com | 902-233-3209



Kristoffer Vik Hansen, CEO
kristoffer@sparelabs.com | 778-995-6401



Brennon Fuqua

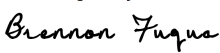
Marc Clifford

Chris Peoples

Director

Deputy CIO

Chief Operating Officer

DocuSigned by:

F21F90D3B0CA4AF...

DocuSigned by:

D6EE99572D6D43B...

DocuSigned by:

383C434421994A4...

02/13/2025

02/13/2025

02/13/2025

Spare Labs

815 W Hastings St Suite 810, Vancouver, BC V6C 1B4

Attachment D: Description of Offeror

Offeror's full name	Spare Labs Inc.
Offeror's address	Suite 810, 815 W Hastings St Vancouver, BC V6C 1B4, Canada
Offeror's telephone number	+1 (855) 551-0585
Ownership	Other (specify) - Private corporation
Date established	November 3, 2015
If incorporated, State of incorporation.	November 3, 2015
North Carolina Secretary of State Registration Number, if currently registered	We are not currently registered in North Carolina, but would be willing to do so upon contract award like we have other states.
Number of full-time employees on January 1st for the last three years or for the duration that the Vendor has been in business, whichever is less.	67 employees
Offeror's Contact for Clarification of offer: Contact's name, Title Email address and Telephone Number	Josh Bethel, Growth Manager josh.bethel@sparelabs.com 902-233-3209
Offeror's Contact for Negotiation of offer: Contact's name, Title Email address and Telephone Number	Josh Bethel, Growth Manager josh.bethel@sparelabs.com 902-233-3209
If Contract is Awarded, Offeror's Contact for Contractual Issues: Contact's name, Title Email address and Telephone Number	Josh Bethel, Growth Manager josh.bethel@sparelabs.com 902-233-3209
If Contract is Awarded, Offeror's Contact for Technical Issues: Contact's name, Title Email address and Telephone Number	Tanveer Pratap, Solutions Engineer tanveer@sparelabs.com 604-347-8434

HISTORICALLY UNDERUTILIZED BUSINESSES

Historically Underutilized Businesses (HUBs) consist of minority, women and disabled business firms that are at least fifty-one percent owned and operated by an individual(s) of the categories. Also included as HUBs are disabled business enterprises and non-profit work centers for the blind and severely disabled.”

Pursuant to N.C.G.S. §§ 143B-1361(a), 143-48 and 143-128.4, the State invites and encourages participation in this procurement process by businesses owned by minorities, women, disabled, disabled business enterprises and non-profit work centers for the blind and severely disabled. This includes utilizing subcontractors to perform the required functions in this RFP. Contact the North Carolina Office of historically Underutilized Businesses at 919-807-2330 with questions concerning NC HUB certification. <http://ncadmin.nc.gov/businesses/hub>

Respond to the questions below.

1. Is Vendor a Historically Underutilized Business? Yes **No**

2. Is Vendor Certified with North Carolina as a Historically Underutilized Business? Yes **No**

If so, state HUB classification: _____

Vendor Response to Specifications and Requirements

Statewide Information Security Manual

We affirm and explicitly acknowledge that Spare's proposed solution at time of award and for the duration of the contract will comply with all applicable State policies, guidelines, standards, practices, procedures, and safeguards as defined in the North Carolina Department of Information Technology Statewide Information Security Manual (SISM).

Project Understanding

Spare understands that the North Carolina Department of Transportation (NCDOT) is seeking to procure a transit demand response scheduling software solution to automate, streamline, and improve the on-demand services for Non-Emergency Medical Transportation (NEMT), elderly and disabled transportation assistance, limited services for the rural general public, and employment transportation assistance provided by its Demand Response Operators (DROs) within the State of North Carolina.

NCDOT is seeking to consolidate terms and conditions for its DROs to alleviate discrepancies in performance by transit scheduling software vendors. NCDOT is looking for a solution that meets the following key objectives:

1. Better cross-agency coordination
2. Simplified scheduling and new payment options
3. Improved integration across services and providers
4. New on-demand scheduling capabilities
5. New mobility services
6. Turnkey transportation services

Making the change from what is familiar can be hard, but with Spare it doesn't have to be. Spare works alongside agencies like the in-state DROs to transition them from legacy providers, including: Pinellas Suncoast Transit Authority (PSTA) in Florida; Mountain Line Transit in Flagstaff, Arizona; Atlanta Regional Commission in Georgia; Twin Transit in Lewis County, Washington; and more. Beyond transition and launch, Spare will work with these DROs to support and scale to their needs. For example, based on partner feedback we developed our eligibility management module, Spare Engage, to streamline, automate and digitize the eligibility process from application to determination to renewal.

In addition to the ways in which the Spare Platform can specifically address the requirements listed in the list of technical specifications, Spare has outlined our high-level approach to the general goals and requirements.

As for the project understanding, Spare can comply, commit and complete the following as outlined in the RFP:

- Supply a solution to schedule, route, and dispatch on-demand rides for different rider types such as seniors and disabled persons with Spare Launch
- Provide a client database that will house rider profiles and improve eligibility processing with Spare Engage
- Provide a solution that will automatically generate the most efficient and realistic schedules and routes with Spare Engine
- Supply and deploy the on-demand solution including new, customized, and off-the shelf modules, mobile applications to meet the RFP requirements with Spare Rider and Spare Driver
- Transfer and install the existing and necessary data from your existing system to the new solution
- Provide ongoing and comprehensive training to DRO staff
- Provide ongoing system support and maintenance

After the Spare Platform overview section, we have duplicated the tables from [Section 3.4 Business and Technical Specifications](#) in the RFP and have provided our answers.

Spare Platform



Admin Panel

Spare Launch, Analyze
and Engage



Rider App



Driver App



Rider Web

For this implementation, we propose the **Spare Platform**, our powerful software platform for demand response operations. Spare Platform is a cloud-based software-as-a-service (SaaS) solution for delivering paratransit, microtransit, and any type of shared-ride demand response services. It is a single, comprehensive modern software solution that provides an easy-to-use administrative/backend panel and frontend applications (Spare Rider, Spare Rider Web, and Spare Driver).

The Spare Platform consists of several modules to deliver reliable and cost-effective transit service: **Spare Launch**, **Spare Analyze**, and **Spare Engage**. These components interact with the **Spare Engine**, our proprietary routing algorithm that optimizes operations. Together, these components provide the

most advanced and exceptional experience for the DROs' riders, administrators, dispatchers/schedulers, customer service representatives, and operators, with the end product being a highly optimized, reliable and accessible solution.

At a high-level, these modules include:

- **Spare Launch.** A backend mapping system that enables fully automated batch scheduling, dispatching, and reservations of the demand response service
- **Spare Analyze.** Data collection and reporting dashboard that provides access to reporting for the National Transit Database (NTD) and real-time service performance data, such as heat maps and service/fleet/trip search analytics
- **Spare Engage.** Centralized, digital customer management, and eligibility tool to manage rider profiles (e.g. into segments/groups) and to automate the paratransit eligibility process
- **Spare Rider (Mobile App and Web Booker).** A customer-facing smartphone application available on iOS and Android apps, Spare Rider is used by passengers to plan and execute their trips. Passengers can create client accounts, manage their user profile, and book and manage trips on Spare-powered services. DROs can opt to white-label the Rider app, giving passengers a cohesive rider experience across all the agency-branded services.
- **Spare Driver app.** The app will be where drivers/operators will sign in and receive real-time, turn-by-turn trip instructions and information on MDT/tablet device –communicated directly from the Spare Platform.
- **Spare Engine.** The Spare routing and pooling engine leverages the latest developments in big data, machine learning, and artificial intelligence to intelligently predict how to best route and dispatch trips in real-time. The Spare Engine matches and routes vehicles in the most optimal and efficient manner, taking into account travel patterns of a region, open traffic data, current vehicle resource allocation, current demand, and past trips. The longer the system operates, the smarter the routing engine becomes—reducing wait times and optimizing the system for higher passengers throughout.
- **Spare Open API.** Spare's infrastructure is built upon an open architecture. The Spare Open API (Application Programming Interface), allows other systems to easily interface with the Spare Platform, a drastic difference compared to other solutions on the market. An Open API platform can bring a wealth of benefits, such as integration opportunities with transit aggregators like the GoPass app, Transit app, Google Maps, Citymapper, and more. The Spare Open API is available at sparelabs.com/docs.



The Spare Platform and the rider and driver-facing apps work together to create a single solution for the DROs' transit operations.

1. Project Management

a. Project Manager and Key Staff

ID	Specifications	Feature	Spare's Response
1.a-1	The Vendor works closely with the State, the DROs, and the NCDOT Lead Representative for the initial implementations. This provides a project implementation framework for all subsequent implementations throughout North Carolina.	Core	With over 200 service implementations, Spare has developed an implementation plan from pre-kickoff through to launch and post-launch support. Each implementation will receive its own implementation plan based on the unique needs of the DROs.
1.a-2	The Vendor assigns responsible and experienced individuals to serve as the Project Manager and Key Project Staff for each implementation.	Core	Each implementation will have its own Project Team comprised of individuals who have completed other implementations. This Key Project Staff generally consists of a Growth Manager, Project Manager, Product Manager, Operators Director, and a member of the executive team with team members from Support, Product, Data Science, and Engineering who are brought in based on the complexity or different needs of the project.
1.a-3	At a minimum, the Vendor provides a qualified Project Manager who shall oversee and coordinate all the DROs implementations throughout the State. The Project Manager will be the single point of contact for the NCDOT Lead Representative.	Core	Spare will appoint a Project Manager who will be the single point of contact for all communication between the DRO and the Spare Project Team. This includes the kickoff meeting and weekly progress calls between the project management team and the DRO's team. As the single point of contact, Spare's Project Manager will provide multiple opportunities to address project concerns that might arise and confirm that they are properly discussed and resolved. She/he will be responsible for delivering a coordinated approach for the demand response software services, including coordinating with internal teams, the DRO's local taxi companies (if applicable), and ride-hailing TNCs (e.g. Lyft, as an option) (if applicable), that would service the demand response service.
1.a-4	The Vendor's Project Manager possesses experience managing demand response	Core	Spare's Project Manager comes from the Partner Success team which will work with the DRO for the full contract from contract award up until contract end. The Project

	scheduling software implementation projects.		Manager will handle duties from project kick-off until the service is launched. Once the service has been launched and has been running for a short time, the Project Manager will hand off the DRO to the Post-Launch Project Manager. The Post-Launch Project Manager will continue the regularly scheduled meetings post-launch, communicating regularly with the DRO to answer any questions, help to continue to refine the service, be a support resource, and anything the DRO needs until contract end.
1.a-5	The Vendor recommends one or more Deputy Project Manager(s) and other Key Staff to facilitate and manage the day-to-day implementation and onboarding of individual DROs within the State as needed.	Core	The day-to-day implementation and onboarding of the individual DROs will be completed by a Project Manager and Key Staff that are specifically assigned to a particular DRO as each project is different. In the unlikely event that a Project Team member is unavailable due to unpredictable circumstances, Spare will enlist backup personnel to step in wherever needed. Spare's Project Success Team is fully staffed with additional resources and contingency plans in case of unexpected team member absences on projects. Each backup team member will be able to ensure continuity in experience, qualifications, and expectations should additional resources be required on the project at any point during the implementation. Backup resources to be used for this project would be managed and overseen by Quinn Kliman, our Operations Director. In the case of a Project Manager needing to be replaced, Spare's Operations Director will first review the implementation requirements and plan. The Operations Director will then review the current implementations of the other project managers on Spare's Project Success Team, as well as the size, complexity, and nuances of the project to find a new Project Manager that has the capacity and experience to ensure success. If the current Project Manager is still available, a formal handover process with robust documentation and transitionary meetings will be engaged to make the transition as seamless as possible. In extenuating circumstances where the current Project Manager leaves abruptly - this has never happened at Spare, but we are prepared for it nonetheless - the replacement Project Manager will review any and all existing project documentation. This includes the project plan, meeting minutes, emails, recordings, internal conversations, and design documents etc. to get up to speed prior to taking over the next project meetings.

			The Partner Success team holds weekly meetings where they discuss Spare's current implementations and each Project Manager highlights key elements of the project. This ensures that the team as a whole is generally aware of project status, needs, and challenges. Each Project Manager also holds weekly 1-on-1s with the Operations Director. Those team members named from the Product & Solution Engineering team will also follow the same process. For any team member substitutions, we would only proceed with this with DRO's written approval.
1.a-6	All identified Key Project Staff will be subject to review by the DROs. Key Project Staff includes: 1. Project Manager 2. Deputy Project Manager(s) 3. Lead developer/engineer(s) 4. Implementation lead(s) 5. QA/QC lead(s) 6. Training lead(s) 7. Support lead(s)	Core	Spare's Project Team is composed of experienced personnel who have played key roles in transitioning, launching, and optimizing Spare's demand response services across the US. The team is composed of a multidisciplinary set of individuals, all critical bringing unique expertise, experience, and skills to the team that will lead to a successful transition to Spare. A high-level summary of departmental resources is below to show the make-up of Spare's project team. Growth & Partnerships Spare's primary RFP contact, Growth Manager Josh Bethel (only assigned staff member) leads the transition from contract negotiations through to the first meeting with the DRO's dedicated Project Manager. Josh will transition the DRO from purchasing to project kickoff. Launch Team Spare will assign a dedicated Project Manager to serve as the DRO's Project Manager. Spare's Project Manager will be the single point of contact and will oversee and direct Spare's resources to help the DRO launch and continuously optimize the demand response program. They will be partnered with the DRO from project kickoff through to service launch. The Project Manager will be the main point of contact, leading the meetings, overseeing the project timelines, training, and testing. Spare's Transit Operations Specialist will be brought in to help with the implementation if additional support is required. A Post-Launch Project Manager will take over from the Project Manager after the services have launched and the DRO team is comfortable and content with the state of the service. The Post-Launch Manager will work with the DRO to continuously optimize the service and be a resource for service ideation, planning, and more. While our Partner

		Success team will lead the transition and overall implementation, this will be a cross-functional effort between all of Spare's key functions, including: growth / partnerships, product, engineering, and partner success. Spare's Support Team, led by Stuart Cantwell, the DRO's Technical Support Manager, will enable the DRO to always receive an accurate and timely resolution on customer questions and concerns. As a key support member to the Project Manager, Stuart and our support resources/tooling will help strengthen the DRO's onboarding experience, including training and provide full support coverage throughout the implementation to ensure response times are quick and 24/7 outage support is provided. With Spare, you will receive a true partnership that's optimized for success. Product & Engineering Spare's Product and Engineering Teams are responsible for ideating, building and refining Spare Platform's modules and their features and functions. Spare's lead Product Manager will serve as the point of contact for Partner Success and Growth should there be custom work to do for the DRO. The Product Manager will be brought in to scope the work and determine a timeline. Straddling the Growth and Product teams is Spare's Solutions Engineer. The Solutions Engineer can support product and engineering with the needs and wants of the DRO. Spare's various engineering teams are also available to provide guidance and support as needed. Executive and Advisory Team Spare's executive supervisory team will be providing oversight for the implementations, providing direction to the project team as required. These team members are not directly assigned tasks, but are available as a technical resource for the project team.

b. Project Meetings

ID	Specifications	Feature	Spare's Response
1.b-1	The Vendor facilitates progress review meetings and shares an agenda at least five (5) business days prior with the	Core	Spare's dedicated Project Manager assigned to the specific DRO for implementation will be in charge of all progress review meetings and will share the agenda with the DRO five days prior. Regular project meetings are part of Spare's implementation plan.

	Agency Project Manager(s) for all implementations.		
1.b-2	The topics to be discussed and reviewed during progress meetings include, but are not limited to: 1. Minutes of the prior progress meeting and progress since the last meeting and action item log 2. Project schedule including sequencing of critical work 3. Project deliverables, with a focus on deliverables due before the next progress meeting 4. Master Issues list and Issues arising since the last meeting 5. Engineering, manufacturing, and quality control summary (if necessary) 6. Any needed corrective measures to maintain the project schedule 7. Any other issues related to the project 8. Other topics as required by the DROs. The discussion topics may vary depending on project needs and priorities.	Core	All recordkeeping and documentation related to a project will be conducted by Spare's Project Manager. All project documentation, including meeting notes and related project information will be completed by our Project Manager at the kickoff and weekly progress calls, and disseminated to the DRO, as requested. Our team will share an Asana project plan throughout the planning and implementation phases of this project so that the DRO's dedicated Project Manager can keep track of the project progress. Asana is a robust project management tool to break down work scope into manageable tasks. The timelines and deliverables of these tasks will be communicated well in advance to the DRO and tracked on Asana. The progress meetings between Spare and the DRO will include the listed topics to ensure the progress is understood by all, including the necessary items the DRO must provide to keep the project on track.
1.b-3	The Vendor documents minutes for all monthly progress review meetings and submitting those minutes for review by the DRO within three (3) business days following each meeting.	Core	The minutes from any meeting will be submitted to the DRO for review within three days of each meeting. Documentation around each task and phase of the project can also be expanded for viewing by the DRO's team on Asana.
1.b-4	All Key Project Staff relevant to the agenda topics are present during progress meetings or as required by the DRO.	Core	Beyond the Spare Project Manager, other Key Project Staff will attend the progress meetings if needed. All of Spare is committed to an implementation's success and many of our staff have attended progress meetings when required.

c. Project Management Deliverables

ID	Specifications	Feature	Spare's Response
1.c-1	The Vendor develops and maintains a Master Program Schedule (MPS). The MPS identifies all program activities, deliverables, and key milestones (including those	Core	The Schedule of Offered Solution section provides a general implementation plan/Master Program Schedule (MPS) that serves as a template. Based on our experience implementing demand response programs throughout the US, this phased approach best sets up a DRO implementation for success.

	owned by the DROs) with expected and actual completion dates.		
1.c-2	The Vendor works with the DROs and the NCDOT Lead Representative to determine acceptable delivery/review timeframes for all DRO-owned deliverables / activities within the MPS. All proposed times are subject to review and approval by the DROs.	Core	Spare will have the DROs and NCDOT Lead Representative review and finalize the MPS and all plans in the first phase, kickoff and project planning as this sets the foundation for the project and ensures the MPS and all roles and responsibilities are understood by all. Throughout this phase, time will also be taken to ensure that overall project success criteria are well defined and clear measurement approaches are established for project milestone/performance tracking.
1.c-3	The Vendor provides a Change Management Plan (CMP) for review and approval by the DROs and the NCDOT Lead Representative.	Core	Spare does not have a change management plan that we make available for review and approval by our clients as we are a cloud-based software. We have an extensive internal testing and review processes that we follow so that any changes we make would not affect the DRO's daily operations. Any updates to our software system goes through Spare's thorough Software Release Management Process. As part of this process, our engineers use a comprehensive suite of automated test runs, in accordance with a standard test pyramid approach. This includes a very large number of "unit tests", a moderate number of "integration tests", and a small number of "end to end" tests. If changes involve a "database migration", which alters the structure of the database or the data within it, all tests run with both the new and old versions of the code to ensure the database changes are compatible with both – instilling confidence for the DRO for system changes. Through each change, Spare's engineers conduct peer code reviews and once approved, changes roll out to a staging environment (similar to our true production that the DROs use), before the rollout process gradually increases with automated monitoring. Only once a staging deploy succeeds without issue, will a production deploy – releasing to the DRO. The DROs will receive new releases on a continuous basis–sometimes many times a day, in line with our change management policy. These releases contain slight adjustments made for better performance or for fixing a bug as an example. They don't contain new features. When a new feature is released, it's first made available in the test environment, with sufficient testing and training time for the agency. Such releases occur less often–roughly one to two times per quarter.

1.c-4	The CMP documents critical changes to program stakeholders and change management and risk mitigation procedures. In addition, the CMP details the Vendors change control process and procedures.	Core	After extensive testing in our separate testing environment, all updates are communicated to the DRO staff by the Spare Project Manager in real-time.
1.c-5	Engineering Change Requests (ECRs) control software changes and updates to approved documents and data.	Core	This does not apply to Spare as we are a cloud-based software. When implementing software changes, Spare uses a staging environment that is similar to our true production, that customers use, but customers do not use it. The rollout process is gradual, with automated monitoring. In most cases, the rollout is slowly ramped up over a 15-30 minute period. If error rates rise during the rollout, it is automatically rolled back, and Engineers are alerted. We also have a bot that continuously performs key workflows against the staging environment, "Spare Monitor". If any of them fail, the rollout is automatically rolled back, and Engineers are alerted. Only after the staging deploy succeeds without issue, a production deploy (releasing to customers) is possible.
1.c-6	ECRs include documentation describing the reasons for, effects of, and rollback plans for the change. The Vendor submits ECRs to the DROs for review and approval at least two (2) weeks before releasing the changes to allow for DRO-led testing (as needed).	Core	After extensive testing in our separate testing environment, all updates are communicated to the DRO staff by the Spare Project Manager in real-time.
1.c-7	The Purchasing DROs directly coordinate and approve exceptions for emergency changes or fixes by Vendor provides comprehensive documentation describing the issue and resolution, and the plan to deploy the change or fix.	Core	Spare will always notify and work with the Purchasing department of the DRO to coordinate and approve any emergency changes or fixes.
1.c-8	The Vendor provides their standard Quality Assurance and Quality Control (QA/QC) policies and procedures. The QA/QC program defines methods for designing for, achieving, and maintaining quality. At a minimum the QA/QC program includes:	Core	Spare will continuously perform quality assurance activities throughout the duration of our partnership in a variety of areas including product upgrades, new releases and security testing which are outlined further in the Security section of the Implementation Plan. Problem areas will be uncovered and addressed on a consistent basis through regular communication between the DRO and Spare.

1. Surveillance overall work, including by Sub Contractors, to ensure compliance with all contract requirements 2. Verification of compliance, including audit; discrepancy identification, notification, and control; and corrective action 3. Evaluation and assessment of Sub Contractors QA programs 4. Provision of technical documentation, drawings, specifications, handbooks, manuals, data flow diagrams, and other technical publications for the new application 5. Design control and version management for changes to documents, drawings, data, and specifications 6. System software development (consistent with IEEE Standard 730 or equivalent ISO 9001 standards for software quality assurance) 7. System integration testing 8. Defect management, including explanations, on how defects will be identified, categorized, reported on, tracked, approved/rejected, and closed out 9. System configuration management 10. Qualification and certification for all personnel performing work under this Contract.	One of the critical components of an operation is a Quality Assurance Program. These programs, in almost all applications, will be contractually required of the software provider as a Prime contractor, especially when utilizing a broker type turnkey model where all operations are subcontracted. The software provider will maintain and implement a robust quality assurance program for each contract in which it provides a turnkey service. Each contract will have an individualized Quality Assurance program in line with contractual outlines and objectives. However, a standard Quality Assurance plan is highly likely to have four distinct areas of quality assurance: People, Vehicles, Service, and Data. In some instances there may be additional categories, such as Facilities or similar types of categories. General Quality Assurance Program Details People Quality Assurance around People involves any employee on a particular contract associated with the software provider or its subcontractors. Common categories of People include: • Drivers • Dispatchers • Call Center Agents • Schedulers • Supervisors / Management • Maintenance staff (if applicable) Generally, Quality Assurance measures around People are related to a couple of different categories: pre employment screening and operational performance. Pre employment screening categories can include FTA required Drug and Alcohol screenings, background checks, and other similar categories. Operational performance categories generally include customer service initiatives, training completion, field performance, and other similar categories. Vehicles Quality assurance around Vehicles is typically the second most important item. This category covers all vehicles used on the contract and sometimes also includes vehicles used for non-revenue service. Common categories of Vehicles include: • Mechanical Repairs and Maintenance • Preventative Maintenance (PMIs) • Interior and Exterior Cleanliness • Vehicle decals / branding

			Quality Assurance measures regarding vehicles will ensure all maintenance and cleanliness timelines are followed and that all vehicles utilized in the project are generally in a State of Good Repair. Non-revenue vehicles (ex. supervisor vehicles, management vehicles, etc.) will generally also be expected to be maintained and cleaned, and typically be branded similarly to revenue vehicles. Service Quality Assurance around Service will primarily focus on the quality delivery of service, be it operations or dispatch/call center. Common categories of Service include: • Contingency Plans • Operational Emergencies • Adequate staffing and training Service Quality Assurance goes beyond service delivery to include all aspects of contingency planning for capacity or emergency needs. Service quality is also impacted by the ability to provide service and leads to ensuring proper staffing levels for an adequate system performance. Data Quality Assurance around Data focuses on ensuring accurate and secure data and accurate and on time reporting. Many agencies will request reports from the software platform at certain intervals, including but not limited to Monthly Operations Reports, Quarterly Summary Reports, and Annual NTD Reporting. Common categories of Data include: • Routine Reporting • Data Integrity • Data Reliability Data is a fairly straightforward Quality Assurance area, albeit very important. Most agencies' primary concern after customer experience is quality of data and reporting, so ensuring data accuracy and integrity is a high priority of any quality assurance plan and turnkey operation.
1.c-9	If damage, defect, error, or inaccuracy is found in any provided work, the DROs have the right to reject or require corrective action to bring the work into compliance with the contract requirements. The Vendor bears all costs incurred in correcting rejected work.	Core	Spare will comply with this.

1.c-1 0	The Vendor maintains an electronic Master Issues List (MIL) to track and manage project issues and action items.	Core	Spare will use two processes for tracking unsolved issues, depending on whether the issue is identified during or after the implementation of Spare Platform. This is because during the implementation process issues will be tracked as part of the overall implementation project plan. After launch, issues will be tracked as part of Spare's ongoing customer support and success processes. During Implementation Issues identified during the implementation will be tracked in Asana as part of the project plan. This allows all implementation project items to be tracked in one place along with the general implementation tasks. Our approach to issue tracking during the project implementation creates one source of truth, Asana, which allows all stakeholders to have visibility into all project matters in one place. Post Implementation After the conclusion of the implementation project and the launch of Spare Platform, the DRO team can get support any time from the Spare Support or Spare Success teams. Either Spare Team can open an issue ticket in our Jira issue management system for the DRO, which can then be easily tracked by either Spare team as well as by the DRO team themselves. Also part of the process is Spare's Engineering team that works constantly to deliver innovative solutions to the problems faced by Spare's customers. The Engineering team works closely with the Partner Success team to identify the most pressing customer pain points, leveraging modern project management tools such as Jira and Productboard to track and prioritize a vast array of potential product improvements, to ensure that the most value is delivered. Spare's daily software deployment cycle empowers Spare Engineers to ship software improvements quickly and reliably.
1.c-1 1	The Vendor identifies and updates MIL items at design review meetings, weekly project coordination meetings, monthly progress review meetings, and on an ad-hoc basis.	Core	Spare will identify and update the DRO on MIL items during the various project meetings.
1.c-1 2	The MIL tracks the following attributes for each entry at a minimum: 1. Item number 2. Date opened 3. Requesting party 4. Description 5. Required action	Core	The MIL issue ticket details include: • Title • Description • Attached files • Submission date • Reporter name • Assignee name • Dates - due date, open and closed date

	6. Assigned party 7. Status (open/closed/in progress/deferred/etc.) 8. Date closed. Other attributes may be required by the DROs. The Vendor assigns no action items to the DROs without the knowledge and consent of the DROs.		• Status • Type • Priority level • Action If the DRO requires other attributes, Spare can add them. No action items will be taken without the consent of the DRO.
1.c-1 3	The Vendor develops and submits a System Implementation Plan (SIP) to be approved by the DROs that purchase systems. The SIP includes detailed implementation activities as it relates to the master program schedule. The SIP includes roles and responsibilities of parties (DROs, Vendor, or other parties) in the proposed project team, progress milestones and status, and assigned Vendor staff.	Core	Spare has developed a SIP that will be approved by each DRO upon purchase of Spare's software. We have detailed a general implementation plan in the Schedule of Offered Solution section. We have developed this based on our experience implementing demand response software for agencies across the US and Canada. Spare has identified the following as keys to a successful implementation: Defining & Updating the Project Plan. Having a clear project plan that is kept continuously updated is key to a successful implementation. This includes leveraging an easy-to-use project management tool that allows for commenting, tagging, and file. Spare uses Asana to provide project team members full visibility into the project plan at all times. Communications: Defining Roles & Responsibilities. Clear responsibilities and accountabilities assigned to individuals in the project plan with clear instructions and due dates is paramount to a successful implementation. We use the RACI diagram, which defines who is responsible, accountable, consulted, and informed throughout the project duration. A clear project communications plan and regularly scheduled meetings where team members can bring up questions, concerns, and issues is key. Spare's Project Manager will host weekly meetings with the DRO to ensure the project is on track. Risk Mitigation. We often dive into risk identification and risk mitigation planning as soon as we receive Notice to Proceed. Particularly for large, complex implementations, such as installation or replacement of enterprise paratransit software, our partner success teams take the learnings from past relevant implementations, and kickstart internal discussions immediately to proactively identify and mitigate risks before they occur. We also share these findings throughout the implementation and share these with the DRO during weekly progress calls. Schedule Reviews Both Ways. Scheduling bi-directional feedback reviews between the Spare team and the DRO's review is also key to success. A bi-directional review ensures that both teams look for mistakes, keeping any major errors out of consideration, where

			possible. As a quality control measure, all work, such as updating service parameters, should be reviewed by someone else on the team to ensure quality and minimize errors. Remove Roadblocks Early. Tackle tasks that have the potential to block launch at the very beginning, including (but not limited to): procurement (devices, hardware, vehicles etc.), hiring, data/systems migration. For data migration from a previous system, we suggest early communications with legacy providers on information that needs to be exported and migrated. Plan Transition Early. Comprehensive scoping of current processes, future processes, and the creation of a full transition plan for staff member workflows/processes. Detailed Reporting. Create comprehensive process documentation for regular and irregular scenarios. Disaster Recovery. Create disaster/outage recovery and contingency plan with backup manual processes Early Scoping Meetings. Comprehensive scoping of integration requirements, deliverables, and potential obstacles (communications and project plan learnings also apply to integrations/integrators). User Acceptance Testing (UAT). Completed for any material changes made to the rider experience (e.g. new app, new trip flexibility configuration, new process for scheduling etc.) and an adjoining rider education strategy Robust end-to-end testing. Completed with all team members and workflows in real-world conditions just as they will be at launch (as part of the SAT and QA plan) Communications & Education for Service Promotion. A comprehensive communications and education plan for riders (and the general public). Tailored Training & Documentation for Ongoing Learning. Tailored training plans for the specific roles of your organization and robust reference materials (guides, FAQs, videos, chat support etc.).
1.c-1 4	The Vendor retains responsibility for accurately migrating existing customer records to the new customer database. Vendor provides a recommended Customer Data Migration (CDM) plan based on industry best practices and relevant experience migrating customer records.	Core	Spare has a robust software transition plan and follows rigorous data migration steps to complete the change from a previous software like Routematch, TransLoc and others to Spare. The success of the implementation during the transition needs careful management to keep the project on schedule and with minimal risk. Completing this transition for the DRO's service is a workflow that we have purpose-built into Spare. We closely monitor the transition by planning all aspects of it, including creating a rider data importation plan and a system operations transition plan. Spare has transitioned dozens of small and large transit systems from legacy softwares to Spare. Our largest paratransit software transition will launch this spring in

	Austin, Texas with CapMetro. This service includes 160 vehicles and 330 drivers, completing roughly 2,200 trips a day. During this transition, Spare migrated all rider profiles over from Trapeze to Spare. The process took approximately three weeks to complete. During this process, Spare worked with the CapMetro's project manager to make sure we were able to capture all data, and ensure that only "clean" data was entered into the new system. In 2022, Spare launched its largest paratransit service at the time, but soon to be second largest service, PSTA in Pinellas County, Florida. During this implementation Spare migrated roughly 4,700 rider profiles from Routematch to Spare. Today this service delivers more than 1,200 trips per day. These are just two examples of Spare's ability to transition large paratransit services from their previous software onto Spare. At a more granular level, the following data migration plan should help illustrate Spare's process for completing software transitions and data migration from legacy software. Step 1: Review, Analysis and Discovery Review rider data that lives in the existing scheduling and dispatching software. Understand all the relevant fields in the existing software platform that needs to be imported into Spare. • What columns/data does the DRO want to keep? • Identify stale profiles (e.g. inactive profiles) Step 2: Data Cleanse • Look for duplicate data, profiles, and consolidate • Look to convert data formats, where necessary. E.g. date formats into one that's aligned with Spare Platform. • Further clean data in additional ways in collaboration with the DRO. Step 3: Custom Fields • Creation of custom fields in Spare that can match existing fields such as phone number, emergency contact etc. • Discuss adding additional fields not previously available in previous software that the DRO wishes to include. • Discussion with the DRO on the custom fields Spare has available within our platform. Step 4: Data Mapping and Prepare Import Sheet • Convert data to match Spare import parameters. • Align column header with custom fields to prepare finalized sheet for import into Spare Platform. • Complete final review and data validation.

			Step 5: Import Testing Complete test import with small subset of rider profiles. Step 6: Import Complete full data import into Spare from a csv extract. Step 7: Validate Validation of data imported into Spare.

2. Common Design Specifications

a. Application Programming Interface (APIs)

ID	Specifications	Feature	Spare's Response
2.a-1	The system uses APIs to share data and connect with third-party applications as required by the DROs. The Vendor provides documentation describing all API calls, data formats, and communication and security protocols used to support the system interfaces.	Core	Spare, unlike other software providers on the market, is built on an open architecture and we make our API available to the public. This is intentional because Spare believes that building partnerships with other software vendors is the best way to deliver a holistic and high-quality transit service for our partner agencies and their riders. An Open API brings virtually unlimited capabilities to easily integrate with third party technologies. For example, Spare Platform can easily integrate with a wealth of customized solutions, new payment solutions, vehicle statistics, maintenance solutions, and multimodal applications, such as our partnership with Transit App. At Spare we believe the future of transit is integrated mobility solutions. Because Spare is invested in openness and transparency, the Spare Open API - the foundation of Spare Platform - is available online at docs.sparelabs.com for all of our partners and competitors to see. This offers developers access to up-to-date Spare Platform information such as vehicle availability, departure times, and live tracking. Our API offers access to protected functions for registered developers, such as booking a trip, getting information about recent trips, canceling trips, and more. Spare's Open API is available for sharing with fare payment and/or cross platform solutions, such as GoPass. Our platform is integrated into solutions for trip booking, payments and multi-modal trip planning. In a world where open APIs are the rule, rather than the exception, the rate of innovation among developers will be rapid and robust, ultimately providing DROs and its residents with more value and choice over what one

			company could ever offer on its own. Spare's commitment to a truly open API is a radically different approach than that of any other mobility platforms out there and is, in our view, an essential asset for the future of mobility services, perfectly aligned with the next generation of public transit.
2.a-2	A system integrates with system applications such as Interactive Voice Response (IVR) system, mobile applications, customer websites, and other such applications using APIs.	Core	Spare's IVR system empowers all riders, including those who are seniors, physically impaired or unbanked to use transit services, no matter their distinct needs. In turn, transit agencies are also able to go cashless in the most inclusive way possible. Spare's IVR system allows organizations to accept credit card, prepaid credit card, and debit card information over the phone in a private, secure and PCI-compliant manner through Twilio. Once this information is taken, the amount charged is deducted from rider accounts so that cash does not have to be used. This means that even riders without access to a smartphone can still pay electronically and transit is as inclusive as possible for all riders. Spare is in the process of developing additional IVR capabilities for riders to book and cancel trips and check ETAs via voice. Additionally, Spare has voice notifications for those who call in on a landline, or for those without text or push notifications. Meaning that 60 minutes before a ride, those who are not able to receive push or text messages will receive an automated phone call reminding them of their upcoming trip, and provide more information such as vehicle, license, ETA, or other information the agency would like to convey. The rider will also receive an automated phone call 5 minutes prior to the vehicle arriving, so they can continue with their day until they are notified and don't have to block off significant time not knowing when their vehicle will arrive. Through our Open API, we can also integrate with other IVR solutions, such as Unified Dispatch, if additional capabilities are desired, such as trip booking, cancellations, etc. IVR utilizes software with chatbot capabilities, as well as live chat and email support ticketing. Spare has direct access to managerial (email) and operational staff (integrated ticketing system with Slack notifications) with a third party call center.
2.a-3	The Vendor develops and exposes APIs that are managed using a commercial off the shelf (COTS) API management solution that supports functionality provided in the demand-response system, including: 1. Client management	Core	Spare has unprecedented experience in building and supporting an API using a commercial off the shelf (COTS) solution such as Spotlight. Our API has been available since the beginning of the company and we have proven integrations with solutions such as GoPass which allow a fully functional booking experience for customers including: 1. Client management 2. Reservations

2. Reservations 3. Dispatching and Scheduling 4. Customer service 5. Fare payment 6. Reporting. Include in the proposal examples of APIs and a description of the features and functions supported by existing APIs.	3. Dispatching and Scheduling 4. Customer service 5. Fare payment 6. Reporting

3. Demand Response Software

a. Demand Response General Specifications

ID	Specifications	Feature	Spare's Response
3.a-1	A secure, cloud-hosted, SaaS solution that includes administrative software to support demand response operations	Core	Spare Launch is where DROs will set-up, run and monitor your demand response service in real-time. The Admin portal serves as the dispatcher and administrator-facing applications where DROs can easily and quickly create service zone(s), specific transit stop locations, set the operational time limit, set driver shifts, track vehicles, book and schedule trips based on requests, and more. As the first software provider that is both SOC 2 and HIPAA compliant, Spare takes special care to ensure customer and corporate data is kept secure and private.
3.a-2	A system that reduces the need for manual data entry and duplicative data entry.	Core	Spare offers many features to reduce reservationist time spent per booking. This includes, but is not limited to: automatic checks to ensure that ride request meets eligibility, service zone, time rules and other requirements before confirmation; favorite locations to pre-fill pickup and drop-off address; one click edits to make any changes to ride booking; one click return, recurring and rebooking feature; and automatically populating accessibility needs like wheelchair, notes and other custom requirements so booking agents do not need to fill them each time.
3.a-3	A system with multi-user capability, allowing simultaneous users working at different workstations to access and effectively use the software for all associated activities.	Core	Multi-user capability is used and encouraged in the Admin portal (Spare Launch & Spare Analyze). The Admin portal serves as the dispatcher and administrator-facing interface where multiple booking agents can simultaneously book trips with no degradation in the booking experience. Administrators can easily and quickly create service zone(s), specific transit stop locations, set the operational time limit, set driver shifts, track vehicles,

			book and schedule trips based on requests, and more. Spare's powerful vehicle management module allows for creating vehicle records with custom fields so that DROs can add all vehicle attributes it requires. Staff can specify capacity of the vehicles and accessibility features to match trips with sufficient vehicle capacity. Vehicle attributes may be changed at any time and can be swapped when duties are started or in progress to allow for maximum flexibility to respond to last minute changes in vehicle availability.
3.a-4	System security features limiting access to major functions based on assigned roles.	Core	Account creation and user management is easy with Spare Platform. Spare utilizes a one-time-password sign in with a user's phone number. This is to ensure that a phone number is on file for notifications about the transit customers' trips. Phone numbers or email can be used for password recovery. Spare uses a combination of role-based permissions and individual product permissions to manage user access to the administrative/staff platform. Spare can support single-sign on for the staff platform through an integration with WorkOS. Each Spare Platform user at the office level has a specific set of permissions based on roles. They are: Administrator (the highest level of permissions), Operations Manager, Booking Agent, Scheduler, Service Planner, and Finance Manager. Additionally, Administrators can grant privileges only for access to Reporting, access to Analytics, and access to Spare Realize. Roles are based on function and do not implement row-based security at this time. As an example, a service planner would have access to configuration options for the service, whereas the booking agent role can only book trips and cannot alter service parameters. DROs can be certain of the security of the system with the access of the different user groups and have visibility into any changes in the platform.
3.a-5	A fully automated system providing real-time and batch order taking, scheduling, and dispatching for demand response transportation trips.	Core	Spare has the capacity to support both real-time and batch rescheduling. The algorithm will automatically prioritize batched trips in this scenario and real time trips will be provided with a realistic ETA. Spare will ensure that real time trips are inserted as early as possible without moving the scheduled trips outside their flexibilities.
3.a-6	A system providing accurate transaction history that includes: 1. Date/Timestamp for all actions taken in the software 2. Associated (and unique) user ID for all actions taken in the system	Core	Event-level logs are available via Spare's 'Activity log' feature. all user activity is recorded and timestamped and user ID is available when an action is taken by an individual. If the action is automated such as an automatic re-match of a request, it is also recorded

	3. Record of all automated system actions to address system failures or issues 4. Any software malfunction resulting in failures or impacts normal operations.		as such. System issues are also recorded in a timestamped manner. Activity logs show the viewer all the activity that has happened on the object, what action was taken, who took it, when did it happen, along with more detailed information about the modification (like what changed) on a details page. As an example the following activities are recorded. Requests logs: - Estimate Generated - Request Created - Request Accepted - Request Rematched - Duty Canceled - Request Edited - Notification Sent - Request Canceled Run activity log: - Duty Created - Duty Edited - Duty Canceled - Duty Paused - Duty Resumed
3.a-7	A system with online "Help" that provides support for end users.	Core	Online "Help" is available and provides support for end users via web interface. An in-platform chat feature is also available to seek support.
3.a-8	A system with a scalable architecture that handles expansion in use as the need arises without adversely impacting systems management and operations.	Core	Spare is built on a highly scalable architecture that lets the platform scale with no disruption or downtime. Spare's multi-region system design illustrates the multi-region environment that allows Spare to operate full operational redundancy. By operating all critical components of its reservations, scheduling and dispatching within the Google Kubernetes Engine (GKE), Spare Platform's system is one of the most robust and stable systems in the world—due to it always having a backup location to fall back on in case of any system issues (i.e. network or server failures within the data centers). Spare also does not put any limits on the number of staff, drivers or riders that can access the system at any given time—further reaffirming our scalable design.
3.a-10	A system that utilizes a recognized relational database management system that allows for mission critical database management capabilities.	Advanced	Spare runs on a Postgres database which is a recognized relational database management system. All data stores (Postgres and Redis) are in "high availability pair" mode, meaning there's a "primary"

			node and a "secondary" that contains the same data for maximum redundancy.
3.a-11	A system that follows an open architecture design model, allowing the DROs to independently develop interfaces and/or enable integration with other internal or third-party systems, including but not limited to the following state programs: 1. Medicaid Brokers (currently ModivCare and OneCall) 2. North Carolina Cares 360 (NCCares360NCCARE360) 3. North Carolina Tracks (NCTracks).	Advanced	As mentioned in our Open API response, Spare has proven experience integrating with various entities including brokering trips via third parties. Spare has already integrated with Uzurv, Lyft, Uber, Unwire etc. Spare will commit to integrating with ModivCare, OneCall, NCCares 360, and NCTracks should we be chosen as the platform for demand response services in North Carolina.
3.a-12	A system that supports the migration of existing manually geo-coded locations from the existing scheduling software to the new scheduling software. The DROs may have created manually coded locations to supplement existing mapping gaps for existing addresses.	Advanced	Spare can migrate existing geocoded locations. However with modern technology using the Google API, there is no need for manual geocoding in Spare. All addresses are automatically geocoded at the time of ride booking. If an address is not available in Google, it can be manually geocoded, but instances of such an event are extremely rare.
3.a-13	A system shall that provides address verification for all addresses entered and supports the ability to editing of mapping coordinates, or manually verifies the address if the system is unable to provide an accurate verification. Any changes or manual verification will be clearly noted as such, be available to all dispatchers, and be used for scheduling and routing.	Advanced	Spare is confident that automated geocoding supported using the Google API is the most robust and error free way to geocode addresses. If there is a need for verification of addresses, Spare will support DROs in this process.
3.a-14	A System that provides an integrated mapping solution that supports frequent mapping updates and is consistent with the map used for routing in the driver display and with scheduling and dispatch staff.	Advanced	Spare provides a fully integrated mapping solution that may be updated at any time using Open Street Map. This background map will be used by the drivers for navigation. Spare can be integrated with mapping and vehicle location services to perform route optimization functions and scheduling based on updated street network data.
3.a-15	A System that displays the approximate route of demand responsive vehicles in service based on their scheduled stops (either straight line or expected	Advanced	Spare always displays a vehicle's anticipated route along with stops. The route becomes active as soon as the run begins.

	turn-by-turn route, with stops highlighted).		

b. Client Management

ID	Specifications	Feature	Spare's Response
3.b-1	A system that allows for real-time customer record updates allowing authorized staff to: 1. Add, remove, and modify client data 2. Suspend and activate clients.	Core	Yes, customer records can be modified at any time by an administrator. This functionality includes the ability to add, remove, and modify client data, as well as suspend and activate clients.
3.b-2	A system that includes the option to display, add, delete, and modify the following data for each client: 1. Client name(s) 2. Gender 3. Birth date 4. Fare type 5. Registration, expiration date, and current status 6. Complementary ADA eligibility, status, and renewal date 7. Mobility aides 8. Unique client identification number 9. Medicaid ID number 10. Ability to include multiple addresses including building name and number, unit name or number, city, state, zip code for pickup, and/or billing/mailling 11. Telephone number (at least two (2) telephone numbers) 12. Emergency contact name and telephone numbers (at least two (2)) 13. Additional passengers (e.g., personal care aid, companions, etc.) 14. Email 15. Comments field.	Core	All of the fields listed may be added to the client profile using a feature called 'custom fields'. Spare has the ability to add custom fields and this shall include: 1. Client name(s) 2. Gender 3. Birth date 4. Fare type 5. Registration, expiration date, and current status 6. Complementary ADA eligibility, status, and renewal date 7. Mobility aides 8. Unique client identification number 9. Medicaid ID number 10. Ability to include multiple addresses including building name and number, unit name or number, city, state, zip code for pickup, and/or billing/mailling 11. Telephone number (at least two (2) telephone numbers) 12. Emergency contact name and telephone numbers (at least two (2)) 13. Additional passengers (e.g., personal care aid, companions, etc.) 14. Email 15. Comments field
3.b-3	A system that allows authorized staff to look up clients by data attached to the profile or client record (e.g., name, date of birth, address, etc.).	Core	Spare can make any field searchable and this can include name, date of birth and address. More fields may be added to the 'searchable list' at any time.
3.b-4	A system that allows authorized users to query tables of riders,	Core	Custom queries for trips may be generated in Spare.

	reservations, and trips based on user-defined search parameters		
3.b-5	system that displays the client's most recent trips, scheduled trips, reservations, canceled trips and no-shows.	Core	Yes, all trips associated with a client with statuses such as 'scheduled', 'reservation', 'in progress', 'canceled' and 'no-shows' can be displayed and filtered.
3.b-6	A system that includes trip details and history specific to each client such as trip origins/destinations and dates, time spent onboard the vehicle, and any other relevant information.	Core	Yes, all trip data can be accessed via client profile or through the ridership report allowing the DROs multiple ways to find information such as origins/destinations and dates, time spent onboard the vehicle, and any other relevant information.
3.b-7	A system that tracks customer eligibility status and automatically notify the DROs and clients of upcoming eligibility expirations.	Advanced	Yes, Spare Engage is a module purpose built for eligibility management and will automatically notify DROs and clients of any eligibility expiration via text, mail, e-mail etc.
3.b-8	A system that allows for the assignment of different eligibility levels with different expirations.	Advanced	Yes, eligibility in Spare is managed via 'Groups' and each group has its own eligibility level and a client can have a unique expiration date under each category or group.
3.b-9	A system that supports online comprehensive rider registration for both complementary ADA paratransit and non-ADA paratransit riders and clearly delineates between them.	Advanced	Yes, Spare can clearly delineate between ADA paratransit and non-ADA paratransit riders and we do in many services we currently operate. For example, Citibus in Lubbock Texas operates over 6 different types of service in Spare. Using 'Groups' we can clearly identify the riders who are ADA vs non-ADA and ensure that each gets the appropriate service. The vehicles may still be common among the 2 services.
3.b-10	System allows the DROs to include additional client data such as: 1. Primary language spoken (with the system automatically defaulting to English) 2. Sponsor/Eligible funding 3. Fare type and preferred fare payment method 4. Contact information formats (i.e. large print, Braille, etc.) 5. Client home GPS coordinates 6. Passenger-specific load time allowance, in minutes, in addition to the default or standard load time allowance 7. Certification/Denials/Appeals history.	Advanced	Yes, using custom fields, the following data may be added by the DROs including: 1. Primary language spoken (with the system automatically defaulting to English) 2. Sponsor/Eligible funding 3. Fare type and preferred fare payment method 4. Contact information formats (i.e. large print, Braille, etc.) 5. Client home GPS coordinates 6. Passenger-specific load time allowance, in minutes, in addition to the default or standard load time allowance 7. Certification/Denials/Appeals history
3.b-1	A System that includes a customer-facing application module that allows clients,	Advanced	Yes, Spare's purpose built eligibility management solution, Engage, dramatically improves the

	caregivers, or care facilities to apply for demand response eligibility through any web browser. 1. The application module is be easy to navigate and meets ADA accessibility standards; 2. To reduce the need for manual data entry, the application module is be linked to the customer database and new client records are automatically created upon application approval.		experience for transit agencies, paratransit riders, and prospective riders by: 1) Digitizing the application process through the use of digital forms and smart scanning of paper forms). If the DRO still collects paper applications, they can utilize the powerful Smart Scanning feature of Spare Engage to scan paper forms with optical character recognition (OCR) and convert handwritten information into usable data within seconds. 2) Creating client records automatically that can then be assigned to the right personnel, updated in real time and tracked through various stages of the eligibility process.
3.b-2	A System that automates correspondence with clients through text messages, emails, or pre recorded phone calls regarding eligibility approvals, expirations, denials, or appeals.	Advanced	All correspondence may be automated with Spare Engage. For example, expirations can also be automated in Spare Engage. When a person is assigned to a group (e.g. ADA paratransit), their group membership could be set to expire when their eligibility does. As that date approaches, the system would send out a series of notifications either by phone, email, SMS, notifications in the white-label app and / or mail. It advises agencies and riders that action needs to be taken and ensures that no one falls through the cracks. Further, Engage can automate applicant communication such as updates on status, request for more information, and more. This reduces time spent on rider communication, and provides a more streamlined customer experience. Doctor's notes and forms can be attached digitally to rider profiles, significantly reducing paper-based management of rider information, particularly sensitive medical information.
3.b-3	A System provides tools or features to support adding clients (e.g., partners living at the same address, group homes, etc.) to facilitate rapid entry of client data.	Advanced	Yes, more associated fields or clients can be added electronically via Engage reducing overhead for such tasks.

c. Reservations

ID	Specifications	Feature	Spare's Response
3.c-1	A system that allows clients, caregivers, and DRO staff to easily view, create, modify, or cancel trips.	Core	Spare Launch allows clients, caregivers and DRO staff to easily view, create, modify or cancel trips.
3.c-2	A System that: 1. books same-day trips	Core	The system supports the ability for same-day trips, subscription based trips, as well as

	2. schedules standing-order (subscription) trips 3. accepts advanced reservations.		advanced reservations. The DROs have the ability to create different and specific booking parameters for each service as they see fit.
3.c-3	A system that allows standing-order trips to be scheduled on a weekly (e.g., every Monday) or monthly (e.g. first and third Monday) basis. A system that allows the DROs to temporarily suspend standing-order trips without needing to modify trips outside of the suspension period.	Core	Spare enables robust options for booking recurring trips such as any combination of days.
3.c-4	A system that books trips based on pickup time or arrival time. When scheduling by arrival time, the system automatically factors in travel time from origin to destination.	Core	The Spare mobile applications and web booker enables riders to view the vehicle's location and estimated pickup (arrival) time on a map-based interface. All Spare systems are synced so a rider will be able to book on one method (such as over the phone or by themselves) and monitor the trip via the mobile app and web booker. Spare will provide an estimated time of departure and arrival before confirmation of the trip.
3.c-5	A system that generates a confirmation number for each reservation, revised reservation, and trip cancellation. The system allows users to query the system by confirmation numbers to display transactions.	Core	Spare tracks all stages of a trip reservation. It preserves the original ID to make tracking of any changes easy and can be queried.
3.c-6	A system that provides safeguards that prevent errors such as past date booking, duplicate trips, and booking clients with expired applications, and booking outside the service area.	Core	Spare's algorithm has built in safeguards that prevent reservation errors such as past date booking, duplicate trips, booking clients with expired eligibility and booking outside the service hours and service area. If a reservation that does not comply with the business rules is being attempted, an error will pop up preventing the reservation from being made.
3.c-7	A system that automatically removes an associated drop-off from the manifest if a pickup is canceled due to a no-show.	Core	The platform will automatically remove a trip from the manifest if a ride is canceled.
3.c-8	A system that automatically finds an earlier or later time for scheduling when a requested time is unavailable based on capacity constraints.	Core	Spare will create an overbooking reservation and find a match as soon as it can closest to the original requested time. There is also a way to manually override constraints to insert important rides in the system.
3.c-9	A system that sends automatic text or phone notifications to clients as a vehicle approaches a location for a pickup.	Core	Spare can send notifications to the rider when the vehicle is approaching. The notifications can be customized and sent via text, email or phone call. The rider can also track the vehicle via web portal or the rider app.

3.c-10	Vendor provides explanations of any limitations for scheduling rides including limitations for the number of vehicles and/or passenger trips that can be scheduled.	Core	The only limitation for scheduling in Spare is the number of vehicles available. There are no IT related limitations on the Spare platform. Spare will scale to as many trips as are needed to run demand response in for each DRO.
3.c-11	A system that alerts the user when the origin or destination of a trip is not within the specified boundary during service hours and prevents the trip from being booked unless overridden by approved DRO staff.	Core	The platform will notify users if the trip cannot be performed because the destination falls outside of the boundary of a given service area.
3.c-12	A system that provides an option to select locations without a street address (e.g., can identify a street corner or XY coordinates).	Core	A coordinate can be selected instead of an address when booking a trip in Spare.
3.c-13	A system that prevents a user from booking a trip if the eligibility of the rider is suspended, except when suspension is because of an expired funding source. If a suspended rider has booked subscription trips or reservations before the suspension, the system will not schedule these trips while the rider is suspended.	Core	Spare's sophisticated algorithm can identify scheduled standing-order trips, and will prevent those trips from being scheduled if a rider is suspended. An expired funding source will be treated differently and rides may be allowed for that rider based on DROs operational policies.
3.c-14	When a subscription standing order trip is canceled, the system checks ahead and displays other trips for this rider that will be canceled. The system permits the user to cancel one, multiple or all future trips.	Core	DROs can add exceptions to the standing order which lets the system know this trip is not required on this day. The cancellation will only impact the exception day(s). If the standing order is canceled then all future trips will be canceled.
3.c-15	The system allows users to schedule one-way, round-trip, and multi-leg trips with minimal data entry, by auto-populating data.	Core	The system will auto-populate data to enable the scheduling of trips with minimal data entry.
3.c-16	The system allows a user to book disconnected legs of a trip.	Core	Spare enables DROs to easily view, create, modify, or cancel one-way, round-trip, and multi-leg trips for all trip types including same-day and standing-order trips.
3.c-17	The system allows reservations to be made for groups traveling together who have an identical origin and destination. These group reservations shall be assigned to the same vehicle to the maximum extent possible.	Core	Spare's advanced algorithm is designed to improve efficiency while ensuring none of the flexibility parameters for such trips are violated. We will group trips based on location and schedule to maximize service efficiency.

3.c-18	The system displays all reservations by a rider or address to facilitate individual and/or group cancellations.	Core	The system displays all rides by a rider. Spare does not currently show rides by address, but can add that option if it is important from an operational point of view. As Spare would automatically pool rides to the same address when it is efficient, it is easy to find rides to the same address. Group cancellations can be done if the trip is under the same reservation.
3.c-19	The system shall shows estimated trip lengths for all trips created.	Core	Yes, Spare shows estimated trip length at time of trip booking.
3.c-20	The system supports lists of vehicles, vehicle run numbers, run times (shifts), and drivers that the user can configure or edit.	Core	Spare Launch is where DROs will set-up, run and monitor their demand response service in real-time. The Admin portal serves as the dispatcher and administrator-facing applications where DROs can easily and quickly create service zone(s), specific transit stop locations, set the operational time limit, set driver shifts, track vehicles, book and schedule trips based on requests, and more. The Spare Launch portal is directly connected and feeds data back and forth with the Analyze Admin Portal. This provides DROs real-time access to system information and configurations for administrative users through an easy to use web-based interface.
3.c-21	The system provides multiple user-defined seating/wheelchair arrangements for each type of vehicle. This must include a minimum of five (5) different arrangements to incorporate zero (0) to four (4) wheelchairs with corresponding seats.	Core	Spare allows for the addition of accessibility features to each vehicle. Vehicle capacity can also be adjusted to account for the addition of accessibility features such as wheelchairs. The system will take into account capacity limits when assigning trips. For example, if the vehicle allows for the seating of 10 but only 4 with two wheelchairs, the system will not assign more than four riders with the two wheelchairs.
3.c-22	The system automatically generates trip reversals or return trips from destination to origin when trips are booked.	Advanced	Spare can automatically generate return trips from destination to origin in a single click.
3.c-23	The system provides quick access for a customer's most frequent trip origins and destinations for quick selection during booking.	Advanced	Favorite locations can be saved to provide quick access to a customer's most frequent destinations for quick selection during booking.
3.c-24	The system supports multiple service providers. The parameters for each provider are configurable such that the service allocation may be based on predetermined factors including but not limited to the following:	Advanced	The system can support multiple providers with unique requirements and configurations. The providers can be given limited permissions so they can schedule their fleet and be automatically assigned trips based on the following factors as identified by NCDOT: 1. Vehicle type

1. Vehicle type 2. Geographic area 3. Day of the week 4. Time of day 5. Origin and/or destination 6. Nature of rider disabilities and/or physical aids.	2. Geographic area 3. Day of the week 4. Time of day 5. Origin and/or destination 6. Nature of rider disabilities and/or physical aids.

d. Scheduling

ID	Specifications	Feature	Spare's Response
3.d-1	The system groups trips based on location to maximize service efficiency and provide the ability to lock recurring trip(s) to specific schedules, drivers, or vehicles to provide stability and consistency for customers with regular/recurring appointments.	Core	Spare provides a high weightage to trips based on location so that efficiency is maximized and riders have to do minimal detour. Recurring trips may be locked to a vehicle or run so that drivers and riders can enjoy familiarity and consistency. If however, there is a disruption, Spare would automatically rematch those trips to the best available alternative.
3.d-2	The system allows for trips to or from same origins, or to same destinations, to be combined to eliminate duplicate trips.	Core	Spare would automatically eliminate duplicate trips. It would also pool riders to minimize detours.
3.d-3	Vehicle assignments are automatically updated if a vehicle needs to be pulled from service or if a vehicle is running late.	Core	Yes, Spare's advanced algorithm and real time optimization called Global Optimization of Live Duties (GOLD) will automatically update assignments and re-allocate trips in seconds and move the trips from late or canceled vehicles to better options. For example, if a vehicle has a canceled trip then that space would be used by another trip.
3.d-4	The system considers capacity constraints of each vehicle or route. These constraints are adjustable and easily altered on a day-to-day basis.	Core	Spare considers actual vehicle capacity at all times in the manifest to ensure that while capacity is maximized there is enough room in the vehicle for riders and accessibility features like wheelchairs. The constraint can be adjusted at any time.
3.d-5	The system takes into account different travel times during specific peak hour traffic periods, in congested areas, and at places where physical barriers affect travel load and unload time.	Core	Spare is always looking at real traffic and travel times for various specific times of the day to predict travel times. Load and unload times are also customizable for each accessibility feature and can be altered for any specific day as well. Further when vehicles are delayed, riders are informed and trips may be moved in a manner to ensure maximum (On-Time Performance) OTP.
3.d-6	The system calculates actual non-revenue hours and mileage as well as actual revenue hours and miles for all vehicles on a daily basis.	Core	Non-revenue, deadhead, mileage and actual revenue hours are calculated for all vehicles on a daily basis.

3.d-7	The system prints vehicle manifests on a daily basis. The system formats printed manifests in a manner that minimizes paper waste, in a legible font size suitable for drivers to reference while enroute, and only includes minimal information (e.g., client name, pick up/drop off address, scheduled window, etc.). Printed manifest details and layout will be defined during design review.	Core	Manifests are dynamic and may change during the day. Therefore, Spare does not recommend printing manifests. There may be an extreme event such as a major network failure that may require printing in which case that may be requested, but the need for printing is extremely rare. If printing of manifest is required, the DRO may choose what fields to include.
3.d-8	The system allows users to view maps that illustrate fixed route bus routes and bus stops relative to trip origins and destinations.	Core	Spare has a multi-modal feature which shows bus stops and routes in map view while booking trips.
3.d-9	The system provides for manual mapping of addresses if the system map does not recognize an address.	Core	Addresses may be manually added. Typically, asking Google to add an address is a preferred solution and they respond very quickly to such requests. For immediate need, a coordinate may also be used to book the trip when the address does not exist in the system.
3.d-10	The mapping system is fully compatible with the mapping system used by tablets and based on an open architecture and integrated with Automatic Vehicle Locator (AVL) and tablet technology.	Core	Spare provides a native driver application for navigation and AVL purposes. This application is compatible with any off the shelf Android or iOS device.
3.d-11	The system supports real-time and batch rescheduling.	Core	Yes, Spare supports both real time and batch rescheduling and optimization.
3.d-12	All trip time changes are within the original promised time window and permit the rider to meet a stated appointment time.	Core	Yes, all time changes and adjustments will follow the original promised time window. For 'Arrive-by' or appointment type bookings, Spare ensures that the rider arrives by the designated time.
3.d-13	The system maintains an open return list (e.g., will calls) for passengers with an uncertain pickup time for the return leg of a trip (e.g., after a medical appointment of uncertain duration).	Core	Will calls can be maintained in a specific service and matched to a vehicle when appropriate. Using real-time optimization, Spare would find the best spot for will-calls when available.
3.d-14	When vehicles are removed from a service, the system converts any previously assigned trips for that vehicle to the status "unassigned" for reassignment. The system supports reassignment of all trips to a new vehicle/driver.	Core	Yes, when vehicles are removed from a service, those trips will automatically get re-assigned to existing vehicles. However, if there isn't any room available on existing runs then those trips will enter an "unassigned" state.

3.d-1 5	For cancellations, or changes to the pick-up time on a route, the system recalculates the remaining pick up and drop-off times.	Core	Yes, unlike tools that can just provide real time ETA information to riders, Spare can do a lot more than updating the ETA and will work to ensure trips are delivered within service parameters set by the agency. The Spare engine can dynamically re-allocate trips, provide notifications and respond to changes in real time. During the course of a typical day several unforeseen situations may occur such as traffic delays, breakdowns, cancellations, on-demand bookings etc. Spare is continually updating the manifests by taking all these factors into consideration. For example, a cancellation may result in a trip being moved from a delayed vehicle to that duty and a new trip request would automatically be matched in a way such that scheduled trips are not affected.
3.d-1 6	The system allows the user to mark specific trips as "critical" or exempt from automated modification. If a critical trip must be modified manually, the system provides sufficient controls or notifications to the dispatcher.	Core	A trip may be "locked to duty" which will prevent it from being reassigned. However, at any time manual intervention is allowed so the trip may be moved or manually edited by the dispatcher.
3.d-1 7	The system avoids sending a vehicle that does not meet the needs of the passenger's disability.	Core	Yes, Spare would never send a vehicle that cannot meet the specific accessibility feature requirements.
3.d-1 8	The system features automatic trip optimization. The system continuously updates and adjusts trips based on vehicle position, trip cancellations, and no shows. Automatic trip optimization maximizes service efficiency while reducing the need for manual schedule adjustments.	Advanced	Yes, with the Global Optimization feature, DROs can define how you want the system to run and then let the system do all the heavy lifting in real-time to continually optimize based on your business rules. This includes optimizing duties that are currently active with a manifest: in essence, rematching near-term trips. This helps keep riders happy in events when drivers may be running late to pickups earlier on in the trip manifest, or when there is new availability on a specific duty due to a cancellation. Additionally, there are protections in place in order to prevent negative experiences for riders. For instance, Spare will not optimize a trip request if a driver is already heading for the pickup. Citibus (Lubbock, TX) leverages GOLD for its paratransit and microtransit service. Powered by Spare, the service highlights a 27% increase in "On-Time Performance" due to Global Optimization. It's a clear win for efficiency as they went from 75% of trips being "On-Time" to averaging 94-97% consistently.
3.d-1 9	The system integrates with mapping and vehicle location services to perform route optimization functions and	Advanced	Yes, all vehicles' live locations are updated every 3-5 seconds and the system performs route optimization in real time using the latest routing data.

	scheduling based on updated street network data. Route and turn-by-turn driving directions are highly desirable.		Turn-by-turn driving directions are available to the driver.
3.d-20	The system allows the DRO to easily add, remove, and modify service boundaries based on service type and driver.	Advanced	Service boundaries can be changed at any time by the administrator and this can be done on an individual service basis.
3.d-21	The system routes and schedules trips according to configurable parameters including: 1. Shared rides 2. Pick up time window 3. Drop-off time 4. Mobility aids or mobility restrictions 5. Number of passengers/space available in vehicle 6. Assignment of runs to specified geographical zones. The system allows DROs to modify all parameters.	Advanced	Spare is highly configurable for specific service and DRO requirements are all parameters including the following may be modified via the user interface: 1. Shared rides (Pooling ability) 2. Pick up time window (Leave-at flexibility) 3. Drop-off time (Arrive-by flexibility) 4. Mobility aids or mobility restrictions (Accessibility features) 5. Number of passengers/space available in vehicle (Vehicle configurations) 6. Assignment of runs to specified geographical zones. The system allows DROs to modify all parameters. (Configuration is done at the service level allowing for individual settings for DROs)

e. Dispatching

ID	Specifications	Feature	Spare's Response
3.e-1	The system displays the following minimum information for dispatchers for all pick up/drop off: a. Vehicle number b. Passenger name, last name first c. Number of passengers, including attendants and companions. d. Pickup and drop-off address e. Promised arrival time window f. Estimated time of arrival g. Any special needs or problem address h. Notes.	Core	Spare can create custom fields which are also visible to the dispatchers. The following information is visible to the dispatchers via 'Mission Control': a. Vehicle number b. Passenger name, last name first c. Number of passengers, including attendants and companions. d. Pickup and drop-off address e. Promised arrival time window f. Estimated time of arrival g. Any special needs or problem address h. Notes
3.e-2	The system provides necessary dispatching tools for making service day operational decisions. At a minimum, this includes tools for same day and standby trips, canceled trips, no-shows, late riders, vehicle breakdowns, and open returns. The system allows the dispatcher to move trips, change drivers and vehicles, and adjust the schedules.	Core	Yes, Spare ensures that the dispatchers have all tools necessary to make real time decisions that would support riders and ensure a smooth functioning operation. Spare provides these tools via mission control. Mission Control is a new command center for dispatchers. It enables dispatchers to keep a close eye on the current day's operations and drill into challenges before they occur. Mission Control consists of two main modules, Live Map and Live

			Requests. Live Map will remain unchanged, but will now live under the “Mission Control” item in the sidebar. Live Requests is a new module that enables dispatchers to: - Get an overview of current aggregated OTP for the day, including completed and predicted OTP - Identify trends in OTP, by breaking down by hour - Drill down into current request stats by Service and Driver - Action immediately with quick filters based on your selection
3.e-3	The system allows for a specific driver to be assigned to a route and allows the dispatcher to change a vehicle number.	Core	Yes, a specific driver can be assigned to a route and the dispatcher can change the vehicle number at any time.
3.e-4	The system allows dispatchers to override routing due to road construction and traffic pattern changes on a one-day or permanent basis.	Core	Road construction and other traffic pattern changes can be incorporated via open street map edits that can be done for a one-day or permanent basis.
3.e-5	The system allows dispatchers to schedule driver breaks.	Core	Yes, Spare offers driver break functionalities configured by the DRO's staff creating driver schedules. Breaks can be configured by policy for example, a driver may drive a maximum of 6 hrs without a break and minimum break time is 30 mins.
3.e-6	The dispatching module displays: 1. Selected route and associated trip details; 2. Vehicle ID numbers and locations updated at least every 30 seconds; 3. Scheduled arrival times; 4. Real-time arrival predictions and on-time performance; 5. Client names and the number of passengers per trip.	Core	The dispatching module, via Mission Control will display the following information: 1. Selected route and associated trip details 2. Vehicle ID numbers and locations updated at least every 30 seconds 3. Scheduled arrival times 4. Real-time arrival predictions and on-time performance 5. Client names and the number of passengers per trip
3.e-7	The dispatching module displays one route at a time or multiple routes.	Core	The dispatching module, via Mission Control can be filtered for one route or multiple routes at a time.
3.e-8	The system allows the user to display a list of all of the day's scheduled trips for a client.	Core	All scheduled trips for a client can be generated for the day or into the future, as well as the past based on filters.
3.e-7	The system allows the dispatcher to manually override each trip's assigned route and pickup or drop-off time.	Core	Yes, Spare allows dispatchers to edit and rematch a trip when required.
3.e-8	The system allows the dispatcher to override batched trips and	Core	Yes, Spare allows batched trips to be moved to another vehicle.

	manually move them to an alternate route.		
3.e-9	The system allows users to easily transfer passenger trips from a selected route(s) based on least incremental mileage.	Core	No. There is no least incremental mileage ability in Spare.
3.e-1 2	The system provides the number of trips for each route and track driving speed history.	Core	Yes, the duty report includes the number of trips, but Spare does not report driving speed currently. This is a roadmap item that can be included if desired by an agency.
3.e-1 3	The system displays all dispatch activity for any route and allow the dispatcher to add dispatch activity notes.	Core	Yes, dispatch activity can be recorded by way of duty notes.
3.e-1 4	The system allows the dispatcher to transfer single trips or a block of trips between vehicles/drivers.	Core	A single trip may be reassigned if the entire duty schedule can be put on a different vehicle.
3.e-1 0	The system logs all dispatcher actions and attributes them to the logged in user.	Core	Yes, Spare's activity log captures all dispatcher actions.
3.e-1 6	The system allows dispatchers to see: 1. Cancellations and insertions occurring within a configurable timeframe 2. Runs not covered by a driver 3. Unassigned trips.	Advanced	Yes, all 3 views are available in the Mission Control feature of Spare. 1. Cancellations and insertions occurring within a configurable timeframe: Spare can track ride status including cancellation by time period 2. Runs not covered by a driver: Runs with no drivers show as 'Unassigned' in the duty schedule 3. Unassigned trips: Trips that don't have a run are shown as 'unscheduled'
3.e-1 7	The system has dispatching tools that are simple to use and efficient to enter and retrieve information. The dispatching solution that is flexible and configurable for each dispatcher allowing dispatchers to create custom dispatch data views based on the type of dispatching methods performed.	Advanced	Yes, custom views may be generated in Mission Control depending on what the dispatcher method is. For example, the dispatcher may only want to address unscheduled rides or late trips and take action on those.
3.e-1 8	The system allows the DROs to manage unexpected enroute origin and destination changes.	Advanced	Yes, through 'edit and rematch' functionality, unexpected origin and destination changes can be addressed.
3.e-1 9	The system provides the DROs with two-way text messaging from dispatch to DRO. Messages shall be saved or archived in the system for future reference.	Advanced	Yes, two way text between the DRO and dispatch can be enabled and saved for future reference.
3.e-2 0	Incoming messages from drivers are grouped by vehicle/driver and	Advanced	Spare offers basic driver dispatch texting, however there can be enhancements made once we

	sorted by prioritization (e.g., high priority messages on top). All messages include an audible tone or notification to alert the dispatcher when messages are received from the driver display solution.		understand the DRO's use case. Spare's goal is to minimize the need for direct communication as manifest changes, notes etc. are automatically communicated to the dispatch center.
3.e-2 1	The system notifies dispatchers when a vehicle is running late by a configurable amount of time. These parameters are configurable based on the parameters set by the individual DROs (e.g., Client type, ADA status, etc.).	Advanced	Yes, the system notifies dispatchers when a vehicle is late over a certain amount of time.

f. Driver Display Functionality

ID	Specifications	Feature	Spare's Response
3.f-1	The driver display provides drivers with an overview of their complete schedule/manifest and allows them to view details for any pickup/drop off. Details include: 1. Client name(s) and companions/PCA 2. Mobility aids used by clients 3. Dispatch and scheduling comments 4. Fare/sponsor 5. Pickup and drop-off address and any applicable notes 6. Pickup and drop off window/appointment time 7. Business name/building name for each pickup or drop-off.	Core	Yes, all the mentioned fields included in the list will displayed for the driver: 1. Client name(s) and companions/PCA 2. Mobility aids used by clients 3. Dispatch and scheduling comments 4. Fare/sponsor 5. Pickup and drop-off address and any applicable notes 6. Pickup and drop off window/appointment time 7. Business name/building name for each pickup or drop-off.
3.f-2	The driver display or tablet requires the Driver to logon using the DRO assigned credential. When applicable, the driver display allows the driver to enter (or confirm) the current odometer reading for the vehicle.	Core	Yes, drivers can log on using their DRO assigned credential and the odometer reading can be entered in the Spare Driver app.
3.f-3	The driver display includes demand response specific functionality to display electronic manifests and receive updates in real-time from the Vendor provided dispatching system. Updates include changes to the schedule, trip specific detailed updates, cancellations, and additions to the manifest.	Core	Yes, the manifest reflected in the Driver app is always updated in real time and these updates include changes to the schedule, trip specific detailed updates, cancellations, and additions or changes in pickup/drop-off time.

3.f-4	The driver display allows the driver to easily scroll through the entire manifest.	Core	Yes, the driver can easily scroll through manifest by selecting 'View all stops'.
3.f-5	The driver display allows the driver to: Arrive, perform, cancel, and no-show trips as required by the DROs.	Core	Yes, all basic driver functionality including ability to arrive, perform, cancel, and no-show trips is included.
3.f-2	The driver display displays mapping using the same mapping software used to schedule the route.	Core	Yes, navigation is consistent using open street map.
3.f-7	Additional trip information includes: 1. Map view 2. Trip ID 3. Client type (e.g., Attended) 4. Estimated time to arrival at destination.	Advanced	Yes, the Driver app has the functionality to display a map view, trip ID may be added as a custom field, rider type and estimated time of arrival is shown.
3.f-8	Where applicable, the driver display includes a pullout and pull in checklist for Drivers at the start and end of service. Items included on the checklist are configurable by the DROs.	Advanced	Yes, a pre and post trip inspection may be performed in the app if required by the DRO.
3.f-9	The system allows drivers to provide pickup and drop-off comments for each trip. The system synchronizes with the client record and is available for future passenger trips.	Advanced	Yes, drivers can leave comments in the custom field if required by the DRO.
3.f-10	The driver display shows the vehicle's current odometer reading as calculated by the previous odometer entry and allows the DRO to manually correct the calculated vehicle odometer value.	Advanced	No, Spare does not show existing odometer reading as the system calculates vehicle miles directly from GPS on driver tablets. Odometer reading can be manually entered by the driver for verification as required by the DRO.
3.f-3	The driver display provides integrated canned messages that drivers may send to dispatch. Integrated canned messaging includes DRO customizable messages that can be sent directly from the driver display to dispatch.	Advanced	Yes, driver to dispatch canned messaging will be included in the Spare platform offering.

g. Billing and Invoicing

ID	Specifications	Feature	Spare's Response
3.g-1	The system supports trip pricing through a billing and payment feature. The system supports any combination required by the DROs: 1. Zone 2. Vehicle miles and/hours (service & revenue) 3. Passenger (rider) mile 4. Direct mile (Taxi)	Core	Yes, Spare offers a robust fare rules engine which can be customized to meet special client needs. All of the following fare structure determinants are supported: 1. Zone 2. Vehicle miles and/hours (service & revenue) 3. Passenger (rider) mile 4. Direct mile (Taxi) 5. Flat rate

	5. Flat rate 6. Hourly 7. Fixed route fares.		6. Hourly 7. Fixed route fares.
3.g-2	The system includes tariff management tools to administer all fare price and fare structure. The Agencies will establish the price of fares.	Core	Yes, a complete tariff management solution is part of the Spare platform and we have experience managing and supporting a variety of fare structures.
3.g-3	The system handles billing and invoicing functions for riders/trips.	Core	Spare offers a direct integration with a credit card processor that allows for automated payment collection. If preferred, all a DRO's services can be set up to accept cash fares to be collected by the driver instead of credit card payments. Fares are automatically calculated in the back office of the platform using a comprehensive fare rules tool that allows for a variety of fare calculations. Riders will know their exact fare at time of booking. Payment subsidies can be set up through fare rules and group membership, which allows specific riders enrolled in a group to have their fare calculated at different subsidized rates.
3.g-4	The system allows the Agencies to generate and print monthly billing invoices for payment. The system generates and prints reports in a CSV or equivalent spreadsheet format.	Core	Spare will provide robust data from which invoices can be generated. The CSV generated will be customizable and the DRO will have the ability to determine which fields are necessary for accurate calculations for the invoicing component.
3.g-5	The system automatically generates mailing labels for client billing and invoicing.	Core	Spare can support the generation of mailing labels.
3.g-6	The Vendor supports Payment Integration with State programs as a funding source for billing and payment. Vendor payment solutions provide Payment Card Industry Data Security Standard (PCI DSS) compliance and Vendor provides evidence of PCI compliance upon request by the DROs.	Core	Yes, Spare has a payment integration with Stripe which is a PCI DSS compliant vendor. The PCI certification can be supplied if requested.
3.g-7	The Vendor works with the DROs to confirm reporting level of detail for billing and invoicing purposes. Billing reports shall include, at a minimum: 1. Trip date(s) 2. Passenger name and number of passengers 3. Pickup/drop off location(s)	Core	Billing reports will include the following: 1. Trip date(s) 2. Passenger name and number of passengers 3. Pickup/drop off location(s) 4. Total number of trips by passenger 5. Total amount owed for each trip

	4. Total number of trips by passenger 5. Total amount owed for each trip.		
3.g-8	The Vendor provides customer service support to the DROs during system and financial audits.	Advanced	Yes, Spare regularly supports agencies with system and financial audits by way of supplying raw data, conducting special analysis etc.

4. Customer Applications

a. Mobile Applications

ID	Specifications	Feature	Spare's Response
4.a-1	The Vendor provides Mobile Applications and website user interface and user experience accessibility testing using a qualified accessibility expert with relevant experience utilizing assistive technologies.	Core	Yes, mobility, like food and running water, is a fundamental human need. It gives us freedom and enables connections. As a result, we are committed to building and maintaining software that is accessible for all and we do so by adhering to level AA of the WCAG 2.1 guidelines, which states that sites should be perceivable, operable, understandable, and robust. Our Product and Engineering teams' work is guided by the principle that transit is for everyone, regardless of age, disability, or access to technology. When accessibility comes first, technology truly starts to work for everyone.
4.a-2	The Mobile Applications are designed and tested for cross-platform compatibility, including Android and iOS mobile application platforms.	Core	Yes, Spare fully supports mobile applications on both Android and iOS mobile platforms.
4.a-3	The Mobile Applications support the most recent version of Google Android and Apple iOS mobile platforms at launch. Mobile Applications will be backwards compatible with a minimum of two (2) previous versions.	Core	Mobile Applications will support the most recent version of Google Android and Apple iOS mobile platforms and will be backwards compatible with a minimum of two previous versions.
4.a-4	The Mobile Applications are free to download from Apple App Store or Google Play Store.	Core	The Spare Rider app is free to download from Apple App Store and Google Play Store.
4.a-5	The Mobile Applications support the following functions: 1. Create an account 2. Link Client ID 3. Manage account (payment, contact information, personal care attendant, emergency contact and frequent address of travel)	Core	Yes, the Spare full supports the following functions: 1. Create an account 2. Link Client ID 3. Manage account (payment, contact information, personal care attendant, emergency contact and frequent address of travel) 4. View scheduled trips

	4. View scheduled trips 5. Book a trip 6. Modify a trip 7. Cancel one or many trip reservations.		5. Book a trip 6. Modify a trip 7. Cancel one or many trip reservations.
4.a-6	The Mobile Applications support shared permissions allowing personal care attendants or caregivers to manage customer profile, book a trip, modify a trip or cancel a trip.	Core	A third party such as a personal care attendant or caregiver can have access to the rider's profile with the rider's credentials. This will allow them to apply for demand response eligibility (register a new client), manage customer profile, book a trip, modify a trip or cancel a trip on the rider's behalf.
4.a-7	The Mobile Applications send a notification to the user when the ride is approaching/on the way.	Core	Spare can send notifications to the rider when the vehicle is approaching. The notifications can be customized and sent via text, email or phone call. The rider can also track the vehicle via web portal or the rider app.
4.a-8	The Mobile Applications adhere to branding guidelines of the DROs and will be approved during Final Design Review (FDR).	Core	Spare will allow for DROs to white-label the rider application and also create a custom branded portal, including a unique web address reflecting the service/system as being provided by the DRO. The portal and app will adhere to the DRO's branding guidelines, which will be approved during Final Design Review (FDR).
4.a-9	The Mobile Applications display text in alternate languages including, but not limited to, Spanish.	Core	Spare is offered in many languages including English, Spanish, French, German, Catalan, Icelandic, Japanese, Norwegian (Bokmal), and Swedish.
4.a-8	The Mobile Applications are intuitive, easy to use, and meet relevant accessibility standards of the ADA, World Wide Web Consortium.	Core	Spare is intuitive, easy to use and navigate. Spare follows all relevant accessibility standards of the ADA and World Wide Web Consortium.
4.a-9	The system's Mobile Applications are integrated with the DROs' fare structures and reservations systems to allow the customer to indicate their payment preference when making a reservation (e.g., cash, payment card, etc.).	Core	Through our Open API, Spare safely outsources payments to our partner Stripe, a certified PCI Level 1 Service Provider that is well known and used around the world. An electronic purchase solution, Stripe supports a variety of payment processors and gateways including but not limited to all major credit cards, debit payments, Paypal, Google Pay etc. Additionally, our open API allows us to partner with any payment solution chosen by the DRO, as long as that solution has an Open API into which we can integrate.
4.a-12	The system's Mobile Applications allows customers to view the vehicle's location and estimated pickup (arrival) time on a map-based interface.	Advanced	The Spare Rider app displays the current location of the vehicle on the map, as well as estimated pickup time on a map-based interface.

b. Customer Website

ID	Specifications	Feature	Spare's Response
4.b-1	The self-service Customer Website supports the following functions: 1. Apply for demand response eligibility 2. Create an account 3. Link Client ID 4. Manage account (payment, contact information, personal care attendant, emergency contact and frequent address of travel) 5. View scheduled trips 6. Book a trip 7. Modify a trip 8. Cancel one or many trip reservations.	Core	Yes, Spare has a fully functional client website called Spare Rider Web Booker which complements the functions of the mobile application and includes the following features: 1. Apply for demand response eligibility: Fully automated web form to apply for eligibility via Spare Engage. 2. Create an account 3. Link Client ID 4. Manage account (payment, contact information, personal care attendant, emergency contact and frequent address of travel) 5. View scheduled trips 6. Book a trip 7. Modify a trip 8. Cancel one or many trip reservations.
4.b-2	The Customer Website is compatible with Windows and Apple operating systems and support the current browser version in addition to the previous three (3) versions. The Customer Website Portal functions on a desktop device (such as a PC), tablet, and wireless smartphone using popular browsers, including but not limited to: Chrome, Edge, Internet Explorer, Firefox, and Safari.	Core	The Spare Rider Web Booker is compatible with all current browsers and supports the previous browser versions. Spare's web Booker can function on a desktop device (such as a PC), tablet, and wireless smartphone using popular browsers, including but not limited to: Chrome, Edge, Internet Explorer, Firefox and Safari.
4.b-3	The Customer Website supports shared permissions allowing personal care attendants or caregivers to manage customer profile, book a trip, modify a trip, and/or cancel a trip.	Core	The Spare Rider Web Booker enables a third party, such as a personal care attendant or caregiver, to have access to the rider's profile with the rider's credentials. This will allow them to apply for demand response eligibility (register a new client), manage customer profile, book a trip, modify a trip or cancel a trip on the rider's behalf.
4.b-4	The Customer Website adheres to the branding guidelines of the DROs and will be approved during FDR.	Core	Spare allows DROs to white-label the rider application and also create a custom branded portal, including a unique web address reflecting the service/system as being provided by the DRO. The portal and app will adhere to the DRO's branding guidelines, which will be approved during Final Design Review (FDR).
4.b-5	The Customer Website displays text in alternate languages	Core	Spare is offered in many languages including English, Spanish, French, German, Catalan, Icelandic, Japanese, Norwegian (Bokmal), and Swedish.

	including, but not limited to, Spanish.		
4.b-6	The Customer Website is intuitive, easy to use, and meet ADA accessibility standards.	Core	Spare is intuitive, easy to use and navigate. Spare follows all relevant accessibility standards of the ADA and World Wide Web Consortium.
4.b-7	The Customer Website allows customers to view the vehicle's location and estimated pickup (arrival) time on a map-based interface.	Advanced	The Spare mobile applications and web booker enables riders to view the vehicle's location and estimated pickup (arrival) time on a map-based interface. All Spare systems are synced so a rider will be able to book on one method, such as over the phone, and monitor the trip via the mobile app and web booker.

c. Phone Notification

ID	Specifications	Feature	Spare's Response
4.c-1	The system interfaces with an interactive voice response (IVR) system to provide customer alerts related to trip reminder and real-time arrival information.	Core	Spare has voice notifications for those who call in on a landline or for those without text or push notifications. Meaning that 60 minutes before a ride, those who are not able to receive push or text messages will receive an automated phone call reminding them of their upcoming trip and provide more information such as vehicle, license, ETA, or other information the agency would like to convey. The rider will also receive an automated phone call 5 minutes prior to the vehicle arriving, so they can continue with their day until they are notified and don't have to block off significant time not knowing when their vehicle will arrive. Through our Open API, we can also integrate with other IVR solutions, such as Unified Dispatch, if additional capabilities are desired, such as trip booking, cancellations, etc.
4.c-2	The system provides the name of the DRO and welcome message as its first response when the IVR is initialized. The system allows additional messages to be spoken after the welcome message as part of the IVR-decision flow.	Core	Yes, the IVR message is customizable and will provide the name of the DRO when first spoken. Additional messages can be spoken as part of the IVR call flow.
4.c-3	The system allows users to interact with the system using their voice or telephone keypad.	Core	Yes, keypad inputs are allowed as part of the IVR process for actions such as cancellation, confirmation etc.
4.c-4	The system supports a skip-ahead feature that allows the customer to choose their option at any point.	Core	Yes, skip ahead feature may be included in the IVR if required.
4.c-5	The system supports a time-out parameter when no voice or	Core	Yes, a time out parameter can be included if required.

	no-keypad tone is identified, the customer is transferred to a Customer Service Representative. The time-out parameter will be approved by the DROs.		
4.c-6	The system supports languages including, but not limited to, English and Spanish.	Core	Yes, both English and Spanish can be supported with the user having a choice of preferred language. More languages may be added in the future.
4.c-7	The system supports incoming calls through an automated menu where customers are encouraged to use an automated menu as a first choice before being transferred to a Customer Service Representative.	Core	Yes, an automated menu would be presented first and if the call has to be escalated, it would be transferred to a Customer Service Representative.
4.c-8	The Vendor provides a list of IVR recordings and prompts to the DRO for review and approval prior to implementation. The system permits DROs to customize system prompts and customer information messages at no charge.	Core	Spare will work with the DROs to review recordings. The IVR will include the ability to customize recordings at no extra charge.
4.c-9	In addition to customer alerts, the system supports messages related to eligibility requirements, usage policies and important contact information specific to the DROs.	Core	Any custom message relating to eligibility requirements, usage policies and contact information can be recorded in the IVR system.
4.c-10	The system allows prompts to the customer to identify a trip reservation, cancel one or many reservations, and confirm the cancellations.	Core	Yes, through advanced IVR functionality, Spare is able to provide trip reservation, cancellation and confirm time etc.
4.c-11	The system is configurable and allows the DROs to configure the reminder and arrival parameters. The DROs will define these parameters during initial implementation.	Core	Arrival and reminder notifications are completely configurable.
4.c-12	The system contacts the customer with a reminder call about their trip the day before their scheduled service.	Core	Automatic phone call notifications can be scheduled a day before service.
4.c-12	The system contacts the customer the day of their service trip with a service reminder when the vehicle is fifteen (15) minutes away from arrival.	Core	A vehicle arriving notification can be sent 15 minutes prior to vehicle arriving.

5. Reporting

a. General Reporting

ID	Specifications	Feature	Spare's Response
5.a-1	The system includes a reporting module that meets all National Transit Database and Federal Transit Administration reporting requirements and allows for the quick analysis of performance and service metrics such as: 1. Overall system report 2. Service hours and miles (revenue and non revenue) 3. Deadhead hours and miles 4. No-Shows/Cancellations 5. Ridership and passenger hours 6. Client Management (e.g., new clients, suspended clients, etc.) 7. On-time performance 8. Trips and Trip origins and destinations 9. Billing and Invoicing 10. Taxi and Brokered services report 11. System Performance Monitoring 12. National Transit Database (NTD) 13. The standard North Carolina reporting package, including operating statistics, origin destination data, and vehicle utilization.	Core	Spare Analyze is Spare's reporting model. Spare Analyze has common reports built in and the data can be filtered to create custom reports. Spare Analyze collects all data required for North Carolina Reporting Package. Data for Operating Statistics, Vehicle Utilization, and Origin-Destination can be filtered to create custom reports. Metrics include all of the following requested by NCDOT: 1. Overall system report 2. Service hours and miles (revenue and non revenue) 3. Deadhead hours and miles 4. No-Shows/Cancellations 5. Ridership and passenger hours 6. Client Management (e.g., new clients, suspended clients, etc.) 7. On-time performance 8. Trips and Trip origins and destinations 9. Billing and Invoicing 10. Taxi and Brokered services report 11. System Performance Monitoring 12. National Transit Database (NTD) 13. The standard North Carolina reporting package, including operating statistics, origin destination data, and vehicle utilization.
5.a-2	The system supports reporting analyses through ad hoc report generation. The system includes at least the following: 1. A display of the number of passengers per vehicle for a user-specified time interval 2. The number of cancellations, no-shows and late pick ups for a given rider for a user specified data range 3. A query of trips by vehicle ID, rider ID, rider name, location name, zone, city, type of trip (e.g., ambulatory, subscription,	Core	Spare Analyze is our reporting and analytics tool, developed to report on the performance of the DRO's Spare-powered service. Analyze offers ability to generate custom report with unique filters including: 1. Number of Passengers Per Vehicle and PPVH by custom time interval. 2. Number of cancellations, no-shows and late pick ups for a given rider for a user specified data range. This information is also visible in the rider profile. 3. All of the history of trips can be extracted including queries by vehicle ID, rider ID, rider name, location name, zone, city, type of travel etc. DROs will be able to make informed, quantitatively-based decisions on the new service as well as generate reports for the National Transit

	canceled), travel duration, travel time interval, etc.		Database (NTD). All services in Spare Platform are tracked, monitored, analyzed, and presented in the Spare Analyze dashboard. Easily available KPIs include on-time performance, demand summary, trip data, ridership data, revenue per service hour, and more. Using Analyze, DROs can simply pull reports in Excel format, including a ridership, driver, and NTD reports. Spare Analyze offers full oversight into your operations in just a few clicks.
5.a-3	The system runs reports based on service type (e.g. Demand response or Shuttle Van) and service days (weekday, Saturday, or Sunday) is required.	Core	The data on Spare Analyze can be filtered to create reports based on service type and service days.
5.a-4	The Reporting System first presents data in a summary format and then allows the DRO staff to drill-down and drill-through the tables for further details. Any graphical illustrations are provided as necessary.	Core	Yes, the reporting system can be built with drill down and drill through features. Graphs such as bar charts and trend lines are included as graphical displays of data.
5.a-5	The system runs custom reports using any of the data elements included in the database. Custom reports are intuitive and require minimal user configuration.	Core	Custom reports created with Spare Analyze are intuitive and require minimal user configuration.
5.a-6	The system provides the DROs and the State with access to both aggregated and non-aggregated raw data for research and reporting.	Core	Spare Analyze provides access to aggregated and non-aggregated raw data for research and reporting.
5.a-7	The system allows users to generate and save ad hoc reports easily.	Core	Spare Analyze support reporting analyses through ad hoc report generation.
5.a-8	The system allows reports to be viewed on screen, sent to a printer or saved to a file.	Core	DROs staff can view reports on screen, download via CSV and Excel files, print, export and save reports. Which can then be shared with the State.
5.a-9	The Reporting System allows report files to be exportable as pdf, Word, Excel, and GIS data formats. Origin and destination reports shall export location addresses as well as geocoded coordinates.	Core	Spare Analyze can export reports as an Excel or CSV file which can then be converted as needed to other formats. Origin-destination information is stored as addresses and geocoordinates.
5.a-10	The Vendor provides the DROs with a list of available reports, sample of detail reports and degree to which the reports can be customized.	Core	DROs staff can filter the data on Spare Analyze to generate and run pre- built template reports and custom/ ad-hoc reports.

5.a-11	The Reporting System provides standard reports based on stored data. The DROs prefer the standard reports provide at least the following features: 1. Log on/ Log off Summary 2. Trips Provided 3. Non-Revenue vehicle hours 4. Passenger travel time by run, trip and user group 5. Cancellations 6. No-shows 7. Vehicle hours/miles 8. Driver attributes (DL endorsement, expiration, certification).	Core	Yes, through custom fields, Spare is able to generate reports based on the following data points: 1. Log on/ Log off Summary 2. Trips Provided 3. Non-Revenue vehicle hours 4. Passenger travel time by run, trip and user group 5. Cancellations 6. No-shows 7. Vehicle hours/miles 8. Driver attributes (DL endorsement, expiration, certification).
5.a-12	The Reporting System accesses the database to allow technical staff to generate, create and save ad hoc reports.	Core	DROs staff can filter the data on Spare Analyze to generate and run pre- built template reports and custom/ ad-hoc reports.

b. Performance Monitoring and Analytics

ID	Specifications	Feature	Spare's Response
5.b-1	The Vendor creates canned reports that can be run, viewed, and downloaded by the DROs using a Vendor-provided Reporting System.	Core	Spare Analyze is the Spare Platform reporting and analytics module. It provides a dashboard that shows key service and fleet KPIs and reports that are exportable. Spare provides both canned reports and ad-hoc reporting capability.
5.b-2	The system generates reports without manual data entry by the Vendor wherever possible.	Core	Spare Analyze enables DROs to generate reports without manual data entry by the vendor.
5.b-3	The reports include tables and graphical charts showing the current and historical performance of each device or feature of the system under measurement where applicable.	Core	Spare Analyze, Spare's reporting module outlining all key KPI's for the service, is data that can be viewed in graphs or fully exported in a tabular, .csv or .xls format within the admin dashboard. All services in Spare Platform are tracked, monitored, analyzed, and presented in the Spare Analyze dashboard.
5.b-4	The reports include a calculation of any credits to be assessed in the current month based on current and prior performance.	Core	Spare's performance reports will include a calculation of any credits to be assessed in the current month based on current and prior performance.
5.b-5	The Vendor commences performance reporting during Pilot Testing and continues to perform this activity throughout the operations agreements.	Core	Spare will commence performance reporting during Pilot Testing and continue to perform regular analysis throughout the operation to ascertain success of the service. Spare also engages with each DRO to do Quarterly Goal Reviews to ensure that we are meeting with performance targets.

5.b-6	The system provides data and reports in a consistent format (e.g., CSV or equivalent spreadsheet format) and structure to support status reporting for active projects/contracts across participating DROs.	Core	Spare Analyze is our reporting and analytics tool, developed to report on the performance of the Spare-powered service. DROs will be able to make informed, quantitatively-based decisions on the new service as well as generate reports for the National Transit Database (NTD). All services in Spare Platform are tracked, monitored, analyzed, and presented in the Spare Analyze dashboard. Easily available KPIs include on-time performance, demand summary, trip data, ridership data, revenue per service hour, and more. Using Analyze, DROs can simply pull reports in Excel format, including a ridership, driver, and NTD reports. The reports can be saved as a .CSV file and easily shared with the necessary parties for project status reporting.

6. Implementation

a. System Design Reviews

ID	Specifications	Feature	Spare's Response
6.a-1	The Vendor prepares a comprehensive System Design/Configuration set of documents (SDD) describing the functionality, user interfaces, network and system interfaces, and other elements to fully describe the system.	Core	Spare will provide a complete system design and infrastructure diagram which will be included in initial proposal submission.
6.a-2	The SDD includes at a minimum: 1. System overview, architecture, and configuration information 2. All onboard and system software and functionality 3. All system interfaces, including data communications and interfaces with other systems 4. All system configurations for all of the participating DROs 5. Performance measures and overall testing and acceptance process.	Core	The SDD will be comprehensive and include all of the specified components including: 1. System overview, architecture, and configuration information 2. All onboard and system software and functionality 3. All system interfaces, including data communications and interfaces with other systems 4. All system configurations for all of the participating DROs 5. Performance measures and overall testing and acceptance process.
6.a-3	The Vendor presents the design documents and related information in initial implementation meetings. The Vendor facilitates a general demonstration of the system	Core	A complete system design and configuration process will be undertaken by Spare with each DRO. A detailed implementation plan will be discussed specific to each DROs requirements.

	identifying each application or module provided under this Contract. The Vendor clearly articulates to the DROs the decisions required to configure the system or design elements of the system.		
6.a-4	Design review meetings will be held at DRO offices or using approved video conferencing tools and will include an overall System Design Review meeting, followed by detailed reviews for each application or module provided by the Vendor. This includes: 1. Client Management 2. Reservations and Scheduling 3. Dispatching and operations 4. Fare payment 5. Customer applications (e.g., mobile app, phone, website) 6. On-demand services 7. Reporting 8. Integrations 9. Hardware (e.g., mobile data terminal (MDT) or tablets) 10. System support and maintenance.	Core	Spare has specific modules for each system component and Spare will ensure that each of the modules is discussed with DROs. These would be include: 1. Client Management 2. Reservations and Scheduling 3. Dispatching and operations 4. Fare payment 5. Customer applications (e.g., mobile app, phone, website) 6. On-demand services 7. Reporting 8. Integrations 9. Hardware (e.g., mobile data terminal (MDT) or tablets) 10. System support and maintenance.
6.a-5	The Vendor conducts interactive workshops using demonstration equipment to “walk through” system operation and develop the screens for all user interfaces.	Core	Yes, as a software, Spare believes in our product and follows a testing procedure that includes internal and beta testing. We are problem solvers and we strive to build the best product to suit DROs’ needs. There are milestones and tasks for testing as part of our implementation plan. Following is a walkthrough of our procedures for integrations, system acceptance, and operability performance testing.
6.a-6	The Vendor conducts interactive workshops to demonstrate the system operation's final design, including final screens for user interfaces and customer facing applications.	Core	As a software, Spare believes in our product and follows a testing procedure that includes internal and beta testing. We are problem solvers and we strive to build the best product to suit DROs’ needs. There are milestones and tasks for testing as part of our implementation plan. Following is a walkthrough of our procedures for integrations, system acceptance, and operability performance testing.
6.a-7	If preferred by the DRO, the Vendor conducts a series of design meetings with the DROs throughout the project implementation rather than conduct the initial	Core	Most of the service planning and design will be done in the early phases of the implementation. However, this doesn’t mean that this is the end of the service design and refinements will continue as the project progresses. Throughout the implementation, the DRO can bring up their service design questions to Spare at

	implementation meetings. If this is the preferred method, the Vendor must clearly describe the alternative process in the proposal.		any time ad hoc or during the designated meetings and we will be ready to answer and assist the DROs.

b. Testing

ID	Specifications	Feature	Spare's Response
6.b-1	The Vendor provides all labor and materials required for system testing, including but not limited to multiple phone types and sizes across iOS and Android platforms, funding sources, and all support services and facilities required to test the system.	Core	Spare will provide all necessary hardware and software necessary to run the service including phone and testing services.
6.b-2	The Vendor prepares and submits a comprehensive testing plan for review and approval by the DROs.	Core	Yes, a comprehensive testing plan will be available for review and approval by the DROs.
6.b-3	The Vendor documents all tests. The DOR and the Vendor will monitor and sign off to indicate completion of the tests.	Core	Yes, all tests are documented and sign off is required to ensure completion of the tests.
6.b-4	The Vendor provides a comprehensive set of test use cases and testing scripts for the DROs to use to test the system. Testing includes: 1. All features and functions provided under this Contract, configured for the Agencies as determined during design review 2. Testing setup/pre-conditions, step by step instructions to complete the test and expected results for each test 3. Test success/acceptance criteria The Vendor generates sufficient data to thoroughly test the reports provided under this Contract for reporting testing.	Core	Yes, Spare will provide testing use cases and testing scripts for the following: 1. All features and functions provided under this Contract, configured for the Agencies as determined during design review 2. Testing setup/pre-conditions, step by step instructions to complete the test and expected results for each test 3. Sufficient data to thoroughly test the reports provided under this Contract for reporting testing.
6.b-5	The Vendor provides the testing use cases to the DROs no later than two (2) weeks prior to the start of testing for review and approval.	Core	Yes, Spare will provide testing use cases no later than 2 weeks prior to start of testing for review and approval.
6.b-6	The Vendor corrects any and all software not passing inspection or testing and retests it at no additional cost to the DRO.	Core	Yes, no additional costs will be charged for fixing issues found during testing.
6.b-7	The DRO may, at its discretion, assign a DRO representative to witness and or/audit all testing.	Core	Yes, the DRO may assign a representative to witness and audit all testing.
6.b-8	Prior to the start of any formal testing, the Vendor conducts a "dry-run" review and testing of software components to identify and resolve any issues that arise.	Core	Yes, prior to the start of any formal testing, Spare conducts a "dry-run" review and testing of software

			components to identify and resolve any issues that arise.
6.b-9	The Vendor provides a test environment for the system to fully test all features and functions provided under this Contract. The testing environment will be separate from the development and production environments.	Core	Yes, the test environment is fully separated from the production and development environment and can fully test all features.
6.b-10	The Vendor facilitates and leads three (3) stages of testing: 1. Functional Testing 2. Pilot Testing or Public Beta Testing 3. System Acceptance Testing (SAT).	Core	Yes, Spare provides all three stages of testing: 1. Functional Testing 2. Pilot Testing or Public Beta Testing 3. System Acceptance Testing (SAT)
6.b-11	Successful completion of each of the three (3) testing stages will be subject to the approval of the DROs based on the test criteria mentioned in specification 6.2-10.	Core	Yes, all testing stages may be approved by the DRO.
6.b-12	Functional Testing includes comprehensive testing of the system as configured for the DROs. Testing is conducted on all components provided under this Contract. The Vendor completes functional tests for the application which demonstrate and verify all functions provided as part of this Contract, including the review and usability testing of all user-accessible screens and commands.	Core	Functional testing includes comprehensive testing of the system as configured by the DRO.
6.b-13	After Functional Testing is successfully completed, Vendor provides a Functional Testing report to the DROs for review and approval before the Vendor proceeds to the next stage of testing.	Core	After Functional Testing is successfully completed, Spare will provide a Functional Testing report to the DROs for review and approval before Spare proceeds to the next stage of testing.
6.b-14	For DROs conducting optional Public Beta Testing, the Vendor facilitates Public Beta Testing of the Mobile App and supports all public beta testers including, but not limited to: 2. Support beta testers through the testing phase 3. Summary of issues identified by beta testers 4. Readiness report for Go-Live.	Core	A public beta testing would be supported by Spare. This may include focus groups, live sessions etc.
6.b-15	The Vendor provides a minimum of one (1) week onsite support during public launch.	Core	Yes, Spare will provide one week onsite support during public launch.
6.b-16	SAT begins after full public launch of the complete solution for all system components and will continue for 45 days.	Core	Spare agrees to these terms.
6.b-17	SAT is performed in the production environment with all features and functions provided under this Contract.	Core	Spare agrees to these terms.

6.b-18	The Vendor supports all elements of SAT, including, but not limited to, system maintenance, reporting, and customer support.	Core	Spare agrees to these terms.
6.b-19	If the applicable performance requirements defined in agreed SLA are not attained during the 45-day period, the SAT is extended a minimum of 90-days to allow for three consecutive 30-day periods in which the requirements are met.	Core	Spare agrees to these terms.
6.b-20	The Vendor identifies and implements remedial action at no cost to the DRO if an applicable system component fails to conform to specifications or performance requirements during SAT.	Core	Spare agrees to these terms.
6.b-21	During SAT, the DRO and the Vendor meet no less than two (2) times per week to discuss progress, issues, and results. The Vendor provides formal reports on system performance at the end of the 45-day period.	Core	Spare agrees to these terms.
6.b-22	The Vendor provides all testing data, reports, and other testing information to the DROs for review and approval within 10 days following the Completion of SAT.	Core	Spare agrees to these terms.
6.b-23	The Vendor is responsible for all system operation and maintenance until the DROs issue approval of SAT.	Core	Spare agrees to these terms.

c. Training and Manuals

ID	Specifications	Feature	Spare's Response
6.c-1	The Vendor offers comprehensive onsite training to the DROs' staff on all provided hardware and software. Digital copies of user manuals, training materials, and all other system documentation will be made available to the DROs.	Core	Comprehensive training reference materials are available for all training modules. These resources help strengthen the DROs' knowledge of the Spare Platform and include recorded training sessions, help articles (FAQ), training videos, and user guides in PDF format. Spare is committed to providing the training materials our customer stakeholders need to be successful in their new workflows.
6.c-2	The Vendor provides all training materials in either Microsoft Office or Adobe PDF and shall provide permission to the DROs to reproduce copies as needed.	Core	Spare can provide the training materials in whatever format the DRO prefers. The DROs can reproduce the copies as needed.
6.c-3	The Vendor keeps all training materials current based on current modifications and releases. The	Core	Spare will keep the training materials up to date and will be tracked on the training manuals.

	date and version shall be tracked on all training manuals.		
6.c-3	The Vendor provides training courses for at least the following positions: 1. Scheduler 2. Dispatcher 3. Administrative Staff 4. DRO Training Instructors (Train the Trainer) 5. DROs 6. Customer Service Representatives 7. Transportation Supervisors and Managers 8. System Administrator/System Engineer (IT Staff) 9. Database Administrator (IT Staff).	Core	Spare approaches all training with a train-the-trainer approach that will be customized to the DROs' needs. Led by the Spare Project Manager, all training is delivered either virtually or in-person. Across our services, we've found that virtual sessions complemented by our training material and resources have worked well for our partners. Training sessions take place over one or two hours depending on the module. Properly training staff is one of the most—if not the most critical part—of new technology implementation. This is why Spare has a comprehensive training program that includes five in-depth training modules tailored to Administrators, Dispatchers/Schedulers, Drivers, Booking Agents, and Data Analysts. These five modules will provide the training for the nine positions mentioned. These training modules are accompanied with a range of resources and reading materials, to equip the DROs' leaders, team members, and end users across the executive, operations, customer service, and IT/business intelligence teams with the know-how to confidently interact with Spare's software. The detailed training will also increase their knowledge of the platform in order to train others themselves. MODULE 1: Administrator User Profile: Management, Administrator, Service Planner, IT staff The administrator module provides the holistic knowledge to successfully launch the DROs service with Spare. This module focuses on the platform's setup and planning features customized to the DROs objectives. A general overview of the platform's various features and functionalities gives administrators, planners, and management a robust understanding of the platform's capabilities and possibilities. Key skills include: ✓ Live map and dashboards ✓ Creating and configure a new service ✓ Setting up fares and payments ✓ Setting up dedicated and non-dedicated fleets ✓ Enable rider notifications ✓ Set up and restrict user permissions ✓ Scheduling and managing driver duties ✓ Managing rider and driver profiles ✓ Managing vehicles ✓ Data, analytics, and reporting MODULE 2: Dispatcher/Scheduler User Profile: Management, Dispatcher, Scheduler

		The dispatcher module provides an overview of managing the daily operations and dealing with specific scenarios and procedures. All of the features of Spare Launch are explained, including duty scheduling, driver management, dealing with and moving trips, real-time operations monitoring, as well as how to conduct data analysis, do deep dives, and create custom reports. Key still include: ✓ Live map ✓ Creating dashboards ✓ Creating and duplicating driver duties ✓ Driver schedule optimization ✓ Managing driver duties and exceptions ✓ Rematching and managing trip requests ✓ Diagnosing operational problems ✓ Standard operating procedures and workflows ✓ Out-of-service vehicle procedures ✓ Setting up admin notifications ✓ Setting up driver break policies MODULE 3: Driver User Profile: Dispatcher, Driver The driver module empowers operators (dedicated/non-dedicated) to use the Spare Driver App to pick up and drop off passengers. Several drivers, along with the trainer in-training, can be trained simultaneously during one training session. After a satisfactory level of training has been performed, the Spare Project Manager will organize a full system dry-run with the driver(s), simulating foreseen and unforeseen situations, to test driver readiness. Key skills include: ✓ Starting and ending a duty ✓ Performing pickups and dropoffs ✓ Reading trip information ✓ Trip navigation ✓ Dealing with no-shows and cancellations ✓ Hands-free notification and communication handling ✓ Emergency response management ✓ Exceptions handling and troubleshooting ✓ Managing “flag-down” trips (if applicable) MODULE 4: Booking Agents User Profile: Booking Agents, Dispatcher The booking agent module provides customer service representatives with an overview of how to manage trip requests and rider profiles with shortcuts to reduce booking call times. Training includes demonstrative and interactive components. After training is complete, booking agents and dispatchers gain access to the configured testing and training environment so that they can practice their new

			workflows ahead of dry run testing and go-live. Key skills include: ✓ Live map and dashboards ✓ Creating and managing rider profiles ✓ Creating and managing trips ✓ Creating and managing subscription trips ✓ Rider payments and Spare Pay IVR ✓ Rider reviews and handling complaints ✓ Rider notifications ✓ Trip investigations and analysis ✓ Exceptions handling and troubleshooting MODULE 5: Data Analyst User Profile: Data analysts, reporting staff, IT/systems personnel, administrators The data analyst module includes reviewing all metrics, data, reports, and charts in Spare Analyze. Information on how data is collected and how metrics are calculated and represented is explained. Training on how to interpret the data, use the data, perform analysis of the data, and develop insights from the data is given. Insights as to what impacts each metric and what levers can be pulled, in the software and operationally, to affect each metric are explained. Key skills include: ✓ Review and define KPIs in: - Service analytics - Fleet analytics - Service reports - Fleet reports ✓ Discuss KPIs and how they relate to the DROs service goals ✓ Discuss what KPIs to track and set quantitative objectives (if not already set) ✓ Discuss how KPIs relate to one another, DROs service configuration, and DROs operational processes ✓ Discuss any specific reporting needs (regulatory or otherwise)
6.c-4	The DROs will provide employee list and number of staff attending above training sessions during Training Plan review.	Core	Spare agrees with this term.
6.c-5	The Vendor conducts training prior to Pilot Testing for the selected employees participating in Pilot Testing. All DROs must be trained before SAT.	Core	Spare agrees with this term.
6.c-6	The Vendor provides additional training and updated training materials to the DROs prior to SAT	Core	Spare agrees with this term and will provide additional training.

	at no additional cost under the following circumstances: 1. If major modifications are made to the system after the initial training due to system upgrades or changes made under warranty or 2. If SAT occurs at least six (6) months after the completion of training, due to delays for which the Vendor is responsible.		
6.c-7	During the System Maintenance Agreement (SMA) period, the Vendor provides additional training to DRO staff at no additional cost. Additional training may include pre-recorded sessions, however, live support from the Vendor is provided to answer any follow up questions from trainees.	Core	Spare agrees with this term.
6.c-8	The Vendor provides an online-based training module (on-demand version) that is built into the base system and allows for future training of the DROs.	Core	Spare's training will be recorded and will be available for the DRO to refer back to at any point. As well, with the train-the-trainer method, further training of additional personnel can be completed.
6.c-9	The Vendor provides a Training Plan, including objectives, schedule, and course outline to the DROs for review at least four (4) weeks in advance of the start of training. The Training Plan shall include: 1. Total number of onsite training session(s) proposed 2. Total number of web-based training session(s) proposed 3. List of training course(s) 4. Number of classes per course 5. Maximum number of attendees per class 6. Preferred day and duration of sessions.	Core	The assigned Spare Project Manager will work with the DRO to set out a training plan that is customized to the specific DRO. This training plan will be agreed upon and approved by the DRO and included the six elements mentioned.
6.c-10	The Training Plan shall be approved by the DROs prior to the start of any trainings.	Core	The Training Plan will be discussed and approved by the DROs prior to the start of training.
6.c-11	The Vendor furnishes all tools, equipment, and training aids to conduct training courses during the training course.	Core	Spare will provide the DRO all the necessary items to conduct the training.

6.c-12	The Vendor provides an instructor with a thorough knowledge and understanding of the system. In addition, the instructor has a familiarity within transit and will effectively leads students in a classroom setting.	Core	The Spare Project Manager assigned to the DRO will act as the instructor during the training. Spare's Project Managers are experts in the Spare Platform and have provided training on implementations of all sizes, much like the DROs.

7. Ongoing System Operations and Maintenance

a. System Maintenance Agreement (SMA)

ID	Specifications	Feature	Spare's Response
7.a-1	Provide a SMA that covers the operations and maintenance of the system for a period of two (2) years plus three (3) one- (1-) year options for a total of five (5) years.	Core	Yes, Spare agrees to these terms.
7.a-2	During the SMA, the Vendor retains responsibility for the operations and maintenance of the services, applications and any hardware provided.	Core	Yes, Spare agrees to these terms.
7.a-3	The Vendor provides comprehensive testing during the SMA for any significant changes to the system. The determination of the significance of the change will be collaboratively determined between the Vendor and the DROs' representatives.	Core	Yes, Spare agrees to these terms.
7.a-4	The Vendor provides at least five (5) business days' notice to the DROs before deploying system updates to Production, except when critical updates require immediate action.	Core	Yes, Spare agrees to these terms.
7.a-5	The Vendor ensures the system is up to date with OS level security updates and patches.	Core	Yes, Spare agrees to these terms.
7.a-6	The Vendor implements Change Management Processes for software and application releases.	Core	Yes, Spare agrees to these terms.
7.a-7	The Vendor provides maintenance support when new OS versions are released and deployed to the system.	Core	Yes, the Spare Platform is regularly updated to current system specs.
7.a-8	The Vendor releases new versions of the Mobile Apps, including obtaining approval through app store deployment processes.	Core	Yes, Spare is fully responsible for making the rider and driver apps available via the app store.
7.a-9	The Vendor maintains the app store pages and metadata for the Mobile Apps and configuring the application for free downloadable.	Core	Yes, Spare maintains app store pages and metadata for mobile app in the app store.
7.a-10	The Vendor monitors the System for security threats and vulnerabilities and notifies the DROs immediately in the event of a suspected breach of the System for DROs, rider(s), or identified fraudulent use.	Core	Spare uses tools available within the Google Cloud platform to run vulnerability scans. External vulnerability scans are run on the

			production environment at least quarterly. Interior vulnerability scans are run against test environments which mirror production configurations. Any suspected breach will be notified to the DRO immediately.
7.a-11	The Vendor provides a phone number and e-mail account for the reporting of software defects or malfunctions, and system outages, 24-hours a day, 7-days a week.	Core	Yes, Spare will provide a phone number and email for reporting software defects on a 24/7 basis.
7.a-12	During the SMA, the Vendor responds to reports of system outages within 15-minutes of notification, 24-hours a day, 7-days a week. A fully qualified service representative arrives onsite within 24- hours after being contacted by the DROs if it is determined that a physical presence is needed to resolve the identified issue.	Core	Spare agrees to these terms.
7.a-13	During the SMA, the Vendor responds to a report of any software defect or malfunction within two (2) hours of notification. A fully qualified service representative arrives onsite within 24-hours after being contacted by the DROs if it is determined that a physical presence is needed to resolve the identified issue.	Core	Spare agrees to these terms.
7.a-14	The Vendor attempts to fix software problems impacting revenue collection within three (3) hours of being reported.	Core	Spare agrees to these terms.
7.a-15	If the software problem impacts revenue collection, and the repair will take longer than three (3) hours, the Vendor reports the cause of the problem as soon as it becomes evident and provides status reports at least every four (4) hours thereafter, until the problem is corrected, or a workaround is established.	Core	Spare agrees to these terms.
7.a-16	The Vendor submits to the DROs, no less than monthly, a notification of planned modifications and updates to the system, upgrade schedules, and a calendar of key dates for system changes for the coming three (3) months and beyond.	Core	Spare agrees to these terms.

b. Service Level Agreement (SLA) and Key Performance Indicators (KPIs)

ID	Specifications	Feature	Spare's Response
7.b-1	The system completes reports within five (5) minutes of initiating the generation or creation of a standard or ad-hoc report.	Core	An ad-hoc report will take less than 5 minutes to generate.

7.b-2	The maximum average response time for all dispatch functions averages less than twenty (20) seconds for up to twenty (20) active workstations using the hardware and software in the Specification.	Core	Spare will meet this performance requirement. Spare does not see any performance degradation with multiple booking stations and will easily scale to 20 workstations.
7.b-3	The system supports each DRO's rider base within the service area without any appreciable degradation of overall system performance.	Core	Yes, Spare is able to scale seamlessly and deliver thousands of trips a day with no degradation in service. We are able to do this today with services that have over 7000 trips a day.
7.b-4	The system schedules a full day's trips in less than thirty (30) minutes.	Core	Spare will run a full day's optimization in less than 30 minutes and continually optimize after that.
7.b-5	System accuracy is determined based on any incident where a device or backoffice-generated transaction is recorded incorrectly within the associated system. See below:	Core	Spare agrees to these terms.

c. Issue Resolution and Remedies

ID	Specifications	Feature	Spare's Response
7.c-1	The Vendor and the DRO will establish an Issue Resolution Team (IRT) for each participating DRO as part of the ongoing operations and maintenance. The IRT will be established prior to Pilot Testing/Public Beta Testing and evaluates the system and back-office issues throughout the term of the Contract.	Core	Each DRO will have their own dedicated Project Manager from Spare. They would be your point of contact for answering technical questions and operations support. Additionally, your support team—led by our Support Manager—complements your dedicated Project Manager to provide responsive and thorough support over email, chat and by live telephone. Spare will provide each DRO with a direct phone line for emergency questions and issues for further debugging. Your support management team is dedicated to delivering fast response times, averaging 10 minutes for email, chat or phone support.
7.c-2	The intent of the IRT is to create a clear and consistent process to settle disputes based on the requirements and facilitate resolution for issues related to the Vendor-provided system. The IRT will use best judgment to collaboratively address scenarios where the requirements are silent or unclear. If the IRT cannot resolve a decision or dispute collaboratively, the DRO representative will make the final and binding decisions for any dispute that remains open by the IRT after a period of 10 business days.	Core	Spare agrees to this term.

7.c-3	The IRT shall evaluate failures and determine the severity and remedies assessed against the monthly SMA payment.	Core	Spare agrees to this term.
7.c-4	At a minimum, critical failures shall include incidents that produce a major or substantial business impact or impact to normal operations, such as: 1. Non-trivial loss of revenue or expense 2. Significant negative customer experience 3. Limited or loss of access to a production application 4. System operation at a degraded level, such that normal business operations cannot be conducted 5. Application or system experiencing continual or repeated issues.	Core	Spare agrees to this term.
7.c-5	A credit to the DRO's monthly subscription service payment will be assessed for a failure to meet any KPIs identified as having an associated credit.	Core	A credit for a KPI not met will be applied as specified in the SLA.
7.c-6	A failure will result in the percentage in the "Credit Assessed" column being applied to the full amount of the operations payment identified in the "Payment Impacted" column for the month of measurement.	Core	Spare agrees to this term.
7.c-7	A failure to meet the same KPI for two (2) or more months in a row will constitute a persistent failure and result in a multiplier being applied to the credit percentage.	Core	Spare agrees to this term.
7.c-8	The credit multiplier will increase by a factor of one for each month that a KPI is not met (e.g., if a KPI is not met two (2) months in a row, the credit will be doubled in the second month; if a KPI is not met three (3) months in a row, the credit will be tripled in the third month).	Core	Spare agrees to this term.
7.c-9	Successfully meeting a KPI will end a persistent failure and reset the credit multiplier.	Core	Spare agrees to this term.
7.c-10	The total credit applied to an SMA payment will be capped at 25% of the full amount of that payment in a calendar month. Credits will not be carried over from month to month.	Core	Spare agrees to this term.
7.c-11	The Vendor reports on credits in the system performance reports and	Core	Spare agrees to this term.

	deducts credits directly from any invoices submitted to the DROs.		
7.c-12	System accuracy is determined based on any incident where a device or back office-generated transaction is recorded incorrectly within the associated system. See below the chart below for requirements and remedies for the devices.	Core	Spare agrees to this term.

8. Priced Options

a. Hardware (Option)

Hardware	Description
Ruggedized Tablets	Extremely portable solid state computing devices engineered from inception to work in extreme temperatures and other harsh conditions. Ruggedized tablets have a rugged shell and can withstand drops, jolts, etc. Tablets are characterized by a single touch screen input mechanism and may or may not include an attachable keyboard.
Integrated Payment Systems	Automates payment acceptance to accept credit card payments directly with the DROs existing software.
Closed-circuit Television (CCTV)	The use of video cameras to transmit a signal to a specific place on a limited set of monitors for surveillance and security purposes.
Peripheral Components	Must be able to attach to, work with, and be supported by, the Ruggedized Tablet Units, the Integrated Payment Systems, and the CCTV systems described elsewhere herein. Peripherals must be present with the general offerings of the manufacturer, and as such, normally available from the manufacturer represented. Peripherals considered within the scope of this contract are monitors, input devices (keyboards, mice), docking stations, memory, cases, etc.

b. Payment Hardware (Option)

ID	Specifications	Feature	Spare's Response
8.b-1	System accuracy is determined based on any incident where a device or back office-generated transaction is recorded incorrectly within the associated system. See below the chart below for requirements and remedies for the devices.	Option	Spare regularly works with PCI compliant payment processor Stripe and will be able to work with DROs to implement a safe and accurate payment system.

8.b-2	The Vendor reconciles refunds, chargebacks, and adjustments.	Option	Spare encourages DROs to work directly with Stripe for reconciliation and other adjustments.
8.b-3	The system secures transmission and storage of Personal Identifiable Information (PII) acquired and used by the system for payment integration and processing.	Option	Stripe is a PCI level 1 compliant payment processor.
8.b-4	Confidential and sensitive data is encrypted and transmitted securely throughout the system.	Option	Yes, all sensitive information is encrypted during transmission.
8.b-5	Customers may add, modify, and delete payment methods to their customer account.	Option	Yes, customers are able to add, modify and delete information.
8.b-6	Customers may utilize all major payment card brands (i.e., Visa, Mastercard, American Express, and Discover) to purchase fare. This includes the use of Transit Benefit credit/debit cards, pre-paid transit credit/debit cards, and payment cards issued for government-funded or sponsored funds for low-income riders to purchase fare.	Option	Yes, all major payment cards are accepted.
8.b-7	The Vendor prepares financial reports that include daily, weekly, monthly, quarterly, and annual sales and revenue for the DROs.	Option	Yes, detailed daily, weekly, monthly, quarterly, and annual sales and revenue reports will be generated by Spare.
8.b-8	The system allows for multiple funding sources per rider and at least one funding source per rider per trip. Describe how funding data are stored and how funding sources are selected or automatically applied to trips.	Option	Manual reporting is extremely tedious and time consuming. Therefore, eliminating manual reporting and the need to break down reporting from multiple funding sources are keys to success. Spare Analyze is our data analytics and reporting module that will empower DROs to grow their operation through real-time data. The following features of Analyze are relevant and beneficial to DROs: Tracking and Reporting by Funding Source. Funding source can easily be added in Analyze at the trip request level or as a full service on its own depending on volume of trips to be facilitated by the funding source. Reports can be generated by funding source and standard metrics such as number of requests and miles traveled. Rider type can also be tracked by funding sources. This data may be used to generate invoices by funding source. Spare's cloud-based platform is off-the-shelf ready. Instead of having to manually export a csv report off of a previous software like Routematch, DROs' administrators can directly view and download reports from Analyze, with the ability to customize

			and sort through data. If the DRO desires to leverage our advanced shared-ride commingling feature, DROs can also report on this across their services. Citibus in Lubbock, Texas is able to efficiently and effectively manage reporting for 7 different services running under a commingled setup. Each mile in Spare is tracked at the level of individual rider, thus the reporting for paratransit does not conflict with on-demand, as an example.

c. Onboard Hardware, Data Communications, and Installation (Option)

ID	Specifications	Feature	Spare's Response
8.c-1	The Vendor provides driver displays (tablets) and all associated mounting hardware, cables, and communications components. All Vendor provided equipment is consistent across the fleet, allows staff to easily swap equipment (including mounting hardware and devices), and includes adequate data communications.	Option	As Spare is a SaaS company, we do not provide hardware, but can source the hardware for the DROs at cost plus markup. If DRO already has devices, the Spare Platform can run on these devices as Spare is device agnostic. The DROs can use any off-the-shelf smartphone or tablet and the assignment of devices are at the discretion of the DRO.
8.c-2	Vendor installs all onboard equipment through close collaboration with the DRO.	Option	Spare does not install equipment as we are a software company, but we can provide the DRO recommendations based on our experience implementing services.
8.c-3	The driver display mount complies with US heavy duty vehicle Society of Automotive Engineers (SAE) J1455 standard.	Option	Not applicable to Spare, but we can provide recommendations.
8.c-4	The driver display is a ruggedized device suitable for operations in a transit environment.	Option	Not applicable to Spare, but we can provide recommendations.

d. On-Demand Trips (Option)

ID	Specifications	Feature	Spare's Response
8.d-1	The system supports on-demand scheduling, where trips can be requested the same day. On demand scheduling does not require advance reservation.	Option	Spare's software runs on-demand scheduling at the same time as demand response scheduling. Our on-demand ability is shown through Spare's first software partnership which was the most creative in the transit industry for its time. Spare integrated with DART's vendor Unwire, a Danish company and the front-end developer of the GoPass MaaS app. This integration enabled Dallas Area Rapid Transit's (DART's) award-winning microtransit service, GoLink, to connect with its fixed route train and bus services, winning the APTA Innovation

			Award in 2019. Since launching with four zones in January 2019, DART's on demand transit service has evolved to become one of the largest providers of on demand transit in North America, with 30,000+ rides per month across over 30 active services. Spare has continued to provide on-demand software solutions on four continents since then.
8.d-2	The system permits trip booking while transit personnel are on the phone with the customer. The System processes both subscription trips (standing-order) and demand response trips.	Option	With Spare Launch, DRO personnel can book trips with customers on the phone for any type of on-demand and/or demand response trip. Spare's time saving features include, but are not limited to: automatic checks to ensure that ride request meets eligibility, service zone, time rules and other requirements before confirmation; favorite locations to pre-fill pickup and drop-off address; one click edits to make any changes to ride booking; one click return, recurring and rebooking feature; and automatically populating accessibility needs like wheelchair, notes and other custom requirements for clients so booking agents do not need to fill them each time. Our transit agency partners regularly see 25% time savings after implementing Spare's software platform. During a recent visit to Twin Transit in Washington, we were told that when using Routematch they had planned to hire an additional full time dispatcher. By implementing Spare software, they no longer need that new hire thanks to the time saving functionality of our innovative solution. As well, Cheyenne Transit Program (CTP) replaced Paraplan's paratransit software with Spare and has seen a 50% reduction in time spent on calls when reserving trips due primarily to the intuitive nature of the system for the reservationists.
8.d-3	The system processes, schedules, and dispatches same day trip orders without the need for manual intervention from dispatch staff.	Option	Spare's ride assignment algorithm comes into play at many points in the ride lifecycle. This includes: at Initial Booking, during Hourly Optimizations (before duties become live), and during Live Optimizations (for duties currently in progress). During Initial Booking: • When initially booking a ride, depending on how the DRO has configured the service, they have two options: the system can either accept no matter what or accept only if there's enough room in the current driver schedule. • If they choose the accept only if there's enough room setup, Spare's algorithm will find an initial spot for the ride, at a specific time with a specific driver. While with the "accept first" setup, the ride will be acceptable and finding a spot for it will happen automatically, later. • Criteria for choosing the best spot for a ride is highly configurable. Example scenarios: • The DRO can configure acceptable pickup and dropoff flexibilities (e.g. if the rider wants 10:00am pickup, you can say any time from 9:45am - 10:15am is allowed based on ADA requirements). • They can configure how much detour is allowed (e.g. if a ride would take 20 mins driving directly, but we do other

			pickups/drop-offs in the interim taking 35 mins, that's 15 mins of detour). • They can configure boarding time for different types of riders and vehicles, traffic, service hours, service areas, and rules like "the first wheelchair on must be the last wheelchair off, as the vehicle is narrow and wheelchairs cannot exit out of order". • They can customize the tradeoffs the algorithm makes For example, weighing rider experience vs. system efficiency and weighing different elements of rider experience, like pickup lateness vs. amount of detour once onboard. Note: if the DRO has multiple fleets connected to a service, all of these criteria are evaluated for each fleet and the best fleet chosen (they can also set priorities between fleets to further customize this). During Hourly Optimizations (before duties/vehicles become live): As more bookings come in and cancellations occur, sometimes the initial schedules chosen at booking time are no longer the best schedules. Once an hour, Spare's algorithm will reorganize the schedules into an optimal schedule. This obeys the same rules and weightings described above for initial bookings. Note that this occurs regardless of whether the DRO choses the "find a spot for rides immediately" or "accept everything up front, find a spot later" configuration. During Live Optimizations – aka GOLD (for duties/vehicles currently in progress): When drivers are out on the road, they can fall behind due to worse than expected traffic, riders not being ready for pickups, etc. At the same time, other drivers will have spare time due to last minute cancellations, better than expected traffic, quicker than expected boardings, etc. Every 10 minutes, Spare's algorithm will automatically assess the service zone to see if the system can reorganize rides into more optimal configurations for live duties. For example, if driver A is falling behind, but driver B has a bit of slack in their schedule, Spare Engine's algorithm automatically offloads a future ride from driver A onto driver B, so that driver A can catch up, and driver B stays busy. As with the hourly optimizations, this follows all of the same rules and weightings you configured for initial bookings.
8.d-4	The system supports on-demand or scheduled trip orders through the mobile application and customer website.	Option	Free to download for any rider, the Spare Rider app is highly intuitive and adheres to level AA of the WCAG 2.1 guidelines to ensure digital accessibility for all people, including those with disabilities. With Spare, riders can book on-demand or scheduled trips with our user-friendly, free to download mobile Spare Rider app or Spare Rider Web booker for scheduled paratransit trips or their same day microtransit trips. Our Rider App and Rider Web Booker can be white-labeled and their interfaces are self-serve, easy to use, reliable, and convenient

			for riders to book a trip in real time, schedule a trip, or set a recurring trip all with a few clicks on a smartphone or strokes on a keyboard. The Spare Rider app and Spare Web booker, gives the customers all the information they need at their fingertips and reduces the burden on the call centers. A paratransit rider using the Spare Rider app said “Finally an app which enables a great deal of resources. Extremely helpful and much much much less phone calls to dispatch.”
8.d-5	The system differentiates between ADA and on-demand trips for reporting purposes.	Option	Spare Analyze is the Spare Platform reporting and analytics module. It provides a dashboard that shows key service and fleet KPIs and reports that are exportable. Reports and dashboards are filterable by service type and time.

e. Fixed Route Scheduling (Option)

ID	Specifications	Feature	Spare's Response
8.d-1	Describe in detail any fixed route and deviated fixed-route scheduling solutions supported by the solution, including: 1. Features and functions of the system 2. Customer facing tools such as real-time arrivals or trip planning 3. Integration with demand-response trip scheduling 4. Integration with other solution.	Option	The Spare Platform can operate in fully on-demand mode (with virtual stops or door to door), in semi-fixed mode (bookable but with pre-scheduled timetables), or it can recreate the operation of a fixed bus route, with or without the need to book rides. The platform allows mixed operations with the same fleet. During peak hours, a traditional fixed line service can be operated, and during periods of low demand, a bookable on-demand service can be run. Semi-fixed lines can also be configured thanks to Spare's flexible interface. This flexibility in the configuration is efficient where there are clear periods of high and low demand in the same area. Spare Routes is our option for running fixed lines that may or not require a booking. Routes allows fixed stops and fixed timetable when desired, in the same interface as the on-demand service. Spare's flexible fixed route feature allows the DRO to combine fixed route type service with demand response transportation, providing the opportunity to offer the riders the best of both worlds. Spare allows DROs to configure start times, slack time and automatically generates the route for such a service. Riders can book and track trips in a similar way as on-demand. However, the times for the vehicle are fixed as set by the DRO. Spare's software works so that there are enough seats available on the vehicle for booking similar to on-demand. The fixed route feature is available via the rider app, web booker and dispatch booking experience. Semi-Fixed Lines Similarly, DROs can configure semi-fixed routes in the Spare Platform by combining configuration parameters such as zone and stop type, direction, and time rules. They could configure an on-demand service that's constrained to a time table, but not to a specific route or destination. In both fixed and semi-fixed cases, a real on-demand service can be operated in parallel. Multimodal App

		Additionally, Spare has a multimodal white label rider app that provides information about conventional public transport lines and their connection with the on-demand services. Based on GTFS data, Spare's Rider app can suggest multimodal trips to users, allowing them to book the on-demand leg of the trip. We invite you to check the multimodal function in the fips App in Mannheim, and the DALLI app in Storkow, both in Germany.

f. CCTV (Option)

ID	Specifications	Feature	Spare's Response
8.f-1	Describe if the solution provides enhanced integrations with CCTV solutions. This includes the ability to trigger events from the driver display or dispatchers to either tag video recordings or allow dispatchers to view video directly from the dispatch screen.	Option	No, we do not integrate with CCTV solutions presently.
8.f-2	Describe CCTV systems that are included or offered from the scheduling software provider.	Option	Spare does not offer or include any CCTV systems.

9. Project Management Specifications

a. Project Deliverables Specifications

Reference	Deliverable Title	Spare's Response
Reference: PM 1	Project Management Documentation: A. Project Schedule and Approach B. Change Management Plan C. Engineering Change Requests D. QA/QC Plan E. Master Issues List (MIL) F. Transition Plan G. Design Review Plan H. Testing Plan I. Training Plan.	A: Spare's general schedule and approach can be found in the Schedule of Offered Solution section. B: Please see our 1.c-3 response regarding this item. C: Please see our 1.c-5 response regarding this item. D: See Appendix B for a template of our QA/QC Plan. E: See Appendix B for a template of our Risk and Mitigation Strategies Plan which is Spare's version of a MIL. F: See 1.c-14 for our transition plan. G: See the Phase 2: Service Planning/Modeling and Design Phase 3: System Setup and Data Provisioning description in the Schedule of Offered Solution section for our approach to the design review plan. H: See Appendix B for our testing plan. I: See our 6.c-3 response for our training plan.
Reference: PM 2	A. Design - Representative Examples System overview and architecture design document B. System design documents including all applications and	We have included our answer to A and B in the Architecture Diagrams section.

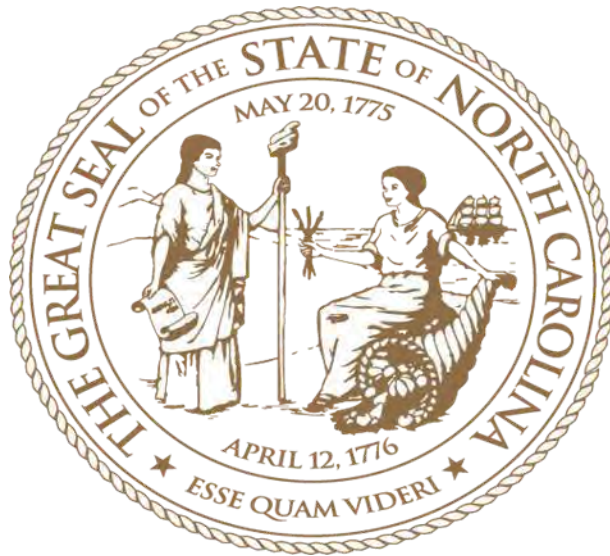
	integrations included as part of this Contract.	
Reference: PM 3	Testing: A. Comprehensive testing use-cases and scripts	See Appendix B for our testing plan.
Reference: PM 4	Training and Manuals: A. Comprehensive training materials for all solutions provided as part of this Contract B. Back-office system manual for all DRO and Vendor controlled configurations C. Mobile Application and Customer Website Design and Configuration Management Manual D. IVR phone tree and Design and Configuration Manual E. Driver Display Manual F. Reporting Manual G. Customer Service Guide	A and B: See Appendix B for our Booking Agent, Dispatcher and Engage guide which covers these items. C: See Appendix B for our Rider guide. D: See Appendix B for Twilio's documentation on the Securing payments with Twilio programmable voice. E: See Appendix B for our Driver guides for dedicated and non-dedicated operators. F: See Appendix B for our Spare Analyze reporting guide. G: See Appendix B for our Escalation Procedure guide which is our customer service guide.

Security Vendor Readiness Assessment Report (VRAR)

(a) Attached on the following page is the completed Vendor Readiness Assessment Report (VRAR) for Solutions Not Hosted on State Infrastructure.

(b) After the form completed for part a) is Spare's SOC 2 Type 2 report.

ENTERPRISE SECURITY & RISK MANAGEMENT OFFICE (ESRMO)



Vendor Readiness Assessment Report (VRAR) for Solutions Not Hosted on State Infrastructure

Executive Summary

The State of NC requires that all systems connected to the State Network or process State data, meet an acceptable level of security compliance. This includes those systems that operate outside of the States' direct control such as Cloud Services defined as Software as a Service (SaaS), Infrastructure as a Service (IaaS) or Platform as a Service (PaaS).

The State of NC has adopted the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 as the foundation for identifying and implementing information technology security controls. These controls are described in the State of NC Statewide Information Security Manual (SISM).

The following is a high-level view of specific security requirements that are needed to meet compliance. The control references (e.g., AC-2) refer to the specific NIST 800-53 control as listed in the SISM, which may be found at the following link:
<https://it.nc.gov/statewide-information-security-policies>.

Note: There may be additional requirements depending on the sensitivity of the data and other Federal and State mandates, or agency specific requirements.

Table of Contents

Executive Summary	i
1. Introduction	1
1.1. Purpose	1
1.2. Outcomes	1
1.3. State Approach and Use of This Document	1
2. VENDOR System Information	2
2.1. Relationship to Other Vendors or CSPs	2
2.2. Data Flow Diagrams	3
2.3. Separation Measures [AC-4, SC-2, SC-7]	3
2.4. System Interconnections	3
3. Capability Readiness	4
3.1. State Mandates	4
3.2. State Requirements	5
3.2.1. Data at Rest and Authentication [SC-13]	5
3.2.2. Transport Layer Security [NIST SP 800-52, Revision 2]	5
3.2.3. Identification and Authentication, Authorization, and Access Control	6
3.2.4. Audit, Alerting, Malware, and Incident Response	7
3.2.5. Contingency Planning and Disaster Recovery	8
3.2.6. Configuration and Risk Management	8
3.2.7. Data Center Security	10
3.2.8. Policies, Procedures, and Training	10
3.3. Additional Capability Information	13
3.3.1. Staffing Levels	13
3.3.2. Change Management Maturity	13
3.3.3. Vendor Dependencies and Agreements	13
3.3.4. Continuous Monitoring Capabilities	14
3.3.5. Status of System Security Plan (SSP)	15

List of Tables

Table 2-1. System Information	2
Table 2-2. Leveraged Systems	2
Table 2-3. Leveraged Services	2
Table 2-4. System Interconnections	3
Table 2-5. Interconnection Security Agreements (ISAs)	3
Table 3-1. State Mandates	4
Table 3-2a. Data at Rest & Authentication	5
Table 3-2b. Transport Encryption	5
Table 3-3. Transport Protocol	5
Table 3-4. Identification and Authentication, Authorization, and Access Control	6
Table 3-5. Audit, Alerting, Malware, and Incident Response	7
Table 3-6. Contingency Planning and Disaster Recovery	8
Table 3-7. Configuration and Risk Management	8
Table 3-8. Data Center Security	10
Table 3-9. Policies and Procedures	10
Table 3-10. Missing Policy and Procedure Elements	12
Table 3-11. Security Awareness Training	12
Table 3-12. Staffing Levels	13
Table 3-13. Change Management	13
Table 3-14. Vendor Dependencies and Agreements	13
Table 3-15. Vendor Dependency Details	14
Table 3-16. Formal Agreements Details	14
Table 3-17. Continuous Monitoring Capabilities	14
Table 3-18. Continuous Monitoring Capabilities – Additional Details	14
Table 3-19. Maturity of the System Security Plan	15
Table 3-20. Controls Designated “Not Applicable”	15
Table 3-21. Controls with an Alternative Implementation	15

1. Introduction

1.1. Purpose

This report and its underlying assessment are intended to enable State agencies to reach a state-ready decision for a specific system **not hosted** on the State of NC's infrastructure that is based on organizational processes and the security capabilities of the Moderate/Low-impact information system.

1.2. Outcomes

Submission of this report by the Vendor **does not guarantee** a state-ready designation, nor does it guarantee that the State will procure services from the vendor.

1.3. State Approach and Use of This Document

The VRAR identifies clear and objective security capability requirements, where possible, while also allowing for the presentation of more subjective information. The clear and objective requirements enable the vendor to concisely identify whether an application or vendor is achieving the most important State Moderate or Low baseline requirements. The combination of objective requirements and subjective information enables State to render a readiness decision based on a more complete understanding of the vendor's security capabilities.

Section 4, Capability Readiness, is organized into three sections:

- **Section 3.1, State Mandates**, identifies a small set of the state mandates a vendor must satisfy. State **will not** waive any of these requirements.
- **Section 3.2, State Requirements**, identifies an excerpt of the most compelling requirements from the National Institute of Science and Technology (NIST) Special Publication (SP) 800 document series and State guidance. **A VENDOR is unlikely to achieve approval if any of these requirements are not met.**
- **Section 3.3, Additional Capability Information**, identifies additional information that is not tied to specific requirements, **yet has typically reflected strongly on a VENDOR's ability to achieve approval.**

2. VENDOR System Information

Provide and validate the information below. For example, if the deployment model is Government only, ensure there are no non-Government customers. The VRAR template is intended for systems categorized at the Moderate or Low security impact level, in accordance with the FIPS Publication 199 Security Categorization.

Table 2-1. System Information

VENDOR Name: Spare Labs Inc.
Solution/System Name: Spare Labs Platform
Service Model: (e.g., IaaS, PaaS, SaaS) SAAS
FIPS PUB 199 System Security Level: (e.g., Moderate, Low) Moderate
Fully Operational as of: Enter the date the system became fully operational. 2007
Number of Customers (State/Others): Enter # of customers / # of other customers: 0/82
Deployment Model: Is the service a Public Cloud, Government-Only Cloud, Federal Government-Only Cloud, or Other? If other, please describe. Public Cloud
System Functionality: Briefly describe the functionality of the system and service being provided. Spare is a system to set-up, run and monitor your microtransit service in real-time. The Admin portal serves as the dispatcher and administrator-facing applications where DROs can easily and quickly create service zone(s), specific transit stop locations, set the operational time limit, set driver shifts, track vehicles, book and schedule trips based on requests, and more.

2.1. Relationship to Other Vendors or CSPs

If this system resides in another VENDOR's environment or inherits security capabilities, please provide the relevant details in Tables 2-2 and 2-3 below. **Please note**, the leveraged system itself must be State Authorized. For example, a large VENDOR may have a commercial service offering and a separate service offering with a State Authorization. Only the service offering with the State Authorization may be leveraged.

IMPORTANT: If there is a leveraged system, be sure to note below every capability that partially or fully leverages the underlying system. When doing so, indicate the capability is fully inherited or describe both the inherited and non-inherited aspects of the capability.

Table 2-2. Leveraged Systems

#	Question	Yes	No	N/A	If Yes, please describe.
1	Is this system leveraging an underlying provider?		No		Spare is a complete platform solution and does not leverage another provider to provide the service.

List all **services** leveraged. The system from which the service is leveraged must be listed in Table 2-2 above.

Table 2-3. Leveraged Services

#	Service	Service Capability	System
1	State what is being leveraged or "None" if no service is leveraged or if the VENDOR is responsible for the entire stack.	List the capability the service provides (e.g., load balancer, SIEM, database, audit logging).	Identify the system from which the service is being leveraged.

2.2. Data Flow Diagrams

Insert Vendor-validated data flow diagram(s) and provide a written description of the data flows. The diagram(s) must:

- *clearly identify anywhere State data is to be processed, stored, or transmitted;*
 - *clearly delineate how data comes into and out of the system boundary;*
 - *clearly identify data flows for privileged, non-privileged and customer access; and*
 - *depict how **all ports, protocols, and services** of all inbound and outbound traffic are represented and managed.*
-
- The state data will be processed at the Google Data Center US-East located at Moncks Corner, South Carolina.
 - Spare's network security architecture consists of multiple security zones. We monitor and protect our network to ensure no unauthorized access is performed, using:
A virtual private cloud, a bastion host or VPN with network access control lists and no public IP addresses. A firewall that monitors and controls incoming and outgoing network traffic.
An In-App WAF and RASP solution that monitors and blocks potential malicious packets.

Please see the data flow diagram below.

The Vendor must base the assessment of separation measures on very strong evidence, such as the review of any existing penetration testing results, or an expert review of the products, architecture, and configurations involved. The Vendor must describe how the methods used to verify the strength of separation measures.

Spare logically segregates every piece of data based on tenantId. Every API call included has the knowledge of tenantId and this data is used by the application layer to prevent unauthorized access.

Cobalt conducted a gray box pentest of the Spare Platform (Web+API) application and API to assess the risk posture and identify security issues that could negatively affect Spare Labs's data, systems, or reputation. The scope of the assessment covered Spare Platform (Web+API) and included credentials for various levels of privilege within the scope. The pentest was conducted by 2 pentesters between Feb 20, 2023 and Mar 6, 2023. This pentest was a manual assessment of the security of the application's functionality, business logic, and vulnerabilities, such as those cataloged in the Open Web Application Security Project (OWASP) Top 10. The assessment also included a review of security controls and requirements listed in the OWASP Application Security Verification Standard (ASVS). The pentesters leveraged tools to facilitate their work. However, the majority of the assessment involved manual analysis. As the pentesting team identified vulnerabilities, they reported all of these issues to Spare Labs for remediation. Sincerely, The Cobalt Team During testing, Cobalt's pentesters tested for vulnerabilities and rated them based on the following categories:

Critical	High	Medium	Low	Informational
0	0	0	3	0

2.4. System Interconnections

A System Interconnection is a dedicated connection between information systems, such as between a SaaS/PaaS and underlying IaaS.

The Vendor must complete the table below. If the answer to any question is "yes," please briefly describe the connection. Also, if the answer to the last question is "yes," please complete Table 2-5 below.

Table 2-4. System Interconnections

#	Question	Yes	No	If Yes, please describe.
1	Does the system connect to the Internet?	Yes		System needs the internet for users to log in to the administrative portal over HTTPS protocol and for riders and drivers to use their apps. All data is encrypted using TLS 1.2
2	Does the system connect to a corporate or state infrastructure/network?		No	
3	Does the system connect to external systems?			<i>If "yes," complete Table 2-5 below.</i>

If there are connections to external systems, please list each in the table below, using one row per interconnection. If there are no external system connections, please type “None” in the first row.

Table 2-5. Interconnection Security Agreements (ISAs)

#	External System Connection	Does an ISA Exist?		Interconnection Description. If no ISA, please justify below.
		Yes	No	
1	None			None
2				

3. Capability Readiness

3.1. State Mandates

This section identifies State requirements applicable to all State approved systems. All requirements in this section must be met. Some of these topics are also covered in greater detail in Section 3.2, *State Requirements*, below.

Only answer “Yes” if the requirement is fully and strictly met. The Vendor must answer “No” if an alternative implementation is in place.

Table 3-1. State Mandates

#	Compliance Topic	Fully Compliant?	
		Yes	No
1	Data at Rest, Authentication: Are FIPS 140-2/-3 Validated or National Security Agency (NSA)-Approved cryptographic modules only used where cryptography is required?	Yes	
2	Transmission, Remote Access: Are FIPS 140-2/-3 Validated or National Security Agency (NSA)-Approved cryptographic modules consistently used where cryptography is required?	Yes	
3	Can the VENDOR’S solution integrate with the State’s NCID solution?	Yes	
4	Does the VENDOR utilize security boundary/threat protection devices to protect the network, system, application...e.g., firewalls intrusion detection/prevention systems, end point protection etc.? [SC-7] [SI-3/SI-4]	Yes	
5	Does the VENDOR have the ability to consistently remediate High risk vulnerabilities within 30 days and Medium risk vulnerabilities within 60 days? [SI-2]	Yes	
6	Does the VENDOR and system meet Federal Records Management Requirements, including the ability to support record holds, National Archives and Records Administration (NARA) requirements, and Freedom of Information Act (FOIA) requirements?	Yes	
7	Does the VENDOR store, process or transmit State data only in the continental US and is that data backed up in only US locations?	Yes	
8	Does the VENDOR have a process to securely dispose of State data from its systems upon request that is in accordance with the National Institute for Standards and Technology (NIST) Special Publication 800-88 revision 1 and will provide to the State a certificate of data destruction? [MP-6]	Yes	
9	All operating systems (OS) AND major application software components (e.g., Microsoft SQL, Apache Tomcat, Oracle Weblogic, etc.), must NOT be past N-1. Applications which are not operating on the most recent platform MUST have a roadmap to upgrade with a State approved timeline. Does the application support the N-1 requirement?	Yes	
10	Does the vendor have a current 3 rd party attestation certification and is it regularly renewed? The State requires an independent 3 rd party attestation (e.g., FedRAMP, SOC 2 Type 2, ISO 27001, or HITRUST) prior to contract award for systems containing Restricted/Highly Restricted data. Note: SaaS vendors cannot use IaaS/PaaS certification unless the application is explicitly covered as part of the IaaS/PaaS assessments. [CA-7, RA-3, SA-9]	Yes	

11	Does the VENDOR's staff have appropriate background checks for unprivileged and privileged access and accounts according to Federal and/or State designation procedures for those systems that require it? [AC-2, PS-3]	Yes	

3.2. State Requirements

This section identifies additional State Readiness requirements. All requirements in this section must be met; however, alternative implementations and non-applicability justifications may be considered on a limited basis.

3.2.1. Data at Rest and Authentication [SC-13]

The Vendor must ensure FIPS 140-2, or 140-3 where available, Validated or NSA-Approved algorithms are used for all encryption modules. FIPS 140-2 Compliant is not sufficient. The Vendor may add rows to the table if appropriate but must not remove the original rows. The Vendor must identify all non-compliant cryptographic modules in use.

Table 3-2a. Data at Rest & Authentication

	Cryptographic Module Type	FIPS 140-2 Validated?		NSA Approved?		Describe Any Alternative Implementations (if applicable)	Describe Missing Elements or N/A Justification
		Yes	No	Yes	No		
1	Data at Rest [SC-28]	Yes					
2	Authentication [IA-5, IA-7]	Yes					

3.2.2. Transport Layer Security [NIST SP 800-52, Revision 2]

The Vendor must ensure FIPS 140-2, or 140-3 where available, Validated or NSA-Approved algorithms are used for all encryption modules relating to block ciphers, digital signatures and hash functions. Full FIPS mode is not required unless other regulatory requirements must be met. The Vendor may add rows to the table if appropriate but must not remove the original rows. The Vendor must identify all non-compliant cryptographic modules in use.

Table 3-2b. Transport Encryption

	Cryptographic Module Type	FIPS 140-2 Validated?		NSA Approved?		Describe Any Alternative Implementations (if applicable)	Describe Missing Elements or N/A Justification
		Yes	No	Yes	No		
1	Transmission [SC-8 (1), SC-12, SC-12 (2, 3)]	Yes					
2	Remote Access [AC-17 (2)]	N/A					All access to system is via HTTPS and not through remote access.

The Vendor must identify all protocols in use. The Vendor may add rows to the table if appropriate, but must not remove the original rows.

Table 3-3. Transport Protocol

#	The Cryptographic Module Type	Protocol In Use?		If “yes,” please describe use for both internal and external communications
		Yes	No	
1	SSL (Non-Compliant)			
2	TLS 1.0 (Non-Compliant)			
3	TLS 1.1 (Non-Compliant)			
4	TLS 1.2 (Compliant)	Yes		Spare uses HTTPS protocol for communication between cloud server and client computers. Users access Spare via browser interface or through Android/iOS apps. All communication is encrypted using TLS 1.2 or better protocol.
5	TLS 1.3 (Compliant)			

3.2.3. Identification and Authentication, Authorization, and Access Control

Only answer “yes” if the answer is consistently “yes.” For partially implemented areas, answer “no” and describe what is missing to achieve a “yes” answer. If inherited, please indicate partial or full inheritance in the “Describe Capability” column. Any non-inherited capabilities must be described.

Table 3-4. Identification and Authentication, Authorization, and Access Control

#	Question	Yes	No	Describe capability, supporting evidence, and any missing elements
1	Does the system uniquely identify and authorize organizational users (or processes acting on behalf of organizational users) in a manner that cannot be repudiated, and which sufficiently reduces the risk of impersonation? [IA-2, IA-4]	Yes		Spare adheres to all privacy regulations in the locations in which it operates. Therefore, user data follows applicable provincial, state and federal privacy laws. Spare’s system has HIPAA-compliant security features, including: • Authentication for site access • The ability to set user groups and their access and editing privileges • The ability to monitor users and maintain an audit trail • The ability for multiple organizations to use the software and have unique logins with a unique audit trail
2	Does the system require multi-factor authentication (MFA) for administrative accounts and functions? [IA-2, IA-2 (1), IA-2 (2)]	Yes		By integrating with NCID or other approved SAML based authentication, Spare can implement MFA.

3	Is role-based access used, managed, and monitored? [IA-4, IA-5]	Yes	Spare uses role based security with full audit and monitoring capability. Roles include: The following roles, with the following user permissions, are available: ● Administrator: Administrators have full view and write access to the entire suite of Spare Launch features, including, but not limited to: creating and editing services, setting and editing duties, creating and editing vehicles, creating and modifying requests, creating and modifying users, changing user permissions, as well as access to Spare Analyze and Realize (if applicable). ● Operations Manager: An Operation Manager looks after day to day operations. Their access is similar to the Administrator, but they are not able to create/edit services and financial aspects of the platform (Promos, Passes, Refunds, Payment Methods, etc.). ● Booking Agent: Booking agents only have write access to the User and Request menus, allowing them to create and edit non-administrator users as well as to create, edit, and delete trip requests. They can also view the Live Map, services, stops, favorite locations, reviews, and charges. ● Scheduler: Schedulers have the same permissions as booking agents, but can also create, edit, and delete driver duties and vehicles.

#	Question	Yes	No	Describe capability, supporting evidence, and any missing elements
				• Service Planner: Service Planners create the Service within the platform. They have access to create and edit Services and their dependent resources (Fleets, Zones, Stops, TimeRules). They can also create Groups and Rider Notifications. • Finance Manager: The Finance Manager has access to create and edit the Financial aspects of the platform. Those include promotions, refunds, and service revenue. • Access to Reporting: Allows for the creation of reports from Spare Analyze. • Access to Analytics: Allows the user to view the real-time analytics in Spare Analyze.
4	Does the system restrict non-authorized personnel's access to resources? [AC-6, AC-6 (1), AC-6 (2)]	Yes		No non-authorized personnel can access system resources and any unauthorized attempts are logged.
5	Does the system restrict non-privileged users from performing privileged function? [AC-6, AC-6 (1), AC-6 (2), AC-6 (10)]	Yes		The 'administrator' role and function is geared towards security administration while 'service planner' is designed for system administration functionality as it does not allow for roles and permissions to be altered. It provides full functionality to configure the transit service.
6	Does the system ensure secure separation of customer data? [SC-4]	Yes		Spare logically segregates every piece of data based on tenantId. Every API call included has the knowledge of tenantId and this data is used by the application layer to prevent unauthorized access.
7	Does the system ensure secure separation of customer processing environments? [SC-2]		No	<i>The capability description is not required here, but must be included in Section 2.3, Separation Measures.</i>

#	Question	Yes	No	Describe capability, supporting evidence, and any missing elements
8	Does the system restrict access of administrative personnel in a way that limits the capability of individuals to compromise the security of the information system? [AC-2]	Yes		<i>The capability description is not required here, but must be included in Section 2.3, Separation Measures.</i>
9	Does the remote access capability include VENDOR-defined and implemented usage restrictions, configuration guidance, and authorization procedure? [AC-17]		No	Remote Access is not available for accessing Spare.
10	How will the State's password policy be enforced? State requires minimum 14-character complex passwords (Upper, Lower, Special Character & Numerical) [IA-5]	Yes		

3.2.4. Audit, Alerting, Malware, and Incident Response

Only answer "yes" if the answer is consistently "yes." For partially implemented areas, answer "no" and describe what is missing to achieve a "yes" answer. If inherited, please indicate partial or full inheritance in the "Describe Capability" column. Any non-inherited capabilities must be described.

Table 3-5. Audit, Alerting, Malware, and Incident Response

#	Question	Yes	No	Describe capability, supporting evidence, and any missing elements
1	Does the system have the capability to detect, contain, and eradicate malicious software? [SI-3]	Yes		Our servers are protected by the highest level of security afforded by the Google Cloud platform. All laptops and workstations are MacOS based which limits vulnerability. Our organization is using Vanta, a tool to track each computer. Vanta actively monitors for any unwanted software/malware installed on the workstations. Vanta tracks various onboarding steps such as registering our workstations, accepting security policies, and making sure a password manager is installed for every member of the organization's devices.
2	Does the system store audit data in a tamper-resistant manner which meets chain of custody and any e-discovery requirements? [AU-4, AU-9]	Yes		Yes, only the CTO can edit audit data. We also leverage Google KMS for encryption key management and key rotation for protection of key data elements.

#	Question	Yes	No	Describe capability, supporting evidence, and any missing elements
3	Does the VENDOR have the capability to detect unauthorized or malicious use of the system, including insider threat and external intrusions? [SI-4, SI-4 (4), SI-4 (5), SI-7, SI-7 (7)]	Yes		Spare supports user authentication via unique passwords and multifactor authentication to protect against unauthorized access, use, disclosure, disruption, modification, and destruction of information assets to provide confidentiality, integrity, availability, and accountability. Network-level security monitoring and protection. Our network security architecture consists of multiple security zones. We monitor and protect our network to ensure no unauthorized access is performed, using: • A virtual private cloud, a bastion host or VPN with network access control lists and no public IP addresses • A firewall that monitors and controls incoming and outgoing network traffic • An Intrusion Detection and/or Prevention technologies solution that monitors and blocks potential malicious packets • IP address filtering

#	Question	Yes	No	Describe capability, supporting evidence, and any missing elements
4	Does the VENDOR log and monitor access to the system? [SI-4]	Yes		Activity Log Spare has developed a historical event log (activity log) that tracks changes made to duties, trips and everything in-between. The enhanced logging capabilities allow [clientname] agents to quickly troubleshoot issues by tracing actions in the system, understand the full story of what has happened in any particular scenario and help them identify the next steps. Traceability of activities in Spare is integral to ensuring a high quality of service. That's why Spare has enhanced logging capabilities that allow customers to easily troubleshoot issues when they arise. An example includes looking at a vehicle that has been "Paused" and wondering who paused it, when they paused it, and why. The activity log provides these answers.
5	Does the VENDOR have an Incident Response Plan and a fully developed Incident Response test plan? [IR-3, IR-8]	Yes		Yes Incident response plan is included in our response package.
6	Does the VENDOR have a plan and capability to perform security code analysis and assess code for security flaws, as well as identify, track, and remediate security flaws? [SA-11]			No CUSTOM CODE
7	Does the VENDOR implement automated mechanisms for incident handling and reporting? [IR-4, IR-4 (1), IR-6]	Yes		
8	Does the VENDOR retain online audit records for at least 90 days to provide support for after-the-fact investigations of security incidents and offline for at least one year to meet regulatory and organizational information retention requirements? [AU-11]	Yes		
9	Does the VENDOR have the capability to notify customers and regulators of confirmed incidents in a timeframe consistent with all legal, regulatory, or contractual obligations? The State of NC's requirement for security breach reporting is 24 hrs. of incident confirmation. [IR-6]	Yes		

#	Question	Yes	No	Describe capability, supporting evidence, and any missing elements
10	If the VENDOR's solution provides email "send as" capabilities, does it support DMARC and DKIM for email protection?			Not Applicable

3.2.5. Contingency Planning and Disaster Recovery

Only answer “yes” if the answer is consistently “yes.” For partially implemented areas, answer “no” and describe what is missing to achieve a “yes” answer. If inherited, please indicate partial or full inheritance in the “Describe Capability” column. Any non-inherited capabilities must be described.

Table 3-6. Contingency Planning and Disaster Recovery

#	Question	Yes	No	Describe capability, supporting evidence, and any missing elements
1	Does the VENDOR have the capability to recover the system to a known and functional state following an outage, breach, DoS attack, or disaster? [CP-2, CP-9, CP-10]	Yes		Spare follows a rigorous Discovery Recovery and Business Continuity Plan to prepare Spare and all of our customers in the event of extended service outages caused by factors beyond our control. Our top priority is to restore services to the widest extent possible in a minimum time frame. Spare’s approach includes the following: ○ Senior managers and executive staff will determine mitigation actions ○ Perform a disaster recovery test on an annual basis, including a test of backup restoration processes ○ Confirm continuity of information security, along with operational continuity ○ For information security incidents, we follow an Incident Response Plan, which involves our Security team who will monitor the incident and event tickets, and assign ticket severity based on three escalation categories: S3/S4 (Low and Medium Severity), S2 (High Severity), and S1 (Critical Severity).

#	Question	Yes	No	Describe capability, supporting evidence, and any missing elements
2	Does the VENDOR have a Contingency Plan and a fully developed Contingency Plan test plan in accordance with Statewide Information Security Manual? [CP-2, CP-4]			Spare follows a rigorous Discovery Recovery and Business Continuity Plan to prepare Spare and all of our customers in the event of extended service outages caused by factors beyond our control. Our top priority is to restore services to the widest extent possible in a minimum time frame. Spare's approach includes the following: Senior managers and executive staff will determine mitigation actions Perform a disaster recovery test on an annual basis, including a test of backup restoration processes Confirm continuity of information security, along with operational continuity For information security incidents, we follow an Incident Response Plan, which involves our Security team who will monitor the incident and event tickets, and assign ticket severity based on three escalation categories: S3/S4 (Low and Medium Severity), S2 (High Severity), and S1 (Critical Severity).
3	Does the system have alternate storage and processing facilities? [CP-6, CP-7]	Yes		The backup data center is physically separated and in the same region as the primary.
4	Does the system have or use alternate telecommunications providers? [CP-8]		No	Spare does not work directly with telecommunication providers.
5	Does the system have backup power generation or other redundancy? [PE-11]	Yes		
6	Does the VENDOR have service level agreements (SLAs) in place with all telecommunications providers? [CP-8]		No	Spare does not work directly with telecommunication providers.

3.2.6. Configuration and Risk Management

Only answer “yes” if the answer is consistently “yes.” For partially implemented areas, answer “no” and describe what is missing to achieve a “yes” answer. If inherited, please indicate partial or full inheritance in the “Describe Capability” column. Any non-inherited capabilities must be described.

Table 3-7. Configuration and Risk Management

#	Question	Yes	No	Describe capability, supporting evidence, and any missing elements
1	Does the VENDOR maintain a current, complete, and accurate baseline configuration of the information system? [CM-2]	Yes		
2	Does the VENDOR maintain a current, complete, and accurate inventory of the information system software, hardware, and network components? [CM-8]	Yes		
3	Does the VENDOR have a Configuration Management Plan? [CM-9]	Yes		
4	Does the VENDOR follow a formal change control process that includes a security impact assessment? [CM-3, CM-4, CM-4 (2)]	Yes		
5	Does the VENDOR employ automated mechanisms to detect inventory and configuration changes? [CM-2, CM-2 (2), CM-6, CM-8]	Yes		
6	Does the VENDOR prevent unauthorized changes to the system? [CM-5]	Yes		
7	Does the VENDOR establish configuration settings for products employed that reflect the most restrictive mode consistent with operational requirements? [CM-6, CM-7]		No	<i>If “yes,” describe if the configuration settings are based on Center for Internet Security (CIS) Benchmarks or United States Government Configuration Baseline (USGCB), or “most restrictive consistent with operational requirements.”</i>
8	Does the VENDOR ensure that checklists for configuration settings are Security Content Automation Protocol (SCAP)-validated or SCAP-compatible (if validated checklists are not available)? [CM-6]		No	

For the following questions, Vendors may use Table 3-18 “Continuous Monitoring Capabilities – Additional Details” to enter the capability descriptions, supporting evidence, and missing elements.

9	Does the VENDOR perform authenticated operating system/ infrastructure, web, and database vulnerability scans at least monthly, as applicable? [RA-5, RA-5 (5)]		No	Spare uses tools available within the Google Cloud platform to run vulnerability scans: External vulnerability scans are run on the production environment at least quarterly. Interior vulnerability scans shall are run against test environments which mirror production configurations. Penetration tests of the applications and production network shall be performed at least annually. Additional scanning and testing shall be performed following major changes to production systems.
10	Does the VENDOR demonstrate the capability to remediate High risk vulnerabilities within 30 days and Moderate risk vulnerabilities within 60 days? [RA-5, SI-2]	Yes		For information security vulnerabilities, we follow an Incident Response Plan, which involves our Security team who will monitor the incident and event tickets, and assign ticket severity based on three escalation categories: S3 / S3 (Low and Medium Severity), S2 (High Severity), and S1 (Critical Severity). All Critical and high Severity vulnerabilities will be remedied within 30 days.
11	When a High risk vulnerability is identified as part of continuous monitoring activities, does the VENDOR consistently check audit logs for evidence of exploitation? [RA-5]	Yes		
12	Does the VENDOR have a Supply Chain Risk Management (SCRM) plan and processes to identify and address weaknesses or deficiencies in the supply chain elements and processes of information systems?	Yes		<i>Describe the Vendor's SCRM plan and processes.</i>

3.2.7. Data Center Security

Only answer "yes" if the answer is consistently "yes." For partially implemented areas, answer "no" and describe what is missing to achieve a "yes" answer. If inherited, please indicate partial or full inheritance in the "Describe Capability" column. Any non-inherited capabilities must be described.

Table 3-8. Data Center Security

#	Question	Yes	No	Describe capability, supporting evidence, and any missing elements
1	Does the VENDOR restrict physical system access to only authorized personnel? [PE-2 through PE-6, PE-8]	Yes		

#	Question	Yes	No	Describe capability, supporting evidence, and any missing elements
2	Does the VENDOR monitor and log physical access to the information system, and maintain access records? [PE-6, PE-8]	Yes		
3	Does the VENDOR monitor and respond to physical intrusion alarms and surveillance equipment? [PE-6, PE-6 (1)]	Yes		

3.2.8. Policies, Procedures, and Training

The Vendor must indicate the status of policy and procedure coverage for the NIST 800-53 Rev 5 families listed in Table 3-9 below.

To answer “yes” to a policy, it must be fully developed, documented, and disseminated; and it must address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. A single policy document may address more than one family provided the NIST requirements of each “-1” are fully addressed.

To answer “yes” to a procedure, it must be fully developed and consistently followed by the appropriate staff. List all applicable procedure documents for each family.

VENDORS must establish their own set of Policies and Procedures (P&Ps). They cannot be inherited from a leveraged system, nor can they be provided by the customer. Any exceptions and/or missing policy and procedure elements must be explained in Table 3-10 below.

Table 3-9. Policies and Procedures

#	Family	Policy		Procedure		Title Version and Date
		Yes	No	Yes	No	
1	Access Control [AC-1]	Yes		Yes		Policy: Access Control Policy ● version 4, April 4, 2023 Procedure(s): ● version 4, April 4, 2023
2	Awareness & Training [AT-1]	Yes		Yes		Policy: Information Security Policy ● version 4, April 4, 2023 Procedure(s): ● version 4, April 4, 2023
3	Audit & Accountability [AU-1]	Yes		Yes		Policy: Code of Conduct Policy ● version 4, April 4, 2023 Procedure(s): ● version 4, April 4, 2023
4	Security Assessment & Authorization [CA-1]	Yes		Yes		Policy: Information Security Policy ● version 4, April 4, 2023 Procedure(s): ● version 4, April 4, 2023
5	Configuration Management [CM-1]	Yes		Yes		Policy: Operations Security Policy ● version 4, April 4, 2023 Procedure(s): ● version 4, April 4, 2023

#	Family	Policy		Procedure		Title Version and Date
		Yes	No	Yes	No	
6	Contingency Planning [CP-1]	Yes		Yes		Policy: Operations Security Policy • version 4, April 4, 2023 Procedure(s): • version 4, April 4, 2023
7	Identification & Authentication [IA-1]	Yes		Yes		Policy: Information Security Policy • version 4, April 4, 2023 Procedure(s): • version 4, April 4, 2023
8	Incident Response [IR-1]	Yes		Yes		Policy: Incident Response Policy • version 4, April 4, 2023 Procedure(s): • version 4, April 4, 2023
9	Maintenance [MA-1]	Yes		Yes		Policy: Secure Development Policy • version 4, April 4, 2023 Procedure(s): • version 4, April 4, 2023
10	Media Protection [MP-1]		No		No	Policy: Information Security Policy • version 4, April 4, 2023 Procedure(s): • version 4, April 4, 2023
11	Physical & Environmental Protection [PE-1]	Yes		Yes		Policy: Physical Security Policy • version 4, April 4, 2023 Procedure(s): • version 4, April 4, 2023
12	Personnel Security [PS-1]	Yes		Yes		Policy: Human Resource Security Policy • version 4, April 4, 2023 Procedure(s): • version 4, April 4, 2023
13	Risk Assessment [RA-1]	Yes		Yes		Policy: Risk Management Policy • version 4, April 4, 2023 Procedure(s): • version 4, April 4, 2023
14	System & Services Acquisition [SA-1]	Yes		Yes		Policy: Third Party Management Policy • version 4, April 4, 2023 Procedure(s): • version 4, April 4, 2023
15	System & Communications Protection [SC-1]	Yes		Yes		Policy: Information Security Policy • version 4, April 4, 2023 Procedure(s): • version 4, April 4, 2023
16	System & Information Integrity [SI-1]	Yes		Yes		Policy: Information Security Policy • version 4, April 4, 2023 Procedure(s): • version 4, April 4, 2023
17	Planning [PL-1]	Yes		Yes		Policy will be created if Spare is awarded the NCDOT contract.

#	Family	Policy		Procedure		Title Version and Date
		Yes	No	Yes	No	
18	Supply Chain Risk Management [SR-1]	Yes		Yes		Policy: Risk Management Policy - version 3, April 2023 Procedure(s): - version 3, April, 2023

For any family with a policy or procedure gap, please describe the gap below.

Table 3-10. Missing Policy and Procedure Elements

Missing Policy and Procedure Elements
•

The Vendor must answer the questions below.

Table 3-11. Security Awareness Training

Question	Yes	No	Describe capability, supporting evidence, and any missing elements
Does the VENDOR train personnel on security awareness and role-based security responsibilities? [AT-2]	Yes		Yes, All personnel are required to review Spare policies and undergo Security Awareness Training as well as HIPAA training. The training progress and completion is maintained using a tool called Haekka.

3.3. Additional Capability Information

State will evaluate the responses in this section on a case-by-case basis relative to a State-Ready designation decision.

3.3.1. Staffing Levels

*In the table below, the Vendor must describe the VENDOR's organizational structure, staffing levels currently dedicated to the security of the system, as well as any planned changes to these staffing levels. This description must clearly indicate role and number of individuals as well as identify which staff is full-time dedicated, and which are performing their role as a collateral duty. **Note: It is not necessary to include specific names of individuals, but rather their roles/titles.***

Table 3-12. Staffing Levels

Staffing Levels
15

3.3.2. Change Management Maturity

While the following change management capabilities are not required, they indicate a more mature change management capability and may influence a State Readiness decision, especially for larger systems.

The Vendor must answer the questions below.

Table 3-13. Change Management

#	Question	Yes	No	If "no", please describe how this is accomplished.
1	Does the VENDOR's change management capability include a fully functioning Change Control Board (CCB)?		No	The CTO is ultimately responsible for change management. Spare does not have a specific board for this purpose.
2	Does the VENDOR have and use development and/or test environments to verify changes before implementing them in the production environment?	Yes		

3.3.3. Vendor Dependencies and Agreements

The Vendor must answer the questions below.

Table 3-14. Vendor Dependencies and Agreements

#	Question	Yes	No	Instructions
1	Does the system have any dependencies on other vendors such as a leveraged service offering, hypervisor and operating system patches, physical security and/or software and hardware support?		No	If "yes," please complete Table 3-15. Vendor Dependencies below.
2	Within the system, are all products still actively supported by their respective vendors?	Yes		If any are not supported, answer, "No."
3	Does the VENDOR have a formal agreement with a vendor, such as for maintenance of a leveraged service offering?		No	If "yes," please complete Table 3-16. Formal Agreements Details below.

If there are vendor dependencies, please list each in the table below, using one row per dependency. For example, if using another vendor's operating system, list the operating system, version, and vendor name in the first column, briefly indicate the VENDOR's reliance on that vendor for patches, and indicate whether the vendor still develops and issues patches for that product. If there are no vendor dependencies, please type "None" in the first row.

Table 3-15. Vendor Dependency Details

#	Product and Vendor Name	Nature of Dependency	Still Supported?	
			Yes	No
1				
2				

If there are formal vendor agreements in place, please list each in the table below, using one row per agreement. If there are no formal agreements, please type "None" in the first row.

Table 3-16. Formal Agreements Details

#	Organization Name	Nature of Agreement
1		
2		

3.3.4. Continuous Monitoring Capabilities

In the tables below, please describe the current state of the VENDOR's Continuous Monitoring capabilities, as well as the length of time the VENDOR has been performing Continuous Monitoring for this system.

Table 3-17. Continuous Monitoring Capabilities

#	Question	Yes	No	Describe capability, supporting evidence, and any missing elements
1	Does the VENDOR have a lifecycle management plan that ensures products are updated before they reach the end of their vendor support period?	Yes		The engineering team is responsible for ensuring that all Products are updated before they reach the end of their lifecycle.
2	Does the VENDOR have the ability to scan all hosts in the inventory?	Yes		
3	Does the VENDOR have the ability to provide scan files in a structure data format, such as CSV, XML files?	Yes		
4	Is the VENDOR properly maintaining their Plan of Actions and Milestones (POA&M), including timely, accurate, and complete information entries for new scan findings, vendor check-ins, and closure of POA&M items?	Yes		

In the table below, provide any additional details the Vendor believes to be relevant to State's understanding of the VENDOR's Continuous Monitoring Capabilities. If the Vendor has no additional details, please state, "None."

Table 3-18. Continuous Monitoring Capabilities – Additional Details

Continuous Monitoring Capabilities – Additional Details

Can the vendor provide a current 3rd party attestation certification **annually** when required? **Note:** SaaS vendors cannot use IaaS/PaaS certification unless the application is explicitly covered as part of the IaaS/PaaS assessments. [CA-7, RA-3, SA-9]

No, Spare does not have any third-party certification of continuous monitoring other than annual external Penetration test report we will include in our proposal package.

3.3.5. Status of System Security Plan (SSP)

In the table below, explicitly state whether the SSP is fully developed, partially developed, or non-existent. Identify any sections that the VENDOR has not yet developed.

Table 3-19. Maturity of the System Security Plan

Maturity of the System Security Plan
non-existent

In the table below, state the number of controls identified as “Not applicable” in the SSP. List the Control Identifier for each, and indicate whether a justification for each has been provided in the SSP control statement.

Table 3-20. Controls Designated “Not Applicable”

<x> Controls are Designated “Not Applicable”

In the table below, state the number of controls with an alternative implementation. List the Control Identifier for each.

Table 3-21. Controls with an Alternative Implementation

<x> Controls have an Alternative Implementation

Organization’s Security Representative or designee

PLEASE PRINT NAME



SIGNATURE

June 16, 2023

Date



**System and Organization Controls (SOC) 2 Type II
Report on Management's Description of its**

Transportation Services System

**And the Suitability of Design of Controls Relevant to the
Controls Placed in Operation and Test of Operating Effectiveness Relevant to
Security, Availability, Confidentiality**

**For the Period
June 1, 2021 to May 31, 2022**

**Together with
Independent Service Auditors' Report**



Table of Contents

I. Independent Service Auditors' Report	3
II. Assertion of Spare's Management	8
III. Description of Spare's Transportation Services System	11
IV. Description of Criteria, Controls, Tests and Results of Tests	28



I. Independent Service Auditors' Report

Independent Service Auditors' Report

To the Management of Spare Labs, Inc. (Spare)

Scope

We have examined Spare's accompanying description of its Transportation Services System titled "Description of Spare's Transportation Services System" throughout the period June 1, 2021 to May 31, 2022 (description) based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*), and the suitability of the design and operating effectiveness of controls stated in the description throughout the period June 1, 2021 to May 31, 2022, to provide reasonable assurance that Spare's service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, Confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

Spare uses subservice organizations to provide application maintenance and support services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Spare, to achieve Spare's service commitments and system requirements based on the applicable trust services criteria. The description presents Spare's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Spare's controls. Our examination did not include the services provided by the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Spare, to achieve Spare's service commitments and system requirements based on the applicable trust services criteria. The description presents Spare's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Spare's controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

Service Organization's Responsibilities

Spare is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Spare's service commitments and system requirements were achieved. Spare has provided the accompanying assertion titled "Assertion of Spare Management" (assertion) about the description and the suitability of design and operating effectiveness of controls stated therein. Spare is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service Auditors' Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of design and operating effectiveness of controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed and operated effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of the description of a service organization's system and the suitability of the design and operating effectiveness of controls involves the following:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively
- Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria
- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria
- Testing the operating effectiveness of controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria
- Evaluating the overall presentation of the description

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Inherent Limitations

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual users may consider important to meet their informational needs.

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design and operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Description of Tests of Controls

The specific controls we tested, and the nature, timing, and results of those tests are listed in section IV.

Opinion

In our opinion, in all material respects,

- a. the description presents Spare's Transportation Services System that was designed and implemented throughout the period June 1, 2021 to May 31, 2022, in accordance with the description criteria.
- b. the controls stated in the description were suitably designed throughout the period June 1, 2021 to May 31, 2022, to provide reasonable assurance that Spare's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period and if the subservice organization and user entities applied the complementary controls assumed in the design of Spare's controls throughout that period.
- c. the controls stated in the description operated effectively throughout the period June 1, 2021 to May 31, 2022, to provide reasonable assurance that Spare's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of Spare's controls operated effectively throughout that period.

Restricted Use

This report, including the description of test of controls and results thereof in section IV, is intended solely for the information and use of Spare, user entities of Spare's Transportation Services System during some or all of the period June 1, 2021 to May 31, 2022, business partners of Spare subject to risks arising from interactions with the Transportation Services System, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization
- How the service organization's system interacts with user entities, business partners, subservice organizations, and other parties
- Internal control and its limitations
- Complementary user entity controls and complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements
- User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services
- The applicable trust services criteria
- The risks that may threaten the achievement of the service organization's service commitments and system requirements and how controls address those risks

This report is not intended to be, and should not be, used by anyone other than these specified parties.



San Jose, California

July 4, 2022



II. Assertion of Spare Management



Assertion of Spare Management

We have prepared the accompanying description of Spare Labs, Inc.'s (Spare) Transportation Services System titled "Description of Spare's Transportation Services System" throughout the period June 1, 2021 to May 31, 2022, (description) based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (AICPA, Description Criteria)*. The description is intended to provide report users with information about the Transportation Services System that may be useful when assessing the risks arising from interactions with Spare's system, particularly information about system controls that Spare has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, Confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria)*.

Spare uses subservice organizations to provide application maintenance and support services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Spare, to achieve Spare's service commitments and system requirements based on the applicable trust services criteria. The description presents Spare's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Spare's controls. The description does not disclose the actual controls at the subservice organizations.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Spare, to achieve Spare's service commitments and system requirements based on the applicable trust services criteria. The description presents Spare's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Spare's controls.

We confirm, to the best of our knowledge and belief, that

- a. the description presents Spare's Transportation Services System that was designed and implemented throughout the period June 1, 2021 to May 31, 2022, in accordance with the description criteria.
- b. the controls stated in the description were suitably designed throughout the period June 1, 2021 to May 31, 2022, to provide reasonable assurance that Spare's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, and if the subservice organization and user entities applied the complementary controls assumed in the design of Spare's controls throughout that period.



- c. the controls stated in the description operated effectively throughout the period June 1, 2021 to May 31, 2022, to provide reasonable assurance that Spare's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of Spare's controls operated effectively throughout that period.

Signed by Spare Management

July 4, 2022



III. Description of Spare's Transportation Services System



Description of Spare's Transportation Services System

Company Background

Spare Labs, Inc. (Spare) was founded in November 2015 with a vision to accelerate the global shift to efficient and autonomous mobility. We're doing that by enabling anyone to plan, launch and analyze a smart transportation network in seconds.

At the core of Spare's offerings is the Spare Platform, a Software-as-a-Service (SaaS) solution that manages, dispatches and handles bookings for pooled on-demand and scheduled transit systems. Spare Platform encompasses a sophisticated back-end with a host of adjustable service parameters and an accessible front-end that keeps riders and drivers informed in real-time. It can handle any service configuration, optimize trips by pooling riders across these different service categories on to the same vehicle, and engage third-party fleets. Ideal use cases for the platform include first/last mile transit, taxi and ride-hail, paratransit, and on-demand transportation.

At Spare we believe that transportation is in the middle of a transition between traditional modes of travel to mobility as a service (MaaS). With this in mind, Spare has seamlessly integrated several smart transportation services on top of the powerful Spare Platform. From the apps to the dispatcher tools, Spare has focused on building an integrated experience where transportation experience is connected – not fragmented. This results in a single platform that can be launched across multiple travel modes that manage the whole journey, not just the trip.

Services Provided

Spare provides a software as a service solution for designing and operating scheduled and real time transportation services.

Spare's core application, Spare Platform is a cloud-based, multi-tenant application suite that enables operation of various on-demand services such as paratransit, microtransit, NEMT, fixed route.

The system is responsible for the following functions:

- Transportation service planning
- Determining ride eligibility
- Providing ride booking functionality to riders
- Providing a driver interface
- Managing operational fleets and scheduling drivers/vehicles
- Managing payments and billing using 3rd party payment integrations
- Providing operational data analysis and reporting



- Keeping riders up-to-date on their trip using notifications through SMS, Phone, Email, MobilePush, operation of various on demand services such as paratransit, microtransit, NEMT, fixed route

Principal Service Commitments and System Requirements

Spare designs its processes and procedures related to Spare Platform to meet its objectives for its transportation services. Those objectives are based on the service commitments that Spare makes to user entities, the laws and regulations that govern the provision of transportation services, and the financial, operational, and compliance requirements that Spare has established for the services.

Some transportation services of Spare are subject to the security and privacy requirements of the Health Insurance Portability and Accountability Act Administrative Simplification, as amended, including relevant regulations, as well as state privacy security laws and regulations in the jurisdictions in which Spare operates.

Security commitments to user entities are documented and communicated in Service Level Agreements (SLAs) and other customer agreements, as well as in the description of the service offering provided online. Security commitments are standardized and include, but are not limited to, the following:

- Security principles within the fundamental designs of the Spare Platform that are designed to permit system users to access the information they need based on their role in the system while restricting them from accessing information not needed for their role
- Use of encryption technologies to protect customer data both at rest and in transit

Spare establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in Spare's system policies and procedures, system design documentation, and contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed and how employees are hired and trained. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of the Spare Platform.

Components of the System

Infrastructure

Primary infrastructure used to provide Spare's services includes the following:



Primary Infrastructure		
Hardware	Type	Purpose
Google Cloud Platform (GCP)	Cloud Provider	Infrastructure provider for Spare's systems

Software

Primary software used to provide Spare's services includes the following:

Primary Software		
Software	Operating System	Purpose
Aiven	DBMS	Database management system
G-Suite	Identity Provider	Provides central access control management for various tools
Jamf Now	MDM	Provides company device management

People

Spare has a staff of approximately 70 employees organized in the following functional areas:

- Corporate: executives, and company administrative support staff, such as legal, compliance, internal audit, training, contracting, accounting, finance, human resources.
- Partner Success: Staff that works with our customers to ensure the successful adoption of Spare Platform for customer use cases.
- Product & Engineering: Staff responsible for innovating on the product and ensuring we meet our internal SLOs for service availability and security.
- Sales: Staff responsible for identifying new client relationships, maintaining existing ones, and creating revenue.

Data

Data, as defined by Spare constitutes the following:

- Master service, trip and fleet data



- Fleet operation data
- System files
- Error logs

All service data is stored within Spare's infrastructure in the cloud with encryption at rest and communicated over to various front end clients over Spare's Open API.

Data is consumed by end users through the Spare Rider App, Spare Driver App, Spare Admin Portal and over API integrations.

Processes, Policies and Procedures

Formal IT policies and procedures exist that describe physical security, logical access, computer operations, change control, and data communication standards. All teams are expected to adhere to the Spare policies and procedures that define how services should be delivered. These are located on the Company's intranet and can be accessed by any Spare team member.

Physical Security

The in-scope systems and infrastructure that supports Spare are hosted by GCP. GCP is responsible for the physical controls around Spare's in-scope systems and infrastructure.

Logical Access

Spare uses role-based security architecture and requires users of the system to be identified and authenticated prior to the use of any system resources. Resources are protected through the use of native system security and add-on software products that identify and authenticate users and validate access requests against the users' authorized roles in access control lists. In the event incompatible responsibilities cannot be segregated, Spare implements monitoring of one or more of the responsibilities. Monitoring must be performed by a superior without responsibility for performing the conflicting activities or by personnel from a separate department.

All resources are managed in the asset inventory system and each asset is assigned an owner. Owners are responsible for approving access to the resource and for performing periodic reviews of access by role. Employees and approved vendor personnel sign on to the Spare network using an Gsuite user ID and password. Users are also required to separately sign on to any systems or applications that do not use the shared sign-on functionality of Gsuite. Passwords must conform to defined password standards and are enforced through parameter settings in the Gsuite. These settings are part of the configuration standards and force users to change passwords at a defined interval, disable the user ID's ability to access the system and components after a specified number of unsuccessful access attempts, and mask workstation screens, requiring reentry of the user ID and password after a period of inactivity.



Customer employees' access Spare services through the Internet using the SSL functionality of their webbrowser. These customer employees must supply a valid user ID and password to gain access to customer cloud resources. Passwords must conform to password configuration requirements configured on the virtual devices using the virtual server administration account. Virtual devices are initially configured in accordance with Spare's configuration standards, but these configuration parameters may be changed by the virtual server administration account.

Customer employees may sign on to their systems using virtual server administration accounts. These administration accounts use a two-factor digital certificate-based authentication system.

Upon hire, employees are assigned to a position in the HR management system. Two days prior to the employees' start date, the HR management system creates a report of employee user IDs to be created and access to be granted. The report is used by the security help desk to create user IDs and access rules. Access rules have been pre-defined based on the defined roles. The system lists also include employees with position changes and the associated roles to be changed within the access rules.

On an annual basis, access rules for each role are reviewed by a working group composed of security help desk, data center, customer service, and HR personnel. In evaluating role access, group members consider job description, duties requiring segregation, and risks associated with access. Completed rules are reviewed and approved by the CISO. As part of this process, the CISO reviews access by privileged roles and requests modifications based on this review.

The HR system generates a list of terminated employees on a daily basis. This daily report is used by the security help desk to delete employee access. On an annual basis, HR runs a list of active employees. The security help desk uses this list to suspend user IDs and delete all access roles from IDs belonging to terminated employees.

On a quarterly basis, managers review roles assigned to their direct reports.

Computer Operations – Backups

Database backups are performed by our database management vendor, Aiven.

Spare's personnel perform annual backup testing.

Computer Operations – Availability

Incident response policies and procedures are in place to guide personnel in reporting and responding to information technology incidents. Procedures exist to identify, report, and act upon system security breaches and other incidents. Incident response procedures are in place to identify and respond to incidents on the network.



Spare monitors the capacity utilization of physical and computing infrastructure both internally and for customers to ensure that service delivery matches service level agreements. Spare evaluates the need for additional infrastructure capacity in response to growth of existing customers and/or the addition of new customers. Infrastructure capacity monitoring includes, but is not limited to, the following infrastructure:

- CPU usage
- Disk storage
- Network bandwidth

Spare has implemented a patch management process to ensure contracted customer and infrastructure systems are patched in accordance with vendor recommended operating system patches. Customers and Spare system owners review proposed operating system patches to determine whether the patches are applied. Customers and Spare systems are responsible for determining the risk of applying or not applying patches based upon the security and availability impact of those systems and any critical applications hosted on them. Spare staff validate that all patches have been installed and if applicable that reboots have been completed.

Change Control

Spare maintains documented Systems Development Life Cycle (SDLC) policies and procedures to guide personnel in documenting and implementing application and infrastructure changes. Change control procedures include change request and initiation processes, documentation requirements, development practices, quality assurance testing requirements, and required approval procedures.

A ticketing system is utilized to document the change control procedures for changes in the application and implementation of new changes. Development and testing are performed in an environment that is logically separated from the production environment. Management approves changes prior to migration to the production environment and documents those approvals within the ticketing system.

Version control software is utilized to maintain source code versions and migrate source code through the development process to the production environment. The version control software maintains a history of code changes to support rollback capabilities and tracks changes to developers.

Spare has implemented a patch management process to ensure contracted customer and infrastructure systems are patched in accordance with vendor recommended operating system patches. Customers and Spare system owners review proposed operating system patches to determine whether the patches are applied. Customers and Spare systems are responsible for determining the risk of applying or not applying patches based upon the security and availability impact of those systems and any critical applications hosted on them. Spare staff validate that all patches have been installed and if applicable that reboots have been completed.



Data Communications

Firewall systems are in place to filter unauthorized inbound network traffic from the Internet and deny any type of network connection that is not explicitly authorized. Network address translation (NAT) functionality is utilized to manage internal IP addresses. Administrative access to the firewall is restricted to authorized employees.

Redundancy is built into the system infrastructure supporting the data center services to help ensure that there is no single point of failure that includes firewalls, routers, and servers. In the event that a primary system fails, the redundant hardware is configured to take its place.

Penetration testing is conducted to measure the security posture of a target system or environment. The third-party vendor uses an accepted industry standard penetration testing methodology specified by Spare. The third-party vendor's approach begins with a vulnerability analysis of the target system to determine what vulnerabilities exist on the system that can be exploited via a penetration test, simulating a disgruntled/disaffected insider or an attacker that has obtained internal access to the network. Once vulnerabilities are identified, the third-party vendor attempts to exploit the vulnerabilities to determine whether unauthorized access or other malicious activity is possible. Penetration testing includes network and application layer testing as well as testing of controls and processes around the networks and applications and occurs from both outside (external testing) and inside the network.

Vulnerability scanning is performed by a third-party vendor on a quarterly basis in accordance with Spare policy. The third-party vendor uses industry standard scanning technologies and a formal methodology specified by Spare. These technologies are customized to test the organization's infrastructure and software in an efficient manner while minimizing the potential risks associated with active scanning. Retests and on-demand scans are performed on an as needed basis. Scans are performed during nonpeak windows. Tools requiring installation in the Spare system are implemented through the Change Management process. Scanning is performed with approved scanning templates and with bandwidth throttling options enabled.

Boundaries of the System

The scope of this report includes the Transportation Services performed by Spare. This report does not include the data center hosting services provided by GCP.

The applicable trust services criteria and the related controls

Common Criteria (Security)

Security refers to the protection of information during its collection or creation, use, processing, transmission, and storage and systems that use electronic information to process, transmit or transfer, and store information to enable the entity to meet its objectives. Controls over security prevent or detect the breakdown and circumvention of segregation of duties, system failure, incorrect processing, theft or other unauthorized removal of information or system resources, misuse of software, and improper access to or use of, alteration, destruction, or disclosure of information.



Common Criteria (Security)

Availability

Availability refers to the accessibility of information used by the entity's systems, as well as the products or services provided to its customers. The availability objective does not, in itself, set a minimum acceptable performance level; it does not address system functionality (the specific functions a system performs) or usability (the ability of users to apply system functions to the performance of specific tasks or problems). However, it does address whether systems include controls to support accessibility for operation, monitoring, and maintenance.

Confidentiality

Confidentiality addresses the entity's ability to protect information designated as confidential from its collection or creation through its final disposition and removal from the entity's control in accordance with management's objectives. Information is confidential if the custodian (for example, an entity that holds or stores information) of the information is required to limit its access, use, and retention and restrict its disclosure to defined parties (including those who may otherwise have authorized access within its system boundaries). Confidentiality requirements may be contained in laws or regulations or in contracts or agreements that contain commitments made to customers or others. The need for information to be confidential may arise for many different reasons. For example, the information may be proprietary, intended only for entity personnel.

Confidentiality is distinguished from privacy in that privacy applies only to personal information, whereas confidentiality applies to various types of sensitive information. In addition, the privacy objective addresses requirements regarding collection, use, retention, disclosure, and disposal of personal information. Confidential information may include personal information as well as other information, such as trade secrets and intellectual property.

Control Environment

Integrity and Ethical Values

The effectiveness of controls cannot rise above the integrity and ethical values of the people who create, administer, and monitor them. Integrity and ethical values are essential elements of Spare's control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the product of Spare's ethical and behavioral standards, how they are communicated, and how they are reinforced in practices. They include management's actions to remove or reduce incentives and temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts. They also include the communication of entity values and behavioral standards to personnel through policy statements and codes of conduct, as well as by example.

Specific control activities that the service organization has implemented in this area are described below:

- Formally, documented organizational policy statements and codes of conduct communicate entity values and behavioral standards to personnel.



- Policies and procedures require employees to sign an acknowledgment form indicating they have been given access to the employee manual and understand their responsibility for adhering to the policies and procedures contained within the manual.
- A confidentiality statement agreeing not to disclose proprietary or confidential information, including client information, to unauthorized parties is a component of the employee handbook.
- Background checks are performed for employees as a component of the hiring process.

Commitment to Competence

Spare's management defines competence as the knowledge and skills necessary to accomplish tasks that define employees' roles and responsibilities. Management's commitment to competence includes management's consideration of the competence levels for particular jobs and how those levels translate into the requisite skills and knowledge.

Specific control activities that the service organization has implemented in this area are described below:

- Management has considered the competence levels for particular jobs and translated required skills and knowledge levels into written position requirements.
- Training is provided to maintain the skill level of personnel in certain positions.

Management's Philosophy and Operating Style

Spare's management philosophy and operating style encompass a broad range of characteristics. Such characteristics include management's approach to taking and monitoring business risks, and management's attitudes toward information processing, accounting functions, and personnel.

Specific control activities that the service organization has implemented in this area are described below:

- Management is periodically briefed on regulatory and industry changes affecting the services provided.
- Executive management meetings are held to discuss major initiatives and issues that affect the business as a whole.

Organizational Structure and Assignment of Authority and Responsibility

Spare's organizational structure provides the framework within which its activities for achieving entitywide objectives are planned, executed, controlled, and monitored. Management believes establishing a relevant organizational structure includes considering key areas of authority and responsibility. An organizational structure has been developed to suit its needs. This organizational structure is based, in part, on its size and the nature of its activities.



Spare's assignment of authority and responsibility activities include factors such as how authority and responsibility for operating activities are assigned and how reporting relationships and authorization hierarchies are established. It also includes policies relating to appropriate business practices, knowledge, and experience of key personnel, and resources provided for carrying out duties. In addition, it includes policies and communications directed at ensuring personnel understand the entity's objectives, know how their individual actions interrelate and contribute to those objectives, and recognize how and for what they will be held accountable.

Specific control activities that the service organization has implemented in this area are described below:

- Organizational charts are in place to communicate key areas of authority and responsibility.
- Organizational charts are communicated to employees and updated as needed.

Human Resource Policies and Practices

Spare's success is founded on sound business ethics, reinforced with a high level of efficiency, integrity, and ethical standards. The result of this success is evidenced by its proven track record for hiring and retaining top quality personnel who ensures the service organization is operating at maximum efficiency. Spare's human resources policies and practices relate to employee hiring, orientation, training, evaluation, counseling, promotion, compensation, and disciplinary activities.

Specific control activities that the service organization has implemented in this area are described below:

- New employees are required to sign acknowledgement forms for the employee handbook and a confidentiality agreement following new hire orientation on their first day of employment.
- Evaluations for each employee are performed on an annual basis.
- Employee termination procedures are in place to guide the termination process and are documented in a termination checklist.

Risk Assessment Process

Spare's risk assessment process identifies and manages risks that could potentially affect Spare's ability to provide reliable services to user organizations. This ongoing process requires that management identify significant risks inherent in products or services as they oversee their areas of responsibility. Spare identifies the underlying sources of risk, measures the impact to organization, establishes acceptable risk tolerance levels, and implements appropriate measures to monitor and manage the risks.

This process has identified risks resulting from the nature of the services provided by Spare, and management has implemented various measures designed to manage these risks. Risks identified in this process include the following:

- Operational risk – changes in the environment, staff, or management personnel
- Strategic risk - new technologies, changing business models, and shifts within the industry



- Compliance – legal and regulatory changes

Spare has established an independent organizational business unit that is responsible for identifying risks to the entity and monitoring the operation of the firm's internal controls. The approach is intended to align the entity's strategy more closely with its key stakeholders, assist the organizational units with managing uncertainty more effectively, minimize threats to the business, and maximize its opportunities in the rapidly changing market environment. Spare attempts to actively identify and mitigate significant risks through the implementation of various initiatives and continuous communication with other leadership committees and senior management.

Integration with Risk Assessment

The environment in which the system operates; the commitments, agreements, and responsibilities of Spare's system; as well as the nature of the components of the system result in risks that the criteria will not be met. Spare addresses these risks through the implementation of suitably designed controls to provide reasonable assurance that the criteria are met. Because each system and the environment in which it operates are unique, the combination of risks to meeting the criteria and the controls necessary to address the risks will be unique. As part of the design and operation of the system, Spare's management identifies the specific risks that the criteria will not be met and the controls necessary to address those risks.

Information and Communications Systems

Information and communication are an integral component of Spare's internal control system. It is the process of identifying, capturing, and exchanging information in the form and time frame necessary to conduct, manage, and control the entity's operations. This process encompasses the primary classes of transactions of the organization, including the dependence on, and complexity of, information technology. At Spare, information is identified, captured, processed, and reported by various information systems, as well as through conversations with clients, vendors, regulators, and employees.

Various weekly calls are held to discuss operational efficiencies within the applicable functional areas and to disseminate new policies, procedures, controls, and other strategic initiatives within the organization. Additionally, all hands meetings are held monthly to provide staff with updates on the firm and key issues affecting the organization and its employees. Senior executives lead all hands meetings with information gathered from formal automated information systems and informal databases, as well as conversations with various internal and external colleagues. General updates to entity-wide security policies and procedures are usually communicated to the appropriate Spare personnel via e-mail messages or Slack messages.



Monitoring Controls

Management monitors controls to ensure that they are operating as intended and that controls are modified as conditions change. Spare's management performs monitoring activities to continuously assess the quality of internal control over time. Necessary corrective actions are taken as required to correct deviations from company policies and procedures. Employee activity and adherence to company policies and procedures is also monitored. This process is accomplished through ongoing monitoring activities, separate evaluations, or a combination of the two.

On-Going Monitoring

Spare's management conducts quality assurance monitoring on a regular basis and additional training is provided based upon results of monitoring procedures. Monitoring activities are used to initiate corrective action through department meetings, internal conference calls, and informal notifications.

Management's close involvement in Spare's operations helps to identify significant variances from expectations regarding internal controls. Upper management evaluates the facts and circumstances related to any suspected control breakdown. A decision for addressing any control's weakness is made based on whether the incident was isolated or requires a change in the company's procedures or personnel. The goal of this process is to ensure legal compliance and to maximize the performance of Spare's personnel.

Reporting Deficiencies

An internal tracking tool is utilized to document and track the results of on-going monitoring procedures. Escalation procedures are maintained for responding and notifying management of any identified risks. Risks receiving a high rating are responded to immediately. Corrective actions, if necessary, are documented and tracked within the internal tracking tool. Annual risk meetings are held for management to review reported deficiencies and corrective actions.

Changes to the System in the Last 12 Months

No significant changes have occurred to the services provided to user entities in the 12 months preceding the end of the review date.

Incidents in the Last 12 Months

No significant incidents have occurred to the services provided to user entities in the 12 months preceding the end of the review date.

Criteria Not Applicable to the System

All relevant trust services criteria were applicable to Spare's Transportation Services System.



Subservice Organizations

Spare Labs, Inc.'s services are designed with the assumption that certain controls will be implemented by subservice organizations. Such controls are called complementary subservice organization controls. It is not feasible for all of the trust services criteria related to Spare's services to be solely achieved by Spare's control procedures. Accordingly, subservice organizations, in conjunction with the services, should establish their own internal controls or procedures to complement those of Spare.

The following subservice organization controls should be implemented by Google Cloud Platform to provide additional assurance that the trust services criteria described within this report are met.

Subservice Organization – GCP		
Category	Criteria	Control
Common Criteria / Security	CC6.4	Physical protection and guidelines are described in the Physical Security Policy, Data Security Policy, Google Photography Policy, and the Data Center Access policy.
		Data center server floors, network rooms, and security systems are physically isolated from public spaces and/or delivery areas.
		Access to sensitive data center zones requires approval from authorized personnel and is controlled via badge readers, biometric identification mechanisms, and/or physical locks.
		Visitors to data center facilities must gain approval from authorized personnel, have their identity verified at the perimeter, and remain with an escort for the duration of their visit.
		Data center perimeters are defined and secured via physical barriers.
		Access lists to high-security areas in data centers are reviewed on a periodic basis and inappropriate access is removed in a timely manner.



Subservice Organization – GCP

Category	Criteria	Control

Security measures utilized in data centers are assessed annually and the results are reviewed by executive management.

Data centers are continuously staffed and monitored by security personnel using real-time video surveillance and/or alerts generated by security systems.

Availability

A1.2

Critical power and telecommunications equipment in data centers is physically protected from disruption and damage.

Redundant power is utilized to support the continued operation of critical data center equipment in the event of a loss of the primary power source(s).

Data centers are equipped with fire detection alarms and protection equipment.

The organization's information processing resources are distributed across distinct, geographically dispersed processing facilities to support service redundancy, and availability.

Backups are periodically performed to support the availability of customer data.

Restore tests are periodically performed to confirm the ability to recover customer data.



Subservice Organization – GCP

Category	Criteria	Control

		The organization conducts disaster recovery (DR) testing on an ongoing basis (and at least annually) to enable infrastructure and application teams to test communication plans, fail-over scenarios, operational transition, and other emergency responses. Participating teams create testing plans and document the results and lessons learned from the tests.

Spare Labs, Inc. management, along with the subservice organization, define the scope and responsibility of the controls necessary to meet all the relevant trust services criteria through written contracts, such as service level agreements. In addition, Spare Labs, Inc. performs monitoring of the subservice organization controls, including the following procedures

- Holding periodic discussions with vendors and subservice organization
- Reviewing attestation reports over services provided by vendors and subservice organization
- Monitoring external communications, such as customer complaints relevant to the services by the subservice organization

Complementary User Entity Controls

Spare's services are designed with the assumption that certain controls will be implemented by user entities. Such controls are called complementary user entity controls. It is not feasible for all the SOC 2 Criteria related to Spare's services to be solely achieved by Spare's control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of Spare's.

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the SOC 2 Criteria described within this report are met. As these items represent only a part of the control considerations that might be pertinent at the user entities' locations, user entities' auditors should exercise judgment in selecting and reviewing these complementary user entity controls.

1. User entities are responsible for understanding and complying with their contractual obligations to Spare.
2. User entities are responsible for notifying Spare of changes made to technical or administrative contact information.
3. User entities are responsible for maintaining their own system(s) of record.



4. User entities are responsible for ensuring the supervision, management, and control of the use of Spare services by their personnel.
5. User entities are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize Spare services.
6. User entities are responsible for providing Spare with a list of approvers for security and system configuration changes for data transmission.
7. User entities are responsible for immediately notifying Spare of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers.



IV. Description of Criteria, Controls, Tests and Results of Tests



Description of Criteria, Controls, Tests and Results of Tests

Relevant trust services criteria and Spare related controls are an integral part of management's system description and are included in this section. Sensiba San Filippo LLP performed testing to determine if Spare's controls were suitably designed and operating effectively to achieve the specified criteria for the Security, Availability, Confidentiality set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*), throughout the period June 1, 2021 to May 31, 2022.

Tests of the controls included inquiry of appropriate management, supervisory and staff personnel, observation of Spare activities and operations and inspection of Spare documents and records. The results of those tests were considered in the planning, the nature, timing, and extent of Sensiba San Filippo LLP's testing of the controls designed to achieve the relevant trust services criteria. As inquiries were performed for substantially all Spare controls, this test was not listed individually for every control in the tables below.

Description of Company Controls	Criteria Number	Service Auditor's Test of Controls	Result
CC1.0 - Control Environment			
CC1.1 - COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.			
The company has established a Code of Conduct and requires all employees to agree to it. Management monitors employees' acceptance of the code.	CC1.1.1a	Inspected the policy that documents the company's Code of Conduct to determine that it was in place and provides guidance on workforce conduct standards.	No exceptions noted
	CC1.1.1b	Inspected the signed Code of Conduct for a sample of employees to determine that they had agreed to the company's Code of Conduct.	No exceptions noted
CC1.2 - COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.			
The company demonstrates a commitment to integrity and ethical values by completing an annual review of ethical management and hiring practices.	CC1.2.1	Inspected the Code of Conduct, Information Security Policy, and evidence of management's review of the policies, to determine that the company demonstrates a commitment to integrity and ethical values.	No exceptions noted



Description of Company Controls	Criteria Number	Service Auditor's Test of Controls	Result
CC1.3 - COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.			
Company management maintains a formal organizational chart to clearly identify positions of authority and the lines of communication and escalation. The organizational charts are made available to employees through the company's HR Information System to facilitate communication in their role with the company.	CC1.3.1	Inspected the company's HR Information System to determine that organizational charts are accessible for employees.	No exceptions noted
CC1.4 - COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.			
All positions have a detailed job description that lists qualifications, such as requisite skills and experience, which candidates must meet in order to be hired by the company.	CC1.4.1	Inspected a sample engineer job description from the company to determine that all positions have a detailed job description that lists qualifications, such as requisite skills and experience, which candidates must meet in order to be hired by the company.	No exceptions noted
CC1.5 - COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.			
The company has established training programs for privacy and information security to help employees understand their obligations and responsibilities to comply with the company's security policies and procedures, including the identification and reporting of incidents. All full-time employees are required to complete these trainings annually.	CC1.5.1	Inspected the security awareness training completion for a sample of employees to determine that the company has established training programs for privacy and information security to help employees understand their obligations and responsibilities to comply with the company's security policies and procedures.	No exceptions noted



Description of Company Controls	Criteria Number	Service Auditor's Test of Controls	Result
Management has approved the company's security policies, and all employees agree to these procedures. Management also ensures that security policies are accessible to all employees and contractors.	CC1.5.2	Inspected the signed security policies for a sample of employees to determine that all employees had agreed to the security policies.	No exceptions noted
CC2.0 - Communication and Information			
CC2.1 - COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.			
The company uses a SOC 2 compliance platform called Vanta which objectively and continuously monitors the company's control environment and alerts management when internal control and security issues arise.	CC2.1.1	Inspected the Vanta tool configurations to determine that the company uses a SOC 2 compliance platform called Vanta which objectively and continuously monitors the company control environment and alerts management when internal control and security issues arise.	No exceptions noted
CC2.2 - COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.			
The company has policies and procedures in place to establish access control of information assets approved by management, posted on the company wiki, and accessible to all employees. All employees must agree to the Access Control Policy upon hire.	CC2.2.1a	Inspected company records to determine that a policy that establishes the access control of information assets is in place, has been approved by management, and is accessible to employees.	No exceptions noted
	CC2.2.1b	Inspected the signed Access Control policy for a sample of new hires to determine that they had agreed to the company's Access Control Policy.	No exceptions noted



Description of Company Controls	Criteria Number	Service Auditor's Test of Controls	Result
CC2.3 - COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.			
The company maintains a Privacy Policy that is available to all external users and internal employees, and it details the company's confidentiality and privacy commitments.	CC2.3.1	Inspected the company Privacy Policy to determine that it is available to all external users and internal employees, and it details the company's confidentiality and privacy commitments.	No exceptions noted
The company maintains a Terms of Service that is available to all external users and internal employees, and the terms detail the company's security and availability commitments regarding the systems. Where the Terms of Service may not apply, the company has Client Agreements or Master Service Agreements in place.	CC2.3.2	Inspected the company Terms of Service to determine that it is available to all external users and internal employees, and the terms detail the company's security and availability commitments regarding the systems.	No exceptions noted
CC3.0 - Risk Assessment			
CC3.1 - COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.			
The company's Risk Management Policy describes the processes the company has in place to identify new business and technical risks and how frequently those risks are mitigated.	CC3.1.1	Inspected the Risk Management Policy to determine that the company has a formal program for identifying and managing risks.	No exceptions noted



Description of Company Controls	Criteria Number	Service Auditor's Test of Controls	Result
CC3.2 - COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.			
The company maintains a risk register that continuously documents risks facing the company and in-progress remediation programs to address those risks.	CC3.2.1	Inspected the security risk assessment, which includes the risks, prioritization, and action plans to determine that the company maintains a risk register that continuously documents risks facing the company.	No exceptions noted
CC3.3 - COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.			
The company identifies and performs forensics regarding potential fraud activity (e.g., fraudulent reporting, loss of assets, unauthorized acquisitions, etc.).	CC3.3.1	Inspected the fraud assessment to determine that the entity identifies and performs forensics regarding potential fraud activity (e.g., fraudulent reporting, loss of assets, unauthorized acquisitions, etc.).	No exceptions noted
CC3.4 - COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.			
The company uses a SOC 2 compliance platform called Vanta which objectively and continuously monitors the company's control environment and alerts management when internal control and security issues arise.	CC3.4.1	Inspected the Vanta tool configurations to determine that the company uses a SOC 2 compliance platform called Vanta which objectively and continuously monitors the company control environment and alerts management when internal control and security issues arise.	No exceptions noted



Description of Company Controls	Criteria Number	Service Auditor's Test of Controls	Result
CC4.0 - Monitoring Activities			
CC4.1 - COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.			
Monitoring software is used to identify and evaluate ongoing system performance, changing resource utilization needs, and unusual system activity.	CC4.1.1	Inspected the monitoring dashboard to determine that monitoring software is used to identify and evaluate ongoing system performance, changing resource utilization needs, and unusual system activity.	No exceptions noted
CC4.2 - COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.			
The company has an established Incident Response Policy that outlines management responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents.	CC4.2.1	Inspected the Incident Response Plan to determine that it outlines formal procedure for responding to security events.	No exceptions noted
The company provides a process to external users for reporting security, confidentiality, integrity and availability failures, incidents, concerns, and other complaints.	CC4.2.2	Inspected the contact form to determine that the company provides a process to external users for reporting security, confidentiality, integrity and availability failures, incidents, concerns, and other complaints.	No exceptions noted



Description of Company Controls	Criteria Number	Service Auditor's Test of Controls	Result
CC5.0 - Control Activities			
CC5.1 - COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.			
A list of the company's system components is maintained for management's use in order to protect inventory from security events, maintain data confidentiality, and ensure system availability.	CC5.1.1	Inspected the inventory listing of information assets the company maintains in order to protect inventory from security events, maintain data confidentiality, and ensure system availability.	No exceptions noted
CC5.2 - COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.			
The company has implemented a vulnerability management program to detect and remediate system vulnerabilities in software packages used in company infrastructure.	CC5.2.1	Inspected the vulnerability scan to determine that the company has implemented a vulnerability management program to detect and remediate system vulnerabilities.	No exceptions noted
A penetration test is performed on an annual basis to identify security exploits. Issues identified are classified according to risk, analyzed and remediated in a timely manner.	CC5.2.2	Inspected the penetration test report to determine that a penetration test is performed on an annual basis to identify security exploits. Issues identified are classified according to risk, analyzed and remediated in a timely manner.	No exceptions noted



Description of Company Controls	Criteria Number	Service Auditor's Test of Controls	Result
CC5.3 - COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.			
Management has approved the company's security policies, and all employees agree to these procedures. Management also ensures that security policies are accessible to all employees and contractors.	CC5.3.1	Inspected the signed security policies for a sample of employees to determine that all employees had agreed to the security policies.	No exceptions noted
CC6.0 - Logical and Physical Access Controls			
CC6.1 - The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.			
Access to corporate network, production machines, network devices, and support tools requires a unique ID.	CC6.1.1a	Inspected the configuration for the company's infrastructure provider to determine that permissions are assigned to groups.	No exceptions noted
	CC6.1.1b	Inspected the configuration for the company's infrastructure tool to determine that employees have unique accounts on the service.	No exceptions noted
CC6.2 - Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.			
Access to infrastructure and code review tools is granted to new employees subsequent to the initial request.	CC6.2.1	Inspected the employee access tracker for a sample of new employees to determine that employee access to infrastructure is granted.	No exceptions noted
Access to infrastructure and code review tools is removed as a component of the termination process.	CC6.2.2	Inspected the termination checklist for a sample of terminated employees to determine that employee access to infrastructure is removed as a component of the termination process.	No exceptions noted



Description of Company Controls	Criteria Number	Service Auditor's Test of Controls	Result
CC6.3 - The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.			
Access is restricted to authorized personnel. Access approval and modification to access list are logged. Access is removed when appropriate. Access reviews are conducted quarterly.	CC6.3.1	Inspected the completed access reviews for Q4 2021 and Q2 2022 for the infrastructure provider to determine that access is limited to authorized personnel and removed when appropriate.	No exceptions noted
CC6.4 - The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.			
The company relies on GCP's physical and environmental controls, as defined and tested within GCP SOC 2 efforts.	CC6.4.1	Not Applicable - Control is Carved Out	The Criterion is carved out and the responsibility of the subservice organization.
CC6.5 - The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.			
Procedures are in place to identify data and software stored on equipment to be disposed and to render such data and software unreadable.	CC6.5.1	Inspected the Data Management Policy to determine that procedures are in place to identify data and software stored on equipment to be disposed and to render such data and software unreadable.	No exceptions noted



Description of Company Controls	Criteria Number	Service Auditor's Test of Controls	Result
CC6.6 - The entity implements logical access security measures to protect against threats from sources outside its system boundaries.			
Access to sensitive systems and applications requires two factor authentication in the form of user ID, password, OTP and/or certificate.	CC6.6.1	Inspected all user accounts with access to company infrastructure to determine that each is configured with MFA.	No exceptions noted
The company implements firewalls and configures them to protect against threats from sources outside its system boundaries.	CC6.6.2	Inspected the firewall configuration to determine that access control lists were used to filter unwanted network traffic.	No exceptions noted
CC6.7 - The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.			
Company management ensures that all company-issued laptop hard drives are encrypted using full disk encryption.	CC6.7.1	Inspected employee computers to determine that each was protected with full-disk encryption.	No exceptions noted
Customer data stored in databases is encrypted at rest.	CC6.7.2	Inspected the database configurations to determine that data is encrypted at rest.	No exceptions noted
Encryption is used to protect user authentication and administrator sessions of the internal admin tool transmitted over the Internet.	CC6.7.3	Inspected the encryption configurations to determine that all connections happen over SSL/TLS with a valid certificate from a reliable Certificate Authority.	No exceptions noted



Description of Company Controls	Criteria Number	Service Auditor's Test of Controls	Result
CC6.8 - The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.			
The company deploys malware detection software on all workstations that can access the production environment and has configured malware detection software to perform daily scans with immediate notification if malware is detected.	CC6.8.1	Inspected the antivirus configurations to determine that the company deploys malware detection software on all workstations that can access the production environment and has configured malware detection software to perform daily scans with immediate notification if malware is detected.	No exceptions noted
CC7.0 - System Operations			
CC7.1 - To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.			
The company has established a process to identify security vulnerabilities, using reputable outside sources, and assign a risk ranking (e.g. "high," "medium," or "low") to newly discovered security vulnerabilities.	CC7.1.1	Inspected the vulnerability management tool to determine that the company has established a process to identify security vulnerabilities, using reputable outside sources, and assign a risk ranking (e.g. "high," "medium," or "low") to newly discovered security vulnerabilities.	No exceptions noted
A penetration test is performed on an annual basis to identify security exploits. Issues identified are classified according to risk, analyzed and remediated in a timely manner.	CC7.1.2	Inspected the penetration test report to determine that a penetration test is performed on an annual basis to identify security exploits. Issues identified are classified according to risk, analyzed and remediated in a timely manner.	No exceptions noted



Description of Company Controls	Criteria Number	Service Auditor's Test of Controls	Result
CC7.2 - The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.			
The company uses a version control system to manage source code, documentation, release labeling, and other change management tasks. Access to the system must be approved by a system administrator.	CC7.2.1a	Inspected the company's version control system and confirmed it is actively used.	No exceptions noted
	CC7.2.1b	Inspected the users of the company's version control tool and confirmed that all accounts were authenticated to the company's account.	No exceptions noted
CC7.3 - The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.			
Remediation of security deficiencies are tracked through internal tools.	CC7.3.1	Inspected the security incident ticket for a sample of incidents to determine that security issues are tagged and prioritized accordingly.	N/A - Non-Occurrence (No security incidents during the period)
Security deficiencies tracked through internal tools are closed once remediated.	CC7.3.2	Inspected the security incident ticket for a sample of incidents to determine that security issues are resolved within the company's specified time frame.	N/A - Non-Occurrence (No security incidents during the period)
CC7.4 - The entity responds to identified security incidents by executing a defined incident-response program to understand, contain, remediate, and communicate security incidents, as appropriate.			
Remediation of security deficiencies are tracked through internal tools.	CC7.4.1	Inspected the security incident ticket for a sample of incidents to determine that security issues are tagged and prioritized accordingly.	N/A - Non-Occurrence (No security incidents during the period)



Description of Company Controls	Criteria Number	Service Auditor's Test of Controls	Result
CC7.4 - The entity responds to identified security incidents by executing a defined incident-response program to understand, contain, remediate, and communicate security incidents, as appropriate.			
Security deficiencies tracked through internal tools are closed once remediated.	CC7.4.2	Inspected the security incident ticket for a sample of incidents to determine that security issues are resolved within the company's specified time frame.	N/A - Non-Occurrence (No security incidents during the period)
The company has an established Incident Response Policy that outlines management responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents.	CC7.4.3	Inspected the Incident Response Plan to determine that it outlines formal procedure for responding to security events.	No exceptions noted
CC7.5 - The entity identifies, develops, and implements activities to recover from identified security incidents.			
The company has created a Disaster Recovery Plan to define the organization's procedures to recover information technology (IT) infrastructure and IT services within set deadlines in the case of a disaster or other disruptive incident.	CC7.5.1	Inspected the Company's Disaster Recovery Plan to determine that it outlines steps to take in the event of a disaster and has been updated in the past year.	No exceptions noted



Description of Company Controls	Criteria Number	Service Auditor's Test of Controls	Result
CC8.0 - Change Management			
CC8.1 - The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.			
The company uses a version control system to manage source code, documentation, release labeling, and other change management tasks. Access to the system must be approved by a system administrator.	CC8.1.1a	Inspected the company's version control system and confirmed it is actively used.	No exceptions noted
	CC8.1.1b	Inspected the users of the company's version control tool and confirmed that all accounts were authenticated to the company's account.	No exceptions noted
System changes must be approved by an independent technical resource prior to deployment to production.	CC8.1.2a	Inspected a sample of change tickets to determine that system changes must be approved by an independent technical resource prior to deployment to production.	No exceptions noted
	CC8.1.2b	Inspected a sample of change tickets to determine that application changes are tested prior to deployment to production.	No exceptions noted
CC9.0 - Risk Mitigation			
CC9.1 - The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.			
The company's Risk Management Policy describes the processes the company has in place to identify new business and technical risks and how frequently those risks are mitigated.	CC9.1.1	Inspected the Risk Management Policy to determine that the company has a formal program for identifying and managing risks.	No exceptions noted



Description of Company Controls	Criteria Number	Service Auditor's Test of Controls	Result
CC9.1 - The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.			
The company has created a Business Continuity Plan to define the criteria for continuing business operations for the organization in the event of a disruption.	CC9.1.2	Inspected the company's Business Continuity Plan to determine that it defined an operational and organizational strategy in the event of a disruption and has been updated in the past year.	No exceptions noted
CC9.2 - The entity assesses and manages risks associated with vendors and business partners.			
The company's team collects and reviews the SOC reports of its sub-service organizations on an annual basis.	CC9.2.1	Inspected the written policy governing the use of external service providers to determine that the sub-service organization approval process includes collecting and reviewing the provider's SOC report(s).	No exceptions noted
The company has implemented a Vendor Risk Management program with a framework for managing the lifecycle of vendor relationships.	CC9.2.2	Inspected the company's vendor management tool to determine that security documentation, including SOC 2 reports, are collected from sub-service organizations and key vendors.	No exceptions noted
A1.0 - Additional Criteria for Availability			
A1.1 - The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.			
Processing capacity and usage is monitored and expanded as necessary to provide for the continued availability of the system in accordance with system commitments and requirements.	A1.1.1	Inspected the monitoring dashboard to determine that processing capacity and usage is monitored and expanded as necessary to provide for the continued availability of the system in accordance with system commitments and requirements.	No exceptions noted



Description of Company Controls	Criteria Number	Service Auditor's Test of Controls	Result
A1.2 - The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data backup processes, and recovery infrastructure to meet its objectives.			
The company relies on GCP's physical and environmental controls, as defined and tested within GCP SOC 2 efforts.	A1.2.1	Not Applicable - Control is Carved Out	The Criterion is carved out and the responsibility of the subservice organization.
A1.3 - The entity tests recovery plan procedures supporting system recovery to meet its objectives.			
Backups are performed daily and retained in accordance with a pre-defined schedule in the Backup Policy.	A1.3.1	Inspected the Operations Security policy and database configuration to determine that backups are made daily using the infrastructure provider's automated backup service.	No exceptions noted
The entity has documented a disaster recovery plan that is tested annually to ensure that recovery procedures are complete and accurate.	A1.3.2	Inspected the annual disaster recovery exercise to determine that the Company's disaster recovery plan is tested annually to ensure that recovery procedures are complete and accurate.	No exceptions noted
C1.0 - Additional Criteria for Confidentiality			
C1.1 - The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.			
Management has approved the company's security policies, and all employees agree to these procedures. Management also ensures that security policies are accessible to all employees and contractors.	C1.1.1	Inspected the signed security policies for a sample of employees to determine that all employees had agreed to the security policies.	No exceptions noted

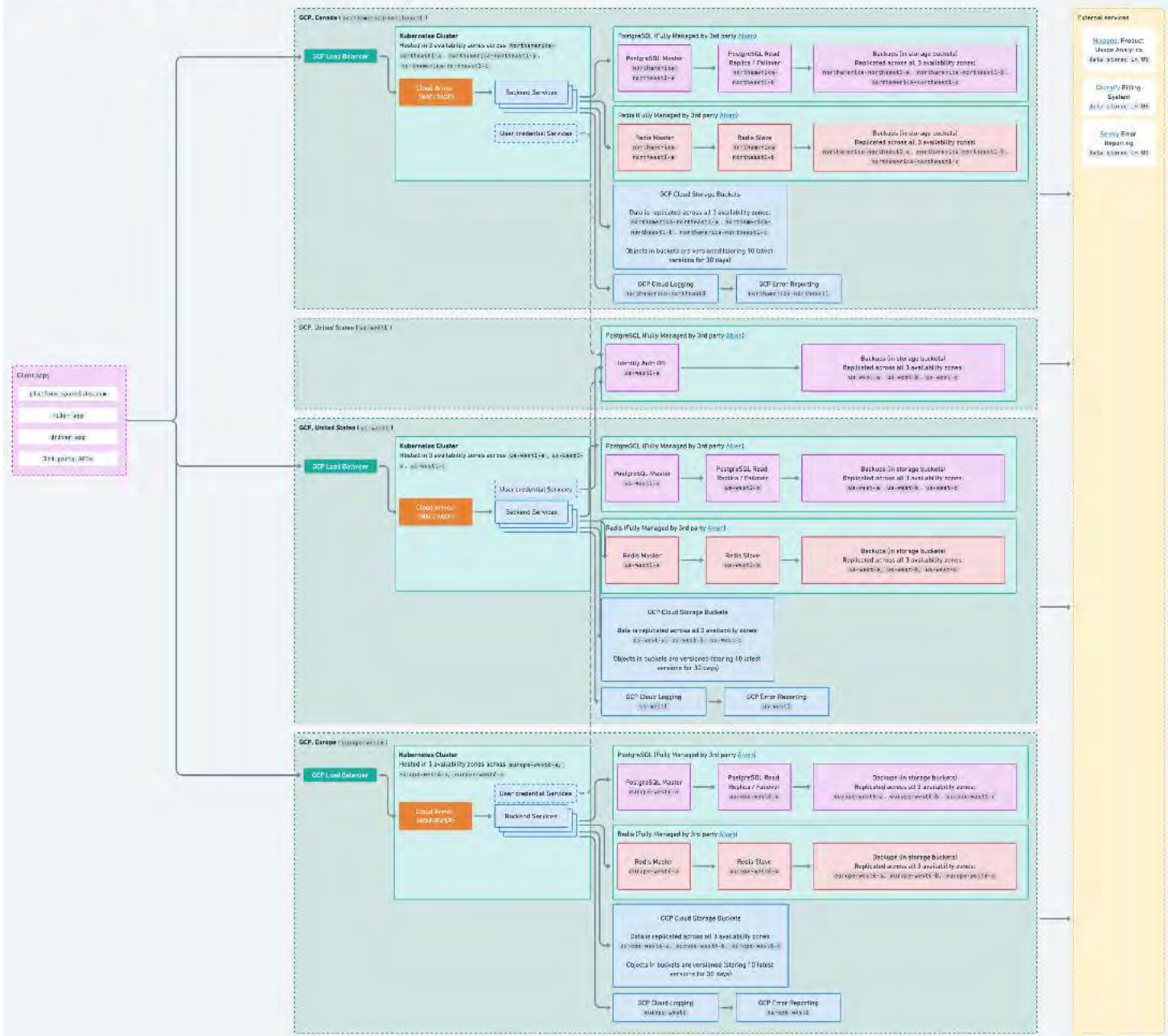


Description of Company Controls	Criteria Number	Service Auditor's Test of Controls	Result
C1.1 - The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.			
Procedures are in place to identify and designate confidential information when it is received or created and to determine the period over which the confidential information is to be retained.	C1.1.2	Inspected the Data Management Policy to determine that procedures are in place to identify and designate confidential information when it is received or created and to determine the period over which the confidential information is to be retained.	No exceptions noted
C1.2 - The entity disposes of confidential information to meet the entity's objectives related to confidentiality.			
Procedures are in place to erase or otherwise destroy confidential information that has been identified for destruction.	C1.2.1	Inspected the Data Management Policy to determine that procedures are in place to erase or otherwise destroy confidential information that has been identified for destruction.	No exceptions noted

Architecture Diagrams

The following two pages are the architectural diagrams of Spare's software system.

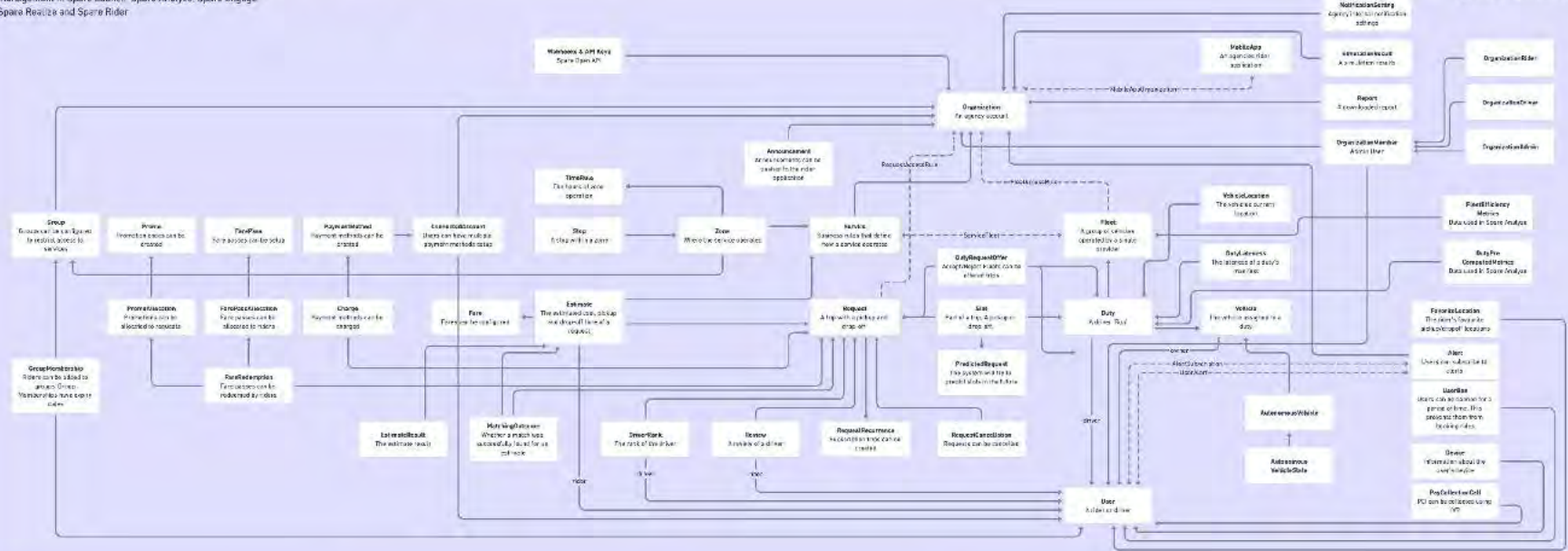
Multi-Region System Design



Spare System Design Diagram

This is the primary data model for powering trips and user management in Spare Launch, Spare Analyze, Spare Engage, Spare Realize and Spare Rider.

Note that some relationships may have been omitted from the diagram for simplification purposes.



CUSTOM SCHEMA SERVICE DATA MODEL

Data model used by the custom schema service for managing custom fields and extending Spare Platform native objects.



GEOGRAPHY SERVICE DATA MODEL

Data model used by the Geography service for managing Geographies.



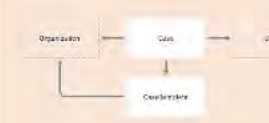
REALIZE SERVICE DATA MODEL

Data model used by the realize service for powering Spare Realize.



ENGAGE SERVICE DATA MODEL

Data model used by the engage service for powering Spare Engage.



OPEN FLEETS SERVICE DATA MODEL

Data model used by the open fleet service for powering Spare Open Fleets.



Cost of Vendor’s Offer (Attachment E)

Spare is a Software as a Service (SaaS) technology company and as such, charges annual recurring fees and one-time fees for project management and associated tasks and implementation tasks. Below is an explanation of how the Spare pricing model works.

We are proposing a simple cost structure while delivering a flexible and scalable offering for the DROs which includes the following:

- Implementation Fee
- Spare Base Platform Fee
- Peak Active Vehicle Variable Fee
- Partner Success Fee

The SaaS Base Fee for the Spare Platform includes annual maintenance, hosting, upgrades, and optimization.

Spare’s Implementation Fee is a one-time cost which relates the resources required for training, setup, and technical implementation. This amount is usually 5% of the total cost, but we’ve waived this fee for all DROs statewide.

Spare’s Base Platform Fee is charged on an annual basis. Our Platform is designed to be scalable and can be extended to enable the DROs to customize the parameters and offerings of their service zones at no additional cost.

Spare charges a Base Platform Fee of \$16,320 annually. This includes annual maintenance, hosting, upgrades, optimization, and 24/7 support (phone, email, and chat).

Our Variable Fee is based on Peak Active Vehicles—enabling DROs to scale easily and be flexible. This is a subscription fee based on the number of vehicles used. The subscription fee is \$2,650 per vehicle per year for any vehicles simultaneously active on the road at once.

Hardware can be provided to DROs as needed at cost plus a 10% markup.

Description	Fee
Spare Platform Package (excludes hardware) Includes base annual maintenance, hosting, upgrades, optimization, and 24/7 support fee, with the following modules: • Spare Realize and Launch • Spare Driver app • White-labeled Rider app • Audit Log	\$16,320 per year

Initial Implementation Fee First-hand Setup, Training, Configuration and Project Management for implementation of Spare technology.	5% of first year total cost - Waived
Spare Partner Success Package • Dedicated Project Manager, Operations Support Staff and Training Staff • Fully managed onboarding & training for staff • Biweekly meetings and quarterly workshops for ongoing optimization • Direct phone number for emergencies/outages	\$9,500 per year
Base per vehicle fee* Additional vehicle feature modules are available to agencies based on their use case which will reflect the ultimate per-vehicle price.	\$2,650 per vehicle/year
Scale discount Applies to the services provided directly by Spare.	0-4 Vehicles: 0% 5-9 Vehicles: 8% 10-19 Vehicles: 17% 20-29 Vehicles: 24% 30-50 Vehicles: 31% 50+ Vehicles: 38%

Travel and Custom Work

Item	Charge Rate
Travel (Airfare / Ground) / Accommodation / Meals	Cost + 10%
Custom development work (agreed upon separately)	\$150 USD/hr

Schedule of Offered Solution

Spare has launched on-demand transit services in as little as 48 hours as a testament to how quickly we can get projects up and running for our clients, though this is not a typical situation. Our Partner Success team is experienced and skilled in project management, having launched dozens of services just in the last few months. The team can support the multitude of demand response software launches under this procurement and their phased approaches for the DROs' services.

Standard timelines range anywhere from one month to six months depending on the integrations, size of the service, specifications needed, scope, intended launch date, availability of the DRO staff to work with Spare, and the size of data to be migrated over. The primary distinguishing feature between the two ranges is the amount of development or integrations that need to be completed for go-live.

Spare will work together with the DROs project team to complete full testing of the DROs' fleet and services within a live system to test real time functionality and to make any adjustments to the service, as needed, prior to service launch. DROs will receive two environments for the duration of our relationship: one for testing and training as well as another for production. Post kick-off, we will work with the DRO team to finalize the implementation schedule and plan.

Please note that implementation timelines is based on the following assumptions:

- Eager and willing DRO project team that can dedicated roughly three hours of meetings a week.
- DRO Project Team is available for training.
- DRO Project Team is willing to work outside of meetings to proactively gather information, set up service details in the platform themselves, and are motivated to have a timely implementation.

This table shows what a schedule would look like as an example of what deliverables, activities, and stakeholders would be involved during each phase. This timeline would increase or decrease based on the various factors mentioned above.

Deliverables	Deployment Activities	Stakeholders
Phase 0: Notice to Proceed and Pre-Kickoff		
✓ Finalized Contract ✓ Agency Service Owner Identified	Phase 0 consists of activities that close out key requirements to begin a partnership together. The beginning of this is getting the project owners and executive sponsors introduced, working on a finalized contract and reviewing any remaining questions from the RFP process/response. This phase typically takes place over multiple calls/meetings to refine and align on the final items before kicking off the new partnership. While each agency has different steps to finalizing contracts, Spare has assumed a duration of around 45-60 days for this step.	Spare Executive Sponsor Growth Manager DRO Legal Counsel Executive Sponsor Project Manager Procurement Manager

Phase 1: Kickoff and Project Planning		
✓ Kickoff Call ✓ Finalized Schedule ✓ Finalized Project Plan/Success Criteria ✓ Confirmed Roles and Responsibilities ✓ Service Data Sent to Spare ✓ White Label Design Assets Sent to Spare (if applicable)	Phase 1 is focused on ensuring the foundation of the partnership is mutually aligned across Spare and the DRO and that we're set up for success throughout the project. This phase consists of multiple touch points that span finalizing this mobilization strategy, agreeing on an implementation schedule/plan, and clearly defining roles and responsibilities across parties. Post-kick off and prior to the first project meeting, Spare will work with the DRO to gather design assets for the white label and service data, such as zone shapefiles, stops (in csv format with stop names and accurate lats/longs), service hours, fare information, accepted payment methods, and vehicle details, to prepare for Phase 2. Throughout this phase, time will also be taken to ensure that overall project success criteria are well defined and clear measurement approaches are established for project milestone/performance tracking.	Spare Project Manager Growth Manager Operations Director DRO Executive Sponsor Project Manager Lyft, Uber, etc. (if trip brokering/Open Fleets is included in scope) Any other subs, incl. DBEs
Phase 2: Service Planning/Modeling and Design		
✓ Service Objectives ✓ Identify Service KPIs ✓ Service Modeling ✓ Service Design ✓ Approve Service Parameters ✓ Integration Scoping (if applicable)	Phase 2 is built to begin the work of service planning and design. This phase helps ensure that Spare fully understands the needs and expectations of the DRO's internal operations and requirements from the agency and riders. Key to the success of this phase is comprehensive scoping, including: • Driver scheduling processes and needs • Trip scheduling processes and needs • Reporting processes and needs • Fare and payment methods processes and needs • Call center processes and needs • Eligibility processes and needs As a starting point to this phase, Spare can complete simulations that provide findings and service expectations using our service planning and simulations tool, Realize. These findings and expectations will be used as a backdrop to support the service design and planning. This phase will culminate in a clear service design that will be created to hit the project/service goals of the DRO and deliver an exceptional rider experience.	Spare Project Manager Operations Director Lead Data Scientist DRO Project Manager Transit Planner
Phase 3: System Setup and Data Provisioning		
✓ System Transition Plan (if applicable)	Phase 3 puts Phase 2 into work and is focused on all of the required platform and data setup for the DRO's services. This phase covers all parts of the service/system setup to ensure the platform is ready for	Spare Project Manager Operations Director Lead Data Scientist

✓ Data Migration Complete (if applicable) ✓ Data Management Plan ✓ Security and Recovery Plan ✓ Risk Assessment ✓ Service Setup & Configuration ✓ Platform Feature Configuration ✓ System ready for end-to-end testing ✓ Final System Setup Approval	the DRO to train, test, and (ultimately) operate. This includes: • Create system transition plan to ensure seamless transition between systems (if applicable only if not a new pilot) • Determine data migration approach and begin execution (if applicable only if not a new pilot) • Develop data management and access approach (including reporting frequency, included metrics, and dashboard) • Develop security and emergency recovery plan • Ensure thorough risk assessment • Set up each service based on approved design parameters • Configure fleets structure • Optimize algorithms around the DRO's service parameters • Localize the system through detailed mapping and traffic modeling • Align product configurations to meet the the DRO's requirements	DRO Project Manager Transit Planner
Phase 4: Training and Education		
✓ User Training and Education ✓ Reference Guides ✓ Training Videos ✓ Training Recordings ✓ Knowledge Articles	Phase 4 is focused on ensuring all required parties at the DRO have the right knowledge of the software, their new workflows, and the updated processes. To achieve this, Spare will conduct training sessions and dry runs for all of the DRO's administrators, dispatchers, schedulers/booking agents, drivers, and data analysts, in advance of service launch. Beyond the defined training, Spare will also provide a robust set of role-specific guides, training recordings, training videos, and knowledge base articles so that self-help is easy and additional training can happen at any time. Spare can also provide direction around how best to ready vehicles for launch, including in-vehicle device setup and installation.	Spare Project Manager Operations Director DRO Project Manager Transit Planner Schedulers/Dispatchers Booking Agents/Reservationists Drivers Lyft, Uber (if trip brokering/Open Fleets is included in scope)
Phase 5: Marketing and Communications		
✓ Marketing & Communications Plan ✓ Stakeholder Engagement ✓ Internal Communications ✓ Rider Communications	Phase 5 is built to ensure Spare and the DRO have a strong internal and external marketing and communications plan in place prior to service launch. The goal here is to ensure all internal and external stakeholders have the right information before and after service launch. Spare will first work with the DRO to identify the marketing and communications objectives of the project along with specific objectives and deliverables. Spare	Spare Project Manager DRO Project Manager Lyft, Uber (if trip brokering/Open Fleets is included in scope)

✓ Service Launch Announcements	will then collaborate with the DRO to develop a marketing and communications strategy that will seek to achieve the project's goals and will market the DRO service to both existing and new transit customers.	
Phase 6: Testing		
✓ Testing Plan Developed ✓ Testing Environments Configured ✓ Desk Testing ✓ User Acceptance Testing ✓ End-to-end Dry Run Tests ✓ Improvements Deployed ✓ System Testing Acceptance	Phase 6 ensures that the service runs as intended across a variety of expected scenarios/situations. These simulations will be both virtual and live (with real drivers and vehicles on the road), and are performed on a broad spectrum of functional tests using a fully localized simulation environment. Spare will work with the DRO to ensure these tests have the right coverage across the service configurations and needs of its drivers, dispatchers, customer service representatives, and riders. Throughout the testing process, Spare will make recommendations on how to further improve the design and setup of the services based on feedback from stakeholders. Some of the key work includes: • Develop a testing plan based on the DRO's unique needs • Configure the testing and simulation environment • Conduct quality assurance and internal "desk" tests of the the DRO's service configurations • Conduct user acceptance testing for the rider application with real riders • Conduct full-scale dry run tests, with real rubber on the road, to test functionalities and ensure staff understand their workflows • Make system adjustments based on testing, as needed	Spare Project Manager Operations Director DRO Project Manager
Phase 7: Pre-Launch		
✓ Final System Acceptance ✓ Final Launch Plan ✓ Validate Data Migrated Successfully ✓ Validate Driver Profiles and Duties ✓ Final System Readiness Checklist ✓ Marketing Plan Execution Underway	Phase 7 builds on Phase 6 and focuses on activities to prepare for the service launch. This phase is focused on any final system configurations and getting approval from the DRO that the system is meeting all its requirements. Spare will also work with the DRO to build and review the launch plan and make sure that all the components inside of it are accurate, ready to go, and all stakeholders are prepared for launch. This phase also focuses on validating that all data migrated successfully (e.g. rider profiles, subscription trips etc.), the systems transition plan has been fully and successfully completed as well as that all driver accounts, platform user accounts, and duties are properly set up in the system.	Spare Project Manager Operations Director DRO Project Manager Transit Planner Lyft, Uber (if trip brokering/Open Fleets is included in scope)
Phase 8: Service Launch		

✓ Marketing Plan Full Execution ✓ System Go Live ✓ Service Review ✓ Early Service Feedback	Phase 8 is the culmination of the earlier phases and is when the service officially goes live. This phase will follow the designed launch plan from Phase 7 and will adapt, as required, based on any real time feedback from the DRO staff and riders. The marketing and communications plan from Phase 5 will be rolled out internally and externally by the DRO, so that the community is aware of the service and how to book and schedule rides based on their needs. The service will be monitored by Spare's Project Manager to ensure that any issues that may arise are handled quickly. Through this process, feedback will be collected so that Spare and the DRO can review and make service changes where improvement opportunities exist.	Spare Project Manager Operations Director DRO Project Manager Transit Planner
Phase 9: Post-Launch Support and Optimization		
Performance reviews completed, which will be shared by Spare and used as a benchmark against collaboratively-determined KPIs.	Phase 9 is an ongoing phase and is not isolated to a defined period of time, as it takes place over the course of our partnership. This work is led by Spare's Project Manager. The Project Team will meet weekly, initially, with the DRO to discuss issues and ongoing optimization and/or expansion plans. Once the service hits maturity, meeting frequency will be reduced. The project staff briefing will cover: • Project status and deliverables • Issue identification and solution resolution • Performance monitoring and optimization • Additional training and process development (where required) • Recommendations to improve service delivery and optimization Spare's Project Manager will host quarterly goal reviews (QGRs) with the DRO to take deep dives into performance and set objectives. We will also assist with creating a plan to achieve the goals that are set. Spare's data science professionals will work with your Project Manager to provide recommendations in optimizing the service further and will periodically conduct market research and analysis of the rider experience through reviews and rider surveys. Spare's product team will also reach out to platform users to gather feedback that feeds into Spare's product development strategy and roadmap.	Spare Growth Manager Project Manager Operations Director Lead Data Scientist Product Manager DRO Project Manager Transit Planner Lyft, Uber (if trip brokering/Open Fleets is included in scope)

Signed Vendor Certification Form (Attachment F)

On the following page is the completed Vendor Certification Form.

ATTACHMENT F: VENDOR CERTIFICATION FORM

1) ELIGIBLE VENDOR

The Vendor certifies that in accordance with N.C.G.S. §143-59.1(b), Vendor is not an ineligible vendor as set forth in N.C.G.S. §143-59.1 (a).

The Vendor acknowledges that, to the extent the awarded contract involves the creation, research, investigation or generation of a future RFP or other solicitation; the Vendor will be precluded from bidding on the subsequent RFP or other solicitation and from serving as a subcontractor to an awarded vendor.

The State reserves the right to disqualify any bidder if the State determines that the bidder has used its position (whether as an incumbent Vendor, or as a subcontractor hired to assist with the RFP development, or as a Vendor offering free assistance) to gain a competitive advantage on the RFP or other solicitation.

2) CONFLICT OF INTEREST

Applicable standards may include: N.C.G.S. §§143B-1352 and 143B-1353, 14-234, and 133-32. The Vendor shall not knowingly employ, during the period of the Agreement, nor in the preparation of any response to this solicitation, any personnel who are, or have been, employed by a Vendor also in the employ of the State and who are providing Services involving, or similar to, the scope and nature of this solicitation or the resulting contract.

3) E-VERIFY

Pursuant to N.C.G.S. § 143B-1350(k), the State shall not enter into a contract unless the awarded Vendor and each of its subcontractors comply with the E-Verify requirements of N.C.G.S. Chapter 64, Article 2. Vendors are directed to review the foregoing laws. Vendors claiming exceptions or exclusions under Chapter 64 must identify the legal basis for such claims and certify compliance with federal law regarding registration of aliens including 8 USC 1373 and 8 USC 1324a. Any awarded Vendor must submit a certification of compliance with E-Verify to the awarding agency, and on a periodic basis thereafter as may be required by the State.

4) CERTIFICATE TO TRANSACT BUSINESS IN NORTH CAROLINA

As a condition of contract award, awarded Vendor shall have registered its business with the North Carolina Secretary of State and shall maintain such registration throughout the term of the Contract.

Signature:  Date: 06 / 14 / 2023

Printed Name: Kristoffer Vik Hansen Title: CEO

Location of Workers Utilized by Vendor Form (Attachment G)

On the following page is the completed Attachment G Form.

ATTACHMENT G: LOCATION OF WORKERS UTILIZED BY VENDOR

In accordance with N.C.G.S. §143B-1361(b), Vendor must identify how it intends to utilize resources or workers located outside the U.S., and the countries or cities where such are located. The State will evaluate additional risks, costs, and other factors associated with the Vendor's utilization of resources or workers prior to making an award for any such Vendor's offer. The Vendor shall provide the following:

- a) The location of work to be performed by the Vendor's employees, subcontractors, or other persons, and whether any work will be performed outside the United States. The Vendor shall provide notice of any changes in such work locations if the changes result in performing work outside of the United States.
- b) Any Vendor or subcontractor providing support or maintenance Services for software, call or contact center Services shall disclose the location from which the call or contact center Services are being provided upon request.

Will Vendor perform any work outside of the United States?

☒ YES ☐ NO

Spare is a Canadian company and the majority of Spare's employees are located in Canada.

References (Attachment H)

GoLink Microtransit and RAP Program | Dallas, Texas

Address: 1401 Pacific Ave, Dallas, Texas 75202

Reference contact: Greg Elsborg, VP and Chief Innovation Officer, 214-749-3434, gelsborg@dart.org

Implementation Timeline: Contract awarded in March 2018. Launch in January 2019. Currently operating.

Products Installed and Operational: Spare Launch, Spare Analyze, Spare Rider, Spare Driver, Spare Engage, Open Fleets

Project Summary: Dallas Area Rapid Transit serves the metropolitan area of Dallas, a geography of 700 square miles and home to 7.5 million people. Within a service area of 13 cities, connecting urban, suburban and rural residents was a challenge. Within this sprawling region, about 28% of all people live more than ¼ mile from a transit stop and 24% of all jobs are more than ¼ mile from a transit stop. Therefore DART selected Spare to bridge this gap by powering a first-mile-last-mile microtransit solution called GoLink.

Spare Platform powers all of DART GoLink's reservations (through the call center and integrated GoPass rider app), scheduling of dedicated vehicles, dispatching and management of dedicated vehicles, trip reservations and automated dispatching to non-dedicated vehicles, as well as reporting, analytics (including an integration with PowerBI), and quality assurance.

GoLink was launched in January 2019 in four zones, which quickly increased to 14 zones upon the service being so highly valued by riders. As of January 2022, GoLink has grown to over 30 zones. Through Spare Platform, DART was able to seamlessly and automatically dispatch non-dedicated TNC and taxi trips to GoLink passengers when a DART-branded dedicated GoLink vehicle could not facilitate the trip in a satisfactory way (for example, if wait times are too high).



To power this service Spare integrated with the GoPass 3.0 app, a MaaS (Mobility as a Service) application that allows DART riders to plan, book, and pay for their journey from end to end. By fully integrating the application with the DART GoLink microtransit service, Spare helped to create the largest public on-demand transit service in North America and a truly multimodal travel planner and ticketing solution across the entire transportation network. Spare's integration with the GoPass 3.0 app for DART GoLink utilizes the full capabilities of Spare Open API. The GoPass 3.0 app is the first time a complete mobility platform has been integrated into an agency-owned tool, combining trip planning, booking, and payment of multi-modal trips (fixed route, on-demand, and third-party trip brokerage) in a seamless interface.

In 2022, Spare took over DART's Rider Assistance Program (RAP), a service handled with only non-dedicated vehicles for registered residents in multiple locations across Dallas, Texas USA. Spare launched our Open Fleets module for DART in October 2022 with Lyft as the primary external fleet. As of December 2022, the service sees 120 boardings each week, an average of 75 daily riders on brokered trips, and a 65 percent of brokered trips overall.

Prior to working with Spare, MV Transportation, DART's dedicated operator, had a hard time hitting a wait time of 15 minutes or less across all of their paratransit trips. Since partnering with Spare on the DART RAP implementation, around 98% of MV Transportation RAP trips have a wait time of 15-mins or less—providing massive performance improvements for DART and MV. The trade-off between rider experience and system efficiency is decided by the Skyss and through our software and team, we can help create a much better rider experience while saving our customers money.

One of the key reasons DART wanted to work with Spare was because of our comprehensive Spare Open API. This allowed DART to seamlessly integrate the GoLink microtransit service into the GoPass app, creating a truly multimodal travel planner and ticketing solution across the entire transportation network. Spare Engine, Spare's flexible routing and pooling algorithm, is able to operate a stop-based service as well as a door-to-door service, which has proved ideal for DART's needs.

Results: With an average of 30,000 boardings a month, Spare has decreased GoLink's operational costs by 26% while maintaining the same excellent service quality, thanks to Spare's ability to dispatch to multiple dedicated and non-dedicated providers, and keeping passenger satisfaction over 95%. The service has provided immense value to transit riders across the region. Plus, by offering a more accessible public transportation service, DART is



reducing the burden on their paratransit service by providing passengers with disabilities the option to use GoLink.

Number of vendor or technical staff: 40 Spare staff

Number of end users: 171,889 total monthly ridership for the past 3 months from GoLink and RAP services.

Number of sites supported: DART is the one operating the software solution.

PSTA Access and PSTA Mobility on Demand | St. Petersburg, FL

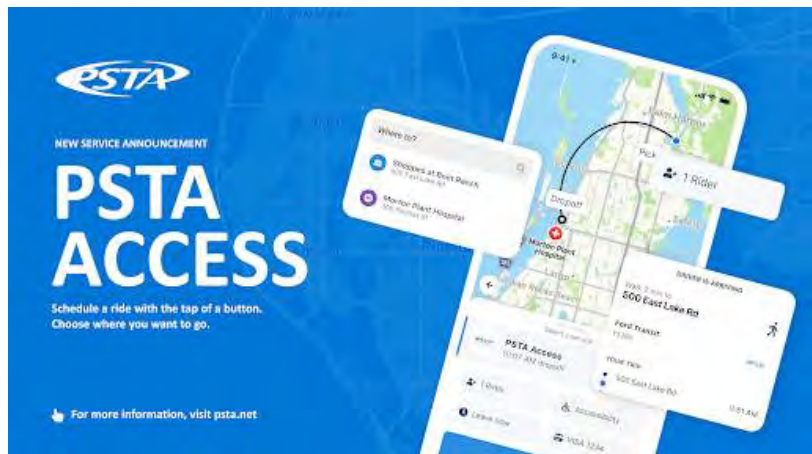
Address: 3201 Scherer Drive, St. Petersburg, Florida, 33716

Reference contact: Bonnie Epstein, Director of Mobility Services, 727-540-1980, bepstein@psta.net

Implementation Timeline: Contract awarded and project kick-off was in June 2021. Launched in December 2021. Currently operating.

Products Installed and Operational: Spare Launch, Spare Analyze, Spare Rider, Spare Driver, Spare Engage, Open Fleets

Project Summary: Spare partnered with Pinellas Suncoast Transit Authority (PSTA) in Florida to deliver game-changing accessible transport to residents in Pinellas County. The County is the most densely populated county in Florida with more than 40% of its nearly 1-million residents reported to have a disability. The County is also home to a high concentration of seniors, making paratransit a vital service in the area.



Serving riders in the St. Petersburg-Clearwater corridor, PSTA's ADA paratransit service, **PSTA Access**, uses Spare Launch to operate its entire ADA paratransit operation, from booking and scheduling to matching and payments. It also leverages Spare's analytics and planning tools to make data-backed decisions about its service. In total, PSTA is running with approximately 70 vehicles in parallel on a day-to-day basis.

Launched in December 2021, Spare successfully carried out a transition from a previous platform (Routematch and Tranware), including the user database migration with all their specific fields, and their service configuration details. Many different overlapped zones were created in order to comply with

Americans with Disabilities Act (ADA) regulations, a set of North American directives for accessible transport or paratransit services. Bookings are centrally managed by PSTA's call center.

Before integrating with Spare's cloud-based software, PSTA reservationists had to connect trip information across multiple systems manually. This made it impossible for reservationists to have a unified view of the operation to ensure operations were running smoothly.

Based on the success of PSTA Access, PSTA expanded its partnership with Spare to include the **Mobility on Demand (MOD)** service in April 2023 to provide same-day trips to Access-eligible riders. MOD uses NDSPs to provide same-day rides to riders who are eligible for paratransit. PSTA sends trips to Lyft and Uber, as well using the new Jagwire and MTI integrations Spare built to send trips to Wheelchair Transport and Bay Area Metro/United Taxi, giving riders four potential providers to choose from. This service provides riders a layer of flexibility and freedom that they wouldn't otherwise have as typically paratransit trips are all scheduled by 5pm the previous day.

With the launch of MOD, PSTA is now using 5 integrations and 6 providers to power 5 different services!

The six different fleet providers include:

- First Transit, acting as the main operator with a fleet of dedicated vehicles. This operator takes care of wheelchair services, and handles bookings directly in the Spare Platform.
- Uzurv, a ride hailing company which developed an API integration to be able to take bookings and manage trips from their own interface
- Bay Area Metro/United Taxi, a taxi company that acts as a non-dedicated fleet, and automatically gets assigned ambulatory trips that cannot be accommodated in the dedicated fleet. Bay Area Metro works with a custom built system which does not allow for API integrations. Instead, Spare created a separate environment with a shared fleet integrated into PSTA's organization, for them to manage only the trips that are assigned to their operation.
- Lyft and Uber, the popular ride sharing platforms for which Spare has a native integration with both act as non-dedicated fleet options
- Wheelchair Transport, a non-dedicated fleet, providing wheelchair-accessible vehicles

Across all of these fleet providers, Spare Platform is responsible for trip reservations, scheduling, and automated dispatching to both dedicated and non-dedicated vehicles to deliver a unified paratransit service for PSTA.

PSTA's deployment of Spare Open Fleets to connect six separate fleets is an industry first. By incorporating these native integrations into Spare's mobility management platform, Spare can now provide transit agencies access to nearly 90% of all bookable vehicles in North America to boost their microtransit and paratransit services.

Results: During this implementation, Spare migrated roughly 4,700 rider profiles from Routematch to Spare, an example of Spare's ability to transition large paratransit services from their previous software onto Spare. Today this service delivers more than 1,200 trips per day. Since launching, 13,811 ADA

paratransit trips are powered by Spare each month for PSTA Access. Below is feedback from a PSTA Access rider showing the benefits of switching to Spare.

Finally an PSTA app which enables a great deal of resources. Extremely helpful and much much much less phone calls to dispatch.

PSTA app tells me estimated time driver in minutes. I'm also able to track the driver on the app map within five minutes up to the initial arrival time to the destination, gives me the drivers name. I can view my trips up to a week in advance. I can greet the driver by name.

Launched in December 2021, Open Fleets has brokered more than 20% of trips to the primary non-dedicated fleet, Uzurv. The result is the ability for PSTA to book FTA-compliant paratransit trips and provide comprehensive reporting that includes real-time data associated with trip execution and reporting information. With each month that passes, the rate increases as riders switch from traditional paratransit to the mobility on demand service that includes the non-dedicated fleet. In 2022, PSTA saw an increase of more than 25% with an average weekday ridership (past month) of 650 riders. This saw a reduction in cost per trip: from \$40.78/trip in May 2022 to \$36.58/trip in November 2022 which equals a 10.3% reduction in 6 months.

Open Fleets continues to save PSTA money; since August 2022, PSTA has received about 8,800 app bookings. In the last few weeks, the proportion of app bookings on the service has reached 15%, which is enormous for a paratransit service. Assuming that each app booking saves PSTA an average of 2 minutes of a booking agent's time, we have saved 17,600 minutes (293 hours) of agent booking time.

This translates to over \$5,000 in saved booking agent time.

The MOD service has been doing over 4,000 weekly rides since its launch. This indicates the transition has been smooth with the switch to Spare as there wasn't any reduction in MOD trips when comparing pre-Spare numbers.



"We pride ourselves on being an innovative transit agency that delivers a variety of options to our low-mobility and older riders. Spare helps propel the innovation of PSTA Access by allowing us to centralise our operations and ultimately deliver a better customer experience,"

— Bonnie Epstein, Director of Mobility Services, PSTA

Number of vendor or technical staff: 40 Spare staff

Number of end users: 85,589 total monthly ridership for the past 3 months from all PSTA services.

Number of sites supported: PSTA is the one operating the software solution.

Citibus On-Demand and CitiAccess, Lubbock, Texas

Address: 801 Texas Avenue, Lubbock, TX 79401

Reference contact: Chris Mandrell, General Manager, 806-775-3435, cmandrell@citibus.com

Implementation Timeline: Contract awarded and project kick-off was in April 2020. Launched in May 2020. Currently operating.

Products Installed and Operational: Spare

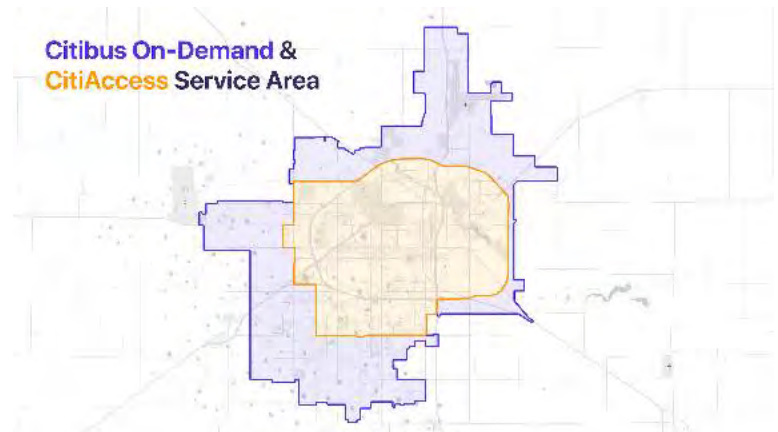
Launch, Spare Analyze, Spare Rider, Spare Driver, Spare Engage, Open Fleets

Project Summary: Before partnering with Spare, Citibus operated its paratransit and NEMT services through a legacy system. The agency wanted to adopt automation, on-duty optimization, and data-driven planning to improve efficiency and the passenger experience. It also had a limited, nighttime-only demand-response service called Citibus NiteRide, which ran as a stand-alone service from its paratransit.

Citibus was launched initially in response to COVID-19 to provide a general public on-demand system because of their reduction in fixed-route schedules. Soon after, Citibus decided to use Spare to transition their paratransit system CitiAccess from their legacy paratransit software, Trapeze, at the same time. Thanks to Spare's optimization processes and delayed matching, Citibus was able to realize extensive operational efficiencies and reduce wait times by implementing Spare Platform for paratransit. It was also decided that the microtransit and paratransit service would share the same fleet of vehicles to reduce their operating costs using Spare's commingling fleets feature.

Spare met the anticipated project schedule where the project was kicked-off on April 20, 2020 and launched on May 20, 2020 with the service design completed in 1 month. The Citibus implementation was one of Spare's quickest and required all hands on deck and daily meetings, but was accomplished in record time, according to plan. This could not have been accomplished without the dedication of the Citibus team.

Results: After it relaunched paratransit and microtransit with Spare, Citibus witnessed a 200% increase in ridership at the peak, with a swift ramp-up in the first 4 weeks despite of COVID-19.



This was a result of switching from manual booking and processes to an automated approach. Riders can now book their transit either ahead of time or the same-day through a smartphone app. They can also continue to call Citibus dispatch and still book real-time on-demand transportation.

Through commingling, the agency also realized a return on investment (ROI) of 3.8% and is forecasted to save approximately \$3 per trip versus the legacy parallel system. Citibus commingles 25% (percentage of all trips) of their 10,000 monthly riders. This approach allowed Citibus to expand microtransit, filling in gaps caused by cuts to fixed-route timetables due to COVID-19.

Switching to Spare also allowed Citibus to use our advanced algorithm in the backend to better assign customers to rides. This creates efficient self-serve dispatching by optimizing across multiple fleets to enable the most efficient ride—accounting for individual criteria. Citibus' rigid legacy system gave little to no insight into ride data once they were dispatched, thus causing a 75% On-Time Performance (OTP). By switching to Spare, Citibus achieved an OTP of 94% and expanded the service area to cover 100% of the city limits. Chris Mandrell, GM Citibus, no longer receives complaints about rides being late and has been able to expand the positive impact of Citibus with service area expansion.



"It's extremely easy to get started with Spare. We signed the contract and three weeks later we were up and running. Our drivers went home one day working out of Trapeze and showed up the next working out of Spare. The transition was super simple." — Chris Mandrell, General Manager at Citibus.

Number of vendor or technical staff: 40 Spare staff

Number of end users: 34,771 total monthly ridership for the past 3 months.

Number of sites supported: Citibus is the one operating the software solution.

Financial Statements (Attachment I)

On the following page is the completed Financial Review Form with copies of our financial statements for the past 3 years as a privately held company.

ATTACHMENT I: FINANCIAL REVIEW FORM

Vendor shall review the Financial Review Form, provide responses in the gray-shaded boxes, and submit the completed Form as an Excel file with its offer. Vendor shall not add or delete rows or columns in the Form, or change the order of the rows or column in the file.

1. Vendor Name: Spare Labs Inc.
2. Company structure for tax purposes (C Corp, S Corp, LLC, LLP, etc.): Corporation
3. Have you been in business for more than three years? ☒ Yes ☐ No
4. Have you filed for bankruptcy in the past three years? ☐ Yes ☒ No
5. In the past three years, has your auditor issued any notification letters addressing significant issues? If yes, please explain and provide a copy of the notification letters. ☐ Yes ☒ No
6. Are the financial figures below based on audited financial statements? ☐ Yes ☒ No
7. Start Date of financial statements: December 31, 2020
End Date of financial statements: December 31, 2022
8. Provide a link to annual reports with financial statements and management discussion for the past three complete fiscal years:
9. Provide the following information for the past three complete fiscal years:

	Latest complete fiscal year minus two years	Latest complete fiscal year minus one year	Latest complete fiscal year
BALANCE SHEET DATA			
a. Cash and Temporary Investments	3,983,386	18,696,598	13,334,009
b. Accounts Receivable (beginning of year)	395,467	319,349	852,241
c. Accounts Receivable (end of year)	319,349	852,241	1,961,796
d. Average Account Receivable for the Year (calculated)	357,408	585,795	1,407,019
e. Inventory (beginning of year)	0	0	0
f. Inventory (end of year)	0	0	0
g. Average Inventory for the Year (calculated)	0	0	0
h. Current Assets	4,828,157	20,298,926	16,343,427
i. Current Liabilities	629,414	1,304,135	1,603,260
j. Total Liabilities	669,414	1,304,135	1,603,260
k. Total Stockholders' Equity (beginning of year)	5,542,618	4,849,535	20,403,946
l. Total Stockholders' Equity (end of year)	4,849,535	20,403,946	16,181,826
m. Average Stockholders' Equity during the year (calculated)	5,196,077	12,626,741	18,292,886
INCOME STATEMENT DATA			
a. Net Sales	1,785,382	3,442,821	7,247,788
b. Cost of Goods Sold (COGS)	462,984	1,129,923	3,752,991
c. Gross Profit (Net Sales minus COGS) (calculated)	1,322,398	2,312,898	3,494,797
d. Interest Expense for the Year	0	0	0
e. Net Income after Tax	-693,084	-2,519,381	-4,956,914
f. Earnings for the Year before Interest & Income Tax Expense	-1,178,100	-2,530,544	-5,312,983
STATEMENT OF CASH FLOWS			
a. Cash Flow provided by Operating Activities	-733,957	-2,239,910	-5,744,177
b. Capital Expenditures (property, plant, equipment)	-22,252	-100,329	-177,163

SPARE LABS INC.

Non-Consolidated Financial Statements
December 31, 2022
(Unaudited)

<u>Index</u>	<u>Page</u>
Independent Practitioners' Review Engagement Report	1
Financial Statements	
Non-Consolidated Balance Sheet	2
Non-Consolidated Statement of Operations and Deficit	3
Non-Consolidated Statement of Cash Flows	4
Notes to Non-Consolidated Financial Statements	5 - 17

INDEPENDENT PRACTITIONERS' REVIEW ENGAGEMENT REPORT

TO THE SHAREHOLDERS OF SPARE LABS INC.

We have reviewed the accompanying non-consolidated financial statements of Spare Labs Inc. (the "Company") that comprise the non-consolidated balance sheet as at December 31, 2022 and the non-consolidated statements of operations and deficit and cash flows for the year then ended, and a summary of significant accounting policies and other explanatory information.

Management's Responsibility for the Non-Consolidated Financial Statements

Management is responsible for the preparation and fair presentation of these non-consolidated financial statements in accordance with Canadian accounting standards for private enterprises, and for such internal control as management determines is necessary to enable the preparation of non-consolidated financial statements that are free from material misstatement, whether due to fraud or error.

Practitioners' Responsibility

Our responsibility is to express a conclusion on the accompanying non-consolidated financial statements based on our review. We conducted our review in accordance with Canadian generally accepted standards for review engagements, which require us to comply with relevant ethical requirements.

A review of non-consolidated financial statements in accordance with Canadian generally accepted standards for review engagements is a limited assurance engagement. The practitioners perform procedures, primarily consisting of making inquiries of management and others within the entity, as appropriate, and applying analytical procedures, and evaluate the evidence obtained.

The procedures performed in a review are substantially less in extent than, and vary in nature from, those performed in an audit conducted in accordance with Canadian generally accepted auditing standards. Accordingly, we do not express an audit opinion on these non-consolidated financial statements.

Conclusion

Based on our review, nothing has come to our attention that causes us to believe that the non-consolidated financial statements do not present fairly, in all material respects, the financial position of Spare Labs Inc. as at December 31, 2022, and the results of its operations and its cash flows for the year then ended in accordance with Canadian accounting standards for private enterprises.

Emphasis of Matter

Without modifying our opinion, we draw attention to note 2 to the non-consolidated financial statements which describes that Spare Labs Inc. adopted Canadian accounting standards for private enterprises on January 1, 2022 with a transition date of January 1, 2021. These standards were applied retrospectively by management to the comparative information in these non-consolidated financial statements, including the balance sheets as at December 31, 2021 and January 1, 2021, and the non-consolidated statements of operations and deficit and cash flows for the year ended December 31, 2021 and related disclosures. We were not engaged to report on the restated comparative information, and as such, it is unaudited and not subject to review.

Smythe LLP

Chartered Professional Accountants

Vancouver, British Columbia
May 30, 2023

VANCOUVER

1700-475 Howe St
Vancouver, BC V6C 2B3
T: 604 687 1231
F: 604 688 4675

1

LANGLEY

600-19933 88 Ave
Langley, BC V2Y 4K5
T: 604 282 3600
F: 604 357 1376

NANAIMO

201-1825 Bowen Rd
Nanaimo, BC V9S 1H1
T: 250 755 2111
F: 250 984 0886

SPARE LABS INC.
Non-Consolidated Balance Sheet
December 31
(Unaudited)

	December 31, 2022	December 31, 2021 (note 2)	January 1, 2021 (note 2)
Assets (note 16)			
Current			
Cash and cash equivalents	\$ 13,334,009	\$ 18,696,598	\$ 3,983,386
Accounts receivable (note 5)	1,961,796	852,241	319,349
Income taxes receivable (note 15)	740,087	556,684	481,619
Prepaid expenses and deposits	307,535	193,403	43,803
	16,343,427	20,298,926	4,828,157
Restricted cash (note 6)	701,567	573,298	-
Furniture and equipment (note 7)	138,342	107,807	89,042
Investment in subsidiary (note 8)	-	126,300	-
Investment subject to significant influence (note 9)	601,750	601,750	601,750
	\$ 17,785,086	\$ 21,708,081	\$ 5,518,949

Liabilities

Current			
Accounts payable and accrued liabilities (note 10)	\$ 747,982	\$ 389,173	\$ 87,438
Deferred revenue	855,278	914,962	541,976
	1,603,260	1,304,135	629,414
Canada Emergency Business Account ("CEBA") loan	-	-	40,000
	1,603,260	1,304,135	669,414

Shareholders' equity

Capital stock (note 11)	23,658,663	23,551,390	6,022,757
Contributed surplus (note 12)	1,172,680	545,159	-
Deficit	(8,649,517)	(3,692,603)	(1,173,222)
	16,181,826	20,403,946	4,849,535
	\$ 17,785,086	\$ 21,708,081	\$ 5,518,949

Commitment (note 13)

Approved by the Board

_____ Director

See notes to non-consolidated financial statements

SPARE LABS INC.**Non-Consolidated Statement of Operations and Deficit****Year Ended December 31****(Unaudited)**

	2022	2021 (note 2)
Sales (note 5)	\$ 7,247,788	\$ 3,442,821
Cost of sales	3,752,991	1,129,923
Gross margin	3,494,797	2,312,898
Expenses		
Sales and marketing	4,358,181	2,190,979
General and administrative	2,274,905	1,575,796
Research and development (note 15)	1,400,625	414,274
Product	505,298	297,802
	8,539,009	4,478,851
Loss before other items	(5,044,212)	(2,165,953)
Other items		
Gain on foreign exchange	659,048	268,961
Interest and other income	356,069	11,163
Writedown of investment in subsidiary (note 8)	(136,132)	-
Stock based compensation (note 12)	(645,059)	(551,988)
Amortization	(146,628)	(81,564)
	87,298	(353,428)
Net loss for year	(4,956,914)	(2,519,381)
Deficit, beginning of year	(3,692,603)	(1,173,222)
Deficit, end of year	\$ (8,649,517)	\$ (3,692,603)

See notes to non-consolidated financial statements

SPARE LABS INC.**Non-Consolidated Statement of Cash Flows
Year Ended December 31
(Unaudited)**

	2022	2021 (note 2)
Operating activities		
Net loss	\$ (4,956,914)	\$ (2,519,381)
Items not involving cash		
Amortization	146,628	81,564
Bad debt	102,868	1,203
Unrealized gain on foreign exchange	(659,048)	(268,961)
Stock-based compensation (note 12)	645,059	551,988
Writedown of investment in subsidiary (note 8)	136,132	-
	(4,585,275)	(2,153,587)
Changes in non-cash working capital		
Accounts receivable	(1,167,194)	(534,095)
Income taxes	(183,403)	(75,065)
Prepaid expenses and deposits	(114,132)	(149,600)
Accounts payable and accrued liabilities	365,511	299,451
Deferred revenue	(59,684)	372,986
	(1,158,902)	(86,323)
Cash used in operating activities	(5,744,177)	(2,239,910)
Investing activities		
Restricted cash	(128,269)	(573,298)
Purchase of furniture and equipment	(177,163)	(100,329)
Increase in investment in subsidiary	(9,832)	(126,300)
Cash used in investing activities	(315,264)	(799,927)
Financing activities		
Repayment of CEBA loan	-	(40,000)
Issuance of capital stock	89,735	17,521,804
Cash provided by financing activities	89,735	17,481,804
Effects of exchange rate changes on cash and cash equivalents	607,117	271,245
Inflow (outflow) of cash and cash equivalents	(5,362,589)	14,713,212
Cash and cash equivalents, beginning of year	18,696,598	3,983,386
Cash and cash equivalents, end of year	\$ 13,334,009	\$ 18,696,598
Cash and cash equivalents consist of:		
Cash	\$ 3,873,837	\$ 18,137,585
Guaranteed investment certificates	9,460,172	559,013
	\$ 13,334,009	\$ 18,696,598
Supplemental cash flow information		
Unrealized foreign exchange gain on accounts receivable	\$ 45,229	\$ -
Unrealized foreign exchange gain (loss) on accounts payable	6,702	(2,284)

See notes to non-consolidated financial statements

SPARE LABS INC.

Notes to Non-Consolidated Financial Statements

Year Ended December 31, 2022

(Unaudited)

1. OPERATIONS

Spare Labs Inc. (the "Company") was incorporated under the *Business Corporations Act* of British Columbia on November 3, 2015. The Company's principal business activities include the development, sale and support of data-driven mobility platforms exclusive for the transportation industry.

2. IMPACT OF THE CHANGE IN THE BASIS OF ACCOUNTING

Effective January 1, 2022, the Company adopted the standards in Part II of the Canadian Professional Accountants of Canada ("CPA Canada") Handbook: Canadian Accounting Standards for Private Enterprises ("ASPE").

These non-consolidated financial statements are the first financial statements for which the Company has applied ASPE. The non-consolidated financial statements for the year ended December 31, 2022 were prepared in accordance with the accounting principles and provisions set out in First-time Adoption, Section 1500, for first-time adopters of this basis of accounting. Section 1500 requires retrospective application of the accounting standards with certain elective exemptions and limited retrospective exceptions. The impact of adopting these standards was accounted for in deficit at the date of transition, i.e., January 1, 2021. There is no adjustment to the deficit at January 1, 2021.

Previously, the Company prepared its non-consolidated financial statements in accordance with the standards of the CPA Canada Handbook. As a result of the adoption of ASPE, it was determined that cash was understated, accounts receivable was understated, deferred revenue was understated, capital stock was understated, and contributed surplus was understated as at December 31, 2021, and subscription revenue was understated, foreign exchange gain was understated, and stock-based compensation expense was understated for the year ended December 31, 2021.

The adoption of these standards had the following impacts on the Company's non-consolidated financial statements in the prior period:

Non-Consolidated Balance Sheet

	December 31, 2021 (As previously stated)	Adjustment	December 31, 2021 (Restated)
Assets			
Cash and cash equivalent	\$ 18,423,275	\$ 273,323	\$ 18,696,598
Accounts receivable	752,875	99,366	852,241
Liability			
Deferred revenue	828,156	86,806	914,962
Shareholders' equity			
Capital Stock	23,581,847	(30,457)	23,551,390
Contributed surplus	-	545,159	545,159
Deficit	3,463,785	228,818	3,692,603

SPARE LABS INC.**Notes to Non-Consolidated Financial Statements****Year Ended December 31, 2022****(Unaudited)****2. IMPACT OF THE CHANGE IN THE BASIS OF ACCOUNTING — continued****Non-Consolidated Statement of Operations and Deficit**

	December 31, 2021 (As previously stated)	Adjustment	December 31, 2021 (Restated)
Revenue			
Sales	\$ 3,430,261	\$ 12,560	\$ 3,442,821
Gain on foreign exchange	(41,648)	310,609	268,961
Expenses			
Stock-based compensation expense	-	551,987	551,987

Non-Consolidated Statement of Deficit

	December 31, 2021 (As previously stated)	Adjustment	December 31, 2021 (Restated)
Beginning balance	\$ (1,173,222)	-	\$ (1,173,222)
Net loss	(2,290,563)	(228,818)	(2,519,381)
Ending balance	\$ (3,463,785)	(228,818)	\$ (3,692,603)

3. SIGNIFICANT ACCOUNTING POLICIES

These financial statements are prepared in accordance with Canadian ASPE and include the following significant accounting policies.

(a) Revenue recognition

Revenues consist of software subscriptions, management fees, operation fees, and one-time services fees.

- (i) Revenue for software subscriptions are recognized monthly as services are provided or equally over the term of the contract primarily commencing with the date the services are made available to customers. Additional usage-based subscription fees are recognized in the month services are rendered. Amounts received for future services are recorded as deferred revenue and the balance will be recognized as revenue as the services are rendered.
- (ii) Management fees, operation fees, and one-time services fees are recognized when services are rendered and collection is reasonably assured.

SPARE LABS INC.

Notes to Non-Consolidated Financial Statements

Year Ended December 31, 2022

(Unaudited)

3. SIGNIFICANT ACCOUNTING POLICIES — continued

(b) Cash and cash equivalents

Cash and cash equivalents include cash and short-term investments with maturities of three months or less from their date of acquisition, which are readily convertible into a known amount of cash, and are subject to an insignificant risk to changes in their fair value.

(c) Furniture and equipment

Furniture and equipment are recorded at cost and are being amortized over their estimated useful lives. The annual amortization rates and methods are as follows:

Computer equipment	100% declining balance
Furniture and fixtures	20% declining balance
Equipment	20% declining balance

(d) Impairment of long-lived assets

A long-lived asset is tested for recoverability whenever events or changes in circumstances indicate that its carrying amount may not be recoverable. An impairment loss is recognized when the carrying amount of the asset exceeds the sum of the undiscounted cash flows resulting from its use and eventual disposition. The impairment loss is measured as the amount by which the carrying amount of the long-lived asset exceeds its fair value. Any impairment results in a write-down of the asset and a charge to income during the year. An impairment loss is not reversed if the fair value of the related long-lived asset subsequently increases.

(e) Investment in subsidiary

The Company records its investment in the subsidiary at cost. When there is an indication of impairment, and such an impairment is determined to have occurred, the carrying amount is reduced to the greater of the discounted future cash flows expected or the proceeds that could be realized from sale. Such impairments can be subsequently reversed if value subsequently improves.

(f) Investment subject to significant influence

Investment in an entity upon which the Company exerts significant influence is accounted for by the cost method under which the investment is carried at the cost thereof and the net earnings of the investment are reflected in the determination of the net earnings of the Company only to the extent of dividends received or receivable. When there is an indication of impairment, and such an impairment is determined to have occurred, the carrying amount is reduced to the greater of the discounted future cash flows expected or the proceeds that could be realized from sale. Such impairments can be subsequently reversed if value subsequently improves.

SPARE LABS INC.

Notes to Non-Consolidated Financial Statements

Year Ended December 31, 2022

(Unaudited)

3. SIGNIFICANT ACCOUNTING POLICIES — continued

(g) Stock-based compensation

For directors and employees, the fair value of the options is measured at the date of grant. For non-employees, the fair value of the options is measured on the earlier of the date at which the counterparty performance is completed or the date the performance commitment is reached or the date at which the equity instruments are granted if they are fully vested and non-forfeitable. The fair value is estimated using the Black-Scholes option pricing model taking into account the terms and conditions upon which the options were granted and using market related inputs at the grant date. The fair value of the options is accrued and charged to operations, with the offset credit to contributed surplus. For directors and employees, the fair value of the options is recognized over the vesting period, and for non-employees the fair value of the options is recognized over the related service period.

If and when the stock options are ultimately exercised, the recorded amounts in contributed surplus are transferred to capital stock. Where the terms and conditions of options are modified, the increase in the fair value of the options, measured immediately before and after the modification, is charged to profit or loss.

(h) Research and development costs

Research costs are charged as expenses in the period in which they are incurred.

Development costs are charged as expenses in the period incurred unless the Company believes a development project meets generally accepted criteria for capitalization and amortization, at which time they are capitalized as intangible assets. Capitalized project development expenditures are amortized over the expected future life of the product to which they relate once product revenues are recorded. These costs are reviewed on an annual basis and an impairment loss is recognized when the carrying amount of the asset exceeds the sum of the undiscounted cash flows resulting from its use or eventual disposition.

(i) Income taxes

The Company has elected to account for income taxes using the taxes payable method. The taxes payable and provision for income taxes are based on the corporate income tax returns filed. There is no adjustment for income taxes related to temporary differences and no recognition of the benefit of income tax losses carried forward.

SPARE LABS INC.

Notes to Non-Consolidated Financial Statements

Year Ended December 31, 2022

(Unaudited)

3. SIGNIFICANT ACCOUNTING POLICIES — continued

(j) Government assistance and investment tax credits

The Company receives government grants for certain eligible operations. Grants received for general operations are recorded as revenue in the period received. Grants received as a reimbursement for specific events are recorded as a reduction of the related expense.

Investment tax credits are recorded using the cost reduction approach. Investment tax credits related to current research and development expenditures are included in net loss as a reduction of the related expense.

Investment tax credits are accrued on qualified expenditures when there is reasonable assurance that the credit will be realized. The investment tax credits are subject to review and audit by the Canada Revenue Agency ("CRA"). Although the Company has used its best judgment and understanding of the related income tax legislation in determining the amounts and timing of investment tax credits, it is possible that the amounts could change by a material amount depending on any future review and audit by CRA.

(k) Foreign currency translation

Amounts recorded in foreign currency are translated into Canadian dollars as follows:

- (i) Monetary assets and liabilities, at the rate of exchange in effect at the balance sheet date;
- (ii) Non-monetary assets and liabilities, at the rate of exchange prevailing at the time of the acquisition of the assets or assumption of the liabilities; and
- (iii) Revenues and expenses are translated at the rate of exchange on the transaction date.

Gains and losses arising from the translation of foreign currency are included in net income for the year.

(l) Use of estimates

The preparation of these financial statements in conformity with ASPE requires management to make estimates and assumptions that affect the reported amounts of assets and liabilities, the disclosure of contingent assets and liabilities at the date of the financial statements, and the reported amounts of revenues and expenses during the reporting period. Significant estimates include the collectability of accounts receivable, useful lives of furniture and equipment, completeness of accrued liabilities, inputs used in the calculation of stock-based compensation expense, and estimated scientific research and experimental development tax credit. While management believes these estimates are reasonable, actual results could differ from those estimates and could impact future results of operations and cash flows.

SPARE LABS INC.

Notes to Non-Consolidated Financial Statements

Year Ended December 31, 2022

(Unaudited)

3. SIGNIFICANT ACCOUNTING POLICIES — continued

(m) Financial instruments

The Company initially measures its financial assets and liabilities at fair value, except for certain non-arm's length transactions.

The Company subsequently measures all its financial assets and financial liabilities at amortized cost.

Financial assets measured at amortized cost include cash and cash equivalents, restricted cash, and accounts receivable.

Financial liabilities measured at amortized cost include accounts payable, deferred revenue, and CEBA loan.

The Company has not designated any financial asset or financial liability to be measured at fair value.

4. FINANCIAL INSTRUMENTS

(a) Currency risk

Currency risk is the risk that the fair value or future cash flows of a financial instrument will fluctuate because of changes in foreign exchange rates.

The Company is exposed to currency risk in respect of its cash, accounts receivable, and accounts payable and accrued liabilities that are denominated in US dollars and other foreign currencies. The Company does not use derivative instruments to manage this risk.

As at December 31, 2022, the Company has the following US dollar and other foreign currencies balances at their Canadian dollar equivalent:

	December 31, 2022	December 31, 2021	January 1, 2021
Cash and cash equivalents	\$ 7,806,254	\$ 11,942,684	\$ 863,357
Accounts receivable	935,348	375,786	257,511
Accounts payable	(321,748)	(80,279)	(18,262)

(b) Credit risk

Credit risk is the risk that one party to a financial instrument will cause a financial loss for the other party by failing to discharge an obligation.

The Company is exposed to credit risk with respect to its cash and cash equivalents. The Company has mitigated this risk by holding this instrument with a major financial institution.

The Company is also exposed to credit risk with respect to its accounts receivable. The Company has mitigated this risk by entering into contracts with credit-worthy counterparties.

SPARE LABS INC.**Notes to Non-Consolidated Financial Statements****Year Ended December 31, 2022****(Unaudited)****4. FINANCIAL INSTRUMENTS — continued****(c) Liquidity risk**

Liquidity risk is the risk that the Company will encounter difficulty in meeting obligations associated with financial liabilities.

The Company is exposed to this risk mainly in respect of its accounts payable and accrued liabilities. The Company relies on cash provided from operating activities and funds raised from financing activities to provide sufficient funds to meet future obligations as they come due.

5. RELATED COMPANY TRANSACTIONS

During the year, the Company charged \$715,268 (2021 - \$386,716) in sales from Spare Technology Solutions Inc, an investment subject to significant influence. Included in accounts receivable was \$317,877 (December 31, 2021 - \$nil; January 1, 2021 - \$nil) due from this related party.

These transactions are in the normal course of operations and have been valued in these financial statements at the exchange amount which is the amount of consideration established and agreed to by the related parties.

6. RESTRICTED CASH

Restricted cash is collateral cash being held as a security for a letter of credit available to the Company (note 16). Restricted cash is in the form of a guaranteed investment certificate that is redeemable and earns interest at prime rate.

7. FURNITURE AND EQUIPMENT

	December 31, 2022		December 31, 2021		January 1, 2021
			(note 2)		(note 2)
	Cost	Accumulated amortization	Net	Net	Net
Computer equipment	\$ 386,165	\$ 297,589	\$ 88,576	\$ 45,597	\$ 11,280
Furniture and fixtures	107,702	59,535	48,167	60,215	75,263
Equipment	2,775	1,176	1,599	1,995	2,499
	\$ 496,642	\$ 358,300	\$ 138,342	\$ 107,807	\$ 89,042

SPARE LABS INC.**Notes to Non-Consolidated Financial Statements****Year Ended December 31, 2022****(Unaudited)****8. INVESTMENT IN SUBSIDIARY**

The Company has 100% interest in Spare Labs Europe S.L. During the year, the Company has determined that an impairment of \$136,132 exists. This amount has been recognized in income as an impairment loss.

9. INVESTMENT SUBJECT TO SIGNIFICANT INFLUENCE

The Company holds 49% (December 31, 2021 - 49%; January 1, 2021 - 49%) interest in Spare Technology Solutions Inc.

10. GOVERNMENT REMITTANCES

Included in accounts payable and accrued liabilities is government remittances payable of \$80,661 (December 31, 2021 - \$55,007; January 1, 2021 - \$nil).

11. CAPITAL STOCK AND SHARE PURCHASE WARRANTS

	December 31, 2022	December 31, 2021 (note 2)	January 1, 2021 (note 2)
Issued and outstanding			
10,280,469 (2021 - 10,220,252) Voting common shares	\$ 6,174,036	\$ 6,066,763	\$ 6,022,757
3,455,636 (2021 - 3,455,636) Series A voting, non-redeemable preferred shares	17,484,627	17,484,627	-
	\$ 23,658,663	\$ 23,551,390	\$ 6,022,757

During the year, the Company issued 60,217 (2021 - 151,542) common shares for gross proceeds of \$89,735 (2021 - \$37,177), and \$17,538 (2021 - \$6,829) of contributed surplus was credited to share capital due to the exercise of 60,127 (2021 - 151,542) stock options.

During the year ended December 31, 2021, the Company issued 3,455,636 Series A preferred shares for gross proceeds of \$17,484,627.

The preferred shares are non-cumulative and are convertible into common shares at the holder's option or automatically convertible upon the closing of a qualified initial public offering resulting in at least USD \$30,000,000 of gross proceeds to the Company, at a conversion ratio of one to one basis subject to proportional adjustments for diluting issues, stock splits and combinations, or stock dividends and distributions.

SPARE LABS INC.

Notes to Non-Consolidated Financial Statements

Year Ended December 31, 2022

(Unaudited)

11. CAPITAL STOCK AND SHARE PURCHASE WARRANTS — continued

Warrants

During the year, the Company issued share purchase warrants in connection with the credit facility agreement with Silicon Valley Bank Canada ("SVB") (note 16). SVB received a right to purchase 31,304 common shares for USD \$1.46 per share by March 22, 2034. During the year, no warrant was exercised.

At December 31, 2022, the Company has outstanding warrants as follows:

Warrants outstanding	Exercise price	Warrants exercisable at December 31, 2022	Expiry date
31,304	USD \$1.46	23,478	March 22, 2034

Total compensation recognized in net loss for stock-based compensation is \$40,077 (2021 - \$nil). This amount is credited to contributed surplus.

The fair value of each warrant of \$1.71 (2021 - \$nil) is estimated on the date of issuance using the Black-Scholes pricing model with the following factors: exercise price of USD \$1.46, expected dividends of 0%, expected volatility of 100%, risk free interest rate of 2.58%, and expected life of 12 years.

12. STOCK BASED COMPENSATION

The Company has a stock option plan whereby options to acquire common shares may be granted to eligible directors, consultants, officers, and employees, provided that the number of options issued under the plan does not exceed 2,157,599. Stock options are issued at a term and exercise price that is not less than the fair value at the date of the grant.

Stock options granted have a maximum term of ten years. The vesting schedule of stock options granted under the Plan is at the discretion of the Board of Directors, and generally vest over a period of four years.

A summary of the Company's stock option activity is presented below:

SPARE LABS INC.**Notes to Non-Consolidated Financial Statements****Year Ended December 31, 2022****(Unaudited)****12. STOCK BASED COMPENSATION — continued**

	Number
Balance January 1, 2021	881,971
Granted	438,420
Exercised	(151,542)
Forfeited	(247,019)
Balance December 31, 2021	921,830
Granted	468,113
Exercised	(60,217)
Forfeited	(145,632)
Balance December 31, 2022	1,184,094

The exercise price of options outstanding as at December 31, 2022 varies from CAD \$0.01 to USD \$1.46 per share.

The exercise price of some options outstanding on February 28, 2022 have been repriced from original exercise price to USD \$1.46 per share and resulted in an additional stock-based compensation of \$69,848 during the year.

	Exercise price	Number outstanding	Weighted average remaining contractual life	Number exercisable
Options issued at	\$ 0.01	128,750	5.16	128,750
Options issued at	0.15	76,364	5.15	76,364
Options issued at	USD 1.46	978,980	8.31	380,639
		1,184,094	7.77	585,753

Total compensation recognized in net loss for stock-based compensation is \$645,059 (2021 - \$551,988). This amount was credited to contributed surplus.

\$17,538 (December 31, 2021 - \$6,829; January 1, 2021 - \$nil) of contributed surplus was reclassified to capital stock resulting from the exercise of 60,217 (December 31, 2021 - 151,542; January 1, 2021 - nil) stock options.

SPARE LABS INC.**Notes to Non-Consolidated Financial Statements****Year Ended December 31, 2022****(Unaudited)****12. STOCK BASED COMPENSATION — continued**

The fair value of each option grant is estimated on the date of grant using the Black-Scholes option pricing model with the following weighted average factors and resulting fair values:

	2022	2021
Range of exercise price	\$0.01 - \$3.43	\$0.01 - \$3.43
Expected dividends	0.00%	0.00%
Expected volatility	100.00%	100.00%
Risk free interest rate (average)	2.74%	2.05%
Expected life (average years)	10.00	9.00
Fair value per option	\$ 1.70	\$ 1.98

13. COMMITMENT

The Company is committed to office lease payments excluding operating costs as follows:

2023	\$ 83,266
2024	34,694
	\$ 117,960

SPARE LABS INC.**Notes to Non-Consolidated Financial Statements****Year Ended December 31, 2022****(Unaudited)****14. INCOME TAXES**

A reconciliation of the statutory income tax rate to the effective income tax rate is as follows:

	2022	2021
Combined basis Federal and Provincial income taxes at statutory rates	\$ (545,270)	\$ (277,090)
SR&ED timing difference	64,933	52,629
Amortization timing difference	(5,040)	6,760
Non-deductible expenses	55,209	(16,192)
Unutilized non-capital losses	430,168	233,893
Income tax expense	\$ -	\$ -

- (a) As at December 31, 2022, the Company has a \$541,413 pool balance of deductible scientific research and development expenditures to be indefinitely carried forward to future years.
- (b) The Company has accumulated non-capital losses for tax purposes of \$7,525,482 available to offset future taxable income. The non-capital losses expire as follows:

2039	\$ 820,085
2040	631,199
2041	2,163,581
2042	3,910,617
	\$ 7,525,482

15. GOVERNMENT ASSISTANCE AND GRANTS

For the year ended December 31, 2022, the Company estimated a SR&ED tax credit recovery of \$740,087 (2021 - \$556,684). The SR&ED income tax credits are included in research and development costs and \$740,087 (December 31, 2021 - \$556,684; January 1, 2021 - \$481,619) was receivable at year-end.

During the year, the Company has also received the National Research Council of Canada's Industrial Research Assistance Program grants of \$189,580 (2021 - \$298,574), and other various grants of \$122,961 (2021 - \$223,229) and are included in research and development costs.

16. CREDIT FACILITIES

During the year, the Company issued share purchase warrants in connection with the following credit facilities with Silicon Valley Bank Canada ("SVB") (note 11):

- (a) Growth capital term loan of USD \$4,000,000, bearing interest at the greater of 1.50% and Wall Street Journal prime rate less 1.75% per annum, and secured by a general security agreement. As at December 31, 2022, the Company had \$nil (December 31, 2021 - \$nil; January 1, 2021 - \$nil) outstanding; and

SPARE LABS INC.

Notes to Non-Consolidated Financial Statements

Year Ended December 31, 2022

(Unaudited)

16. CREDIT FACILITIES — continued

- (b) Growth capital term loan of USD \$2,000,000, bearing interest at the greater of 3.25% and Wall Street Journal prime rate per annum, and secured by a general security agreement. As at December 31, 2022, the Company had \$nil (December 31, 2021 - \$nil; January 1, 2021 - \$nil) outstanding.

During the year, the Company has entered into a credit facility agreement with Royal Bank of Canada ("RBC") in Vancouver, British Columbia and has the following credit facilities available:

- (a) Letter of credit or letter of guarantee to a maximum of \$594,789 with fees to be advised on a transaction-by-transaction basis, and secured by a cash collateral (note 6) assigning term deposits and/or guarantee investment certificate in the amount of \$594,789. As at December 31, 2022, the Company had \$nil (December 31, 2021 - \$nil; January 1, 2021 - \$nil) outstanding; and
- (b) Letters of guarantee to a maximum of \$3,325,000 with fees to be advised on a transaction-by-transaction basis, and secured by Export Development Canada's guarantee. As at December 31, 2022, the Company had \$nil (December 31, 2021 - \$nil; January 1, 2021 - \$nil) outstanding; and
- (c) Business credit card facility to a maximum of \$100,000.

17. COMPARATIVE FIGURES

Financial statements for the year ended December 31, 2021 were compiled by other accountants and are presented for comparative purposes only. No opinion is or was expressed thereon.

SPARE LABS INC.
COMPILED FINANCIAL INFORMATION
DECEMBER 31, 2021

ALISTAIR & VICTOR
CHARTERED PROFESSIONAL ACCOUNTANTS

COMPILATION ENGAGEMENT REPORT

To Management of Spare Labs Inc.

On the basis of information provided by management, we have compiled the balance sheet of Spare Labs Inc. as at December 31, 2021, the statement of operations and deficit for the year then ended, and Note 1, which describes the basis of accounting applied in the preparation of the compiled financial information ("financial information").

Management is responsible for the accompanying financial information, including the accuracy and completeness of the underlying information used to compile it and the selection of the basis of accounting.

We performed this engagement in accordance with Canadian Standard on Related Services (CSRS) 4200, Compilation Engagements, which requires us to comply with relevant ethical requirements. Our responsibility is to assist management in the preparation of the financial information.

We did not perform an audit engagement or a review engagement nor were we required to perform procedures to verify the accuracy or completeness of the information provided by management. Accordingly, we do not express an audit opinion or a review conclusion, or provide any form of assurance on the financial information.

Readers are cautioned that the financial information may not be appropriate for their purposes.



CHARTERED PROFESSIONAL ACCOUNTANTS

Vancouver, B.C.
June 30, 2022

SPARE LABS INC.
BALANCE SHEET
AS AT DECEMBER 31, 2021

ASSETS

	2021	2020
CURRENT		
Cash and cash equivalents	\$18,423,275	\$ 3,983,386
Corporate taxes recoverable	556,684	481,619
Accounts receivable	569,754	319,349
Accrued receivable	183,750	-
Deposit	57,369	3,753
Prepaid expenses	<u>136,034</u>	<u>40,050</u>
	<u>19,926,866</u>	<u>4,828,157</u>
LONG TERM INVESTMENTS	573,298	-
INVESTMENTS IN JOINT VENTURE	601,750	601,750
INVESTMENTS IN SUBSIDIARY	126,300	-
CAPITAL ASSETS, net of amortization	<u>107,807</u>	<u>89,042</u>
	<u>1,409,155</u>	<u>690,792</u>
TOTAL ASSETS	<u>\$21,336,021</u>	<u>\$ 5,518,949</u>

LIABILITIES

CURRENT		
Accounts payable and accrued liabilities	\$ 389,804	\$ 87,439
DEFERRED REVENUE	828,156	541,976
LONG TERM DEBT	<u>-</u>	<u>40,000</u>
TOTAL LIABILITIES	<u>1,217,960</u>	<u>669,415</u>

SHAREHOLDERS' EQUITY

CAPITAL STOCK	23,581,847	6,022,757
DEFICIT	<u>(3,463,786)</u>	<u>(1,173,223)</u>
	<u>20,118,061</u>	<u>4,849,534</u>
TOTAL LIABILITIES AND EQUITY	<u>\$21,336,021</u>	<u>\$ 5,518,949</u>

SPARE LABS INC.
STATEMENT OF DEFICIT
FOR THE PERIOD ENDING DECEMBER 31, 2021

	2021	2020
DEFICIT - BEGINNING OF YEAR	\$ (1,173,223)	\$ (480,139)
Net loss	<u>(2,290,563)</u>	<u>(693,084)</u>
DEFICIT - END OF YEAR	<u>\$ (3,463,786)</u>	<u>\$ (1,173,223)</u>

SPARE LABS INC.
STATEMENT OF OPERATIONS
FOR THE YEAR ENDING DECEMBER 31, 2021

	2021	2020
REVENUE		
Sales	\$ 3,482,981	\$ 1,785,382
Grants	521,804	573,811
Interest	9,015	41,435
Loan forgiveness	-	20,000
Other	<u>2,262</u>	<u>68</u>
	<u>4,016,062</u>	<u>2,420,696</u>
EXPENSES		
Accounting and legal	239,952	112,642
Advertising and promotion	66,274	44,776
Amortization	81,564	66,189
Bad debt	1,203	-
Dues and subscription	758,703	322,140
Foreign exchange loss	41,648	22,440
Insurance	41,814	23,703
Interest and bank charges	1,017	(1,554)
Meals and entertainment	17,510	9,213
Office	175,951	156,360
Research and development	1,438,097	795,850
Rental	30,648	12,650
Salaries and benefits	3,257,580	1,461,859
Subcontract labour	475,237	506,317
Telephone and internet	109,745	26,711
Travel	<u>74,555</u>	<u>37,946</u>
	<u>6,811,498</u>	<u>3,597,242</u>
LOSS BEFORE INCOME TAXES	(2,795,436)	(1,176,546)
Income tax recovery	<u>504,873</u>	<u>483,462</u>
NET LOSS	<u><u>\$ (2,290,563)</u></u>	<u><u>\$ (693,084)</u></u>

SPARE LABS INC.
NOTES TO THE COMPILED FINANCIAL INFORMATION
FOR THE YEAR ENDING DECEMBER 31, 2021

NOTE 1 - BASIS OF ACCOUNTING

The basis of accounting to be applied in the preparation of the financial information is on the historical cost basis, reflecting cash transactions with the additions of:

- Accounts payable and accrued liabilities;
- Accounts receivable less an allowance for doubtful accounts;
- Current income taxes payable as at the reporting date; and
- Capital assets recorded at historical cost and amortized on a declining balance basis.

NOTE 2 - DESCRIPTION OF BUSINESS

Spare Labs Inc. (the "Company") is incorporated under the Canada Business Corporations Act. The Company's principal business activity is mobility management and sales of related services.

SPARE LABS INC.
FINANCIAL STATEMENTS
DECEMBER 31, 2020
(Unaudited - See Notice To Reader)

ALISTAIR & VICTOR

CHARTERED PROFESSIONAL ACCOUNTANTS

NOTICE TO READER

On the basis of information provided by management, we have compiled the balance sheet of **Spare Labs Inc.** as at December 31, 2020 and the statements of income and deficit for the year then ended. We have not performed an audit or a review engagement in respect of these financial statements and, accordingly, we express no assurance thereon. Readers are cautioned that these statements may not be appropriate for their purposes.

A handwritten signature in black ink, appearing to read 'Alistair & Victor', is written over a faint, light-colored rectangular stamp.

CHARTERED PROFESSIONAL ACCOUNTANTS

Vancouver, B.C.
June 18, 2021

SPARE LABS INC.
BALANCE SHEET
AS AT DECEMBER 31, 2020
(Unaudited - See Notice To Reader)

ASSETS

	2020	2019
CURRENT		
Cash and cash equivalents	\$ 3,983,386	\$ 4,716,223
Corporate taxes recoverable	481,619	382,121
Accounts receivable	323,102	395,467
Prepaid expenses	<u>40,050</u>	<u>19,895</u>
	<u>4,828,157</u>	<u>5,513,706</u>
INVESTMENTS IN JOINT VENTURE	601,750	601,750
PROPERTY, PLANT AND EQUIPMENT, at cost	219,150	196,898
Accumulated amortization	<u>130,108</u>	<u>63,920</u>
	<u>89,042</u>	<u>132,978</u>
	<u><u>\$ 5,518,949</u></u>	<u><u>\$ 6,248,434</u></u>

LIABILITIES

CURRENT		
Accounts payable and accrued liabilities	\$ 87,439	\$ 153,070
DEFERRED REVENUE	541,976	552,746
LONG TERM DEBT	<u>40,000</u>	<u>-</u>
	<u>669,415</u>	<u>705,816</u>

SHAREHOLDERS' DEFICIT

CAPITAL STOCK	6,022,757	6,022,757
DEFICIT	<u>(1,173,223)</u>	<u>(480,139)</u>
	<u>4,849,534</u>	<u>5,542,618</u>
	<u><u>\$ 5,518,949</u></u>	<u><u>\$ 6,248,434</u></u>

SPARE LABS INC.
STATEMENT OF DEFICIT
FOR THE YEAR ENDED DECEMBER 31, 2020
(Unaudited - See Notice To Reader)

DEFICIT - BEGINNING OF YEAR	\$ (480,139)
Net loss for the year	<u>(693,084)</u>
DEFICIT - END OF YEAR	<u><u>\$ (1,173,223)</u></u>

SPARE LABS INC.
STATEMENT OF INCOME
FOR THE YEAR ENDED DECEMBER 31, 2020
(Unaudited - See Notice To Reader)

	2020	2019
REVENUE		
Sales	\$ 1,785,382	\$ 1,002,835
Grants	573,811	92,395
Interest	41,435	79,640
Loan forgiveness	20,000	-
Other	68	909
	<u>2,420,696</u>	<u>1,175,779</u>
EXPENSES		
Accounting and legal	112,642	212,913
Advertising and promotion	44,776	75,613
Amortization	66,189	54,068
Bad debt	-	3,037
Dues and subscription	322,140	146,266
Foreign exchange loss/(gain)	22,440	2,166
Insurance	23,703	17,299
Interest and bank charges	(1,554)	9,115
Meals and entertainment	9,213	32,594
Office	156,241	101,369
Purchases	-	14
Research and development	795,850	183,211
Rental	12,650	-
Repairs and maintenance	119	552
Salaries and benefits	1,461,859	920,030
Subcontract labour	506,317	117,146
Telephone and internet	26,711	28,884
Travel	37,946	130,702
	<u>3,597,242</u>	<u>2,034,979</u>
LOSS BEFORE INCOME TAXES	(1,176,546)	(859,200)
Income tax recovery	483,462	394,947
NET INCOME/(LOSS)	<u>\$ (693,084)</u>	<u>\$ (464,253)</u>

Errata and Exceptions

Spare does not have any errata or exceptions to the State's requirements.

Vendor's License, Maintenance, and Service Level Agreements

Spare has included our Standard Master Agreement in [Appendix C](#) which includes our Service Level Agreement for review by the State.

Supporting Material

Spare has provided this type of documentation as part of our response to the [9. Project Management Specifications](#). Please see that section for evidence of our technical system documentation, training examples and materials, and other necessary plans and methodology examples.

Other Supporting Materials

Spare has included in [Appendix D](#):

- Identify and Access Management protocol
- Commingling for A More Efficient Service
- Including Non-Dedicated Service Providers for An Elastic Vehicle Supply
- Optional Call Centre: Telelink
- Planning and Service Design Support with Spare Realize

Description of Vendor Submitting Offer Form

Spare was founded in 2015 to make every ride possible by empowering public transit agencies with innovative tools to drive operational efficiencies and offer a superior rider experience. Eight years, over 150 transit partners, and over 200 service implementations later, Spare is one of the leading providers of accessible on-demand transit platforms worldwide with over 7.3 million (and growing daily) total riders.

Our tech-enabled solution makes it easy for public transit agencies to launch and manage microtransit, ADA paratransit, non-emergency medical transportation (NEMT), and other demand responsive commingled services. These include two award-winning agencies, Citibus in Texas and Dallas Area Rapid Transit (DART)—one of the largest multi-modal microtransit services in the world. We're similarly proud to

count among our agency partners Japan's award-winning KnowRoute—the country's first on-demand transit service.

Since our founding, Spare has consistently developed our product suite and partnerships to help public transit agencies to deliver paratransit operations that:

- Compliant:** Spare simplifies the process of paratransit compliance by making it more automatic. Spare Platform modernizes paratransit features to help agencies satisfy the +/- 1 hour booking rule, ¾ mile rule, 30 minute pickup window, accommodating demand with the fleets you have, and more.
- Multi-Fleet Operations:** Spare manages multiple operator systems on one centralized platform, which in turn creates the ability to conduct accurate reporting and contract management. For example, PSTA's door-to-door, on-demand paratransit service dispatches to five different external fleet dispatch systems through Spare Platform to meet ACA/ADA requirements and reduce costs.
- Complex:** We tailor complex and custom workflows that are specific to an agency's needs around paratransit to efficiently manage conditional eligibility. This reduces human error and ensures one single source of truth for customer management.
- Cost-Efficient:** Spare empowers agencies to do more with less. For example, by leveraging underutilized vehicle supply from another service to commingle trips with paratransit riders, which drastically improves transportation services and provides a better integration of service networks. Spare's intelligent routing and pooling algorithm takes into account parameters such as empty vehicle seats, locations, timing of schedules, and wait times to decide when to commingle trips.
- Easy to Use Interfaces:** Spare provides riders with easy-to-use booking services including a mobile app and customer portal app - allowing them to receive trip notifications, manage/load fares, and review trip history—further enhancing access to all services within the transportation network.



Spare is trusted by the most innovative and forward-thinking transit agencies of all sizes across four continents. In the past few years we have expanded to urban and rural transit agencies across North America including Florida, Texas, Nevada, Colorado, Missouri, Massachusetts, Oregon, and Minnesota.

Spare is also trusted by many of the biggest automakers, including Toyota and Mitsubishi, in providing on-demand transportation services to their customers.

Headquartered in Vancouver, Canada, our team of over 80 is driven by meaningful innovation – focused on empowering everyone to unlock the potential of mobility. Our cloud-based software offers a scalable, flexible, end-to-end transit platform for transit operators, drivers and riders. Some of our latest offerings include Open Fleets, giving operators the ability to access third-party fleet networks such as TNCs and taxis within our platform. Also on offer, our new Spare Call Center for providing both overflow or replacement call center services.

In 2021, Spare raised a Series A funding round that we employ to further build out our vision of the world's most sophisticated on-demand transit platform. Our goal is to enable better cooperation between different transportation providers in increasing access to cost-efficient and inclusive shared rides.

All Pages Solicitation Document

The Disaster Recovery Assessment (DRA) spreadsheet and Security Evaluation Form have been completed. We have uploaded the spreadsheet to the portal as it is an Excel document, but have attached the Security Evaluation Form along with all of our security policies in [Appendix E](#). As well is the completed Attachment K.

Appendix A - Signed Addendum #1



**NORTH CAROLINA
DEPARTMENT OF TRANSPORTATION**

Solicitation Addendum

Solicitation Number: 54-12008772-CM

Solicitation Description: Transit Software Solution

Solicitation Opening Date and Time: June 19, 2023, at 2:00PM EST

Addendum Number: 1

Addendum Date: May 16, 2023

Purchasing Agent: Christie Murphy, clmurphy1@ncdot.gov, (919) 707-4848

1. Return one properly executed copy of this addendum with bid response or prior to the Bid Opening Date/Time listed above.
2. The following are questions received about the solicitation and the State's answers to the questions.

No.	REFERENCE	VENDOR QUESTION	STATE'S RESPONSE
1	Section - 2.4 AGENCY BACKGROUND Page 4	Can NCDOT confirm the total number of vehicles that currently requires software licenses for this pilot project? And will there be any increase in the fleet size as the data stats is for the year 2019?	Approximately 1440 demand response vehicles are in operation at a given time among NC transit systems; 2019 is the latest fleet information that is available at this time
2	Section - 2.4 AGENCY BACKGROUND Page 4	Can NCDOT provide the number of vehicles for Urban, small Urban, and rural system separately?	Detailed fleet numbers for NC transit systems are provided in Appendix A.
3	Section - 2.4 AGENCY BACKGROUND Page 4	Who is the incumbent provider of Demand Response Software?	There is no current universal Demand Response software provider for NC transit systems.
4	Section - 2.4 AGENCY BACKGROUND Page 4	Is there NEMT brokerage component required with the transportation providers?	Not all NEMT systems in the state necessarily require a brokerage component but that is the case with the vast majority of NC DROs
5	Section - 2.4 AGENCY BACKGROUND Page 4	Can NCDOT clarify whether the Advanced specifications are optional in the vendor responses?	Yes, advanced specifications are optional to respond to for this bid.
6	Section 2.5 Problem Statement Page 5	Can NCDOT clarify what is meant by new mobility services and turnkey transportation services? E.g., what specific	NCDOT prefers to keep these items open ended to allow for as many potential submissions as possible since this is intended as a multi-vendor contract.

		services/requirements are included in these two?	
7	Section 3.3.2 Architecture Diagrams Defined Page 7	As the template provided in the link, the file is empty when opened. Can NCDOT confirm whether the two architecture pictures in the link is the preferred template?	Template can be downloaded at https://it.nc.gov/services/vendor-engagement-resources
8	Section 3.3.4 IDENTITY AND ACCESS MANAGEMENT (IAM) Page 7	Can NCDOT confirm where this offer should be placed in terms of the format given that this is not mentioned in the section 6.3.2 Offer Organization?	Vendor may attach the supporting documentation as a separate appendix noted Section 3.3.4.
9	Section 3.4 BUSINESS AND TECHNICAL SPECIFICATIONS Under - 2 Common Design Specifications (ID -2.a-3) Page 13	Can NCDOT spell out in greater detail what is meant by the instruction to Include in the proposal examples of APIs and a description of the features and functions supported by existing APIs?	NCDOT prefers to keep these items open ended to allow for as many potential submissions as possible since this is intended as a multi-vendor contract.
10	Section 3.4 BUSINESS AND TECHNICAL SPECIFICATIONS 3 Demand Response Software – ID 3.a-10 Page 14	Can NCDOT clarify what is meant by – “A system that utilizes a recognized relational database management system that allows for mission critical database management capabilities”?	NCDOT prefers to keep these items open ended to allow for as many potential submissions as possible since this is intended as a multi-vendor contract.
11	Section 3.4 BUSINESS AND TECHNICAL SPECIFICATIONS b. Client Management ID - 3.b-3 Page 16	Can NCDOT clarify what is meant by the statement “System provides tools or features to support adding clients (e.g., partners living at the same address, group homes, etc.) to facilitate rapid entry of client data.”?	NCDOT prefers to keep these items open ended to allow for as many potential submissions as possible since this is intended as a multi-vendor contract.
12	Section 3.4 BUSINESS AND TECHNICAL SPECIFICATIONS c. Reservations ID -3.c-10	Can NCDOT explain what is meant by –“Vendor provides explanations of any limitations for scheduling rides including limitations for the number of vehicles and/or passenger trips that can be scheduled.”?	NCDOT prefers to keep these items open ended to allow for as many potential submissions as possible since this is intended as a multi-vendor contract.
13	Section 3.4 BUSINESS AND TECHNICAL	Can NCDOT explain what is meant by “Printed manifest details and layout will be	The intent was that final layout of the printed manifest can be discussed and finalized at time of the transit system’s design review period.

	SPECIFICATIONS d. Scheduling 3.d-7 Page 19	defined during design review”?	
14	Section 3.4 BUSINESS AND TECHNICAL SPECIFICATIONS d. Scheduling, ID 3.d-8 Page 19	Can NCDOT clarify what is meant by the statement “The system allows users to view maps that illustrate fixed route bus routes and bus stops relative to trip origins and destinations.”?	This refers to systems being able to access maps that show existing bus routes and bus stops along with demand response origin and destination points.
15	Section 3.4 BUSINESS AND TECHNICAL SPECIFICATIONS d. Scheduling, ID 3.d-13 Page 19	Can NCDOT what is meant by the statement “The system maintains an open return list (e.g., willcalls) for passengers with an uncertain pickup time for the return leg of a trip (e.g., after a medical appointment of uncertain duration.”?	This refers to the scheduling system being able to accommodate flexible return times for trips that have no standing return time. An example of this would be a medical visit with no standing return home time.
16	Section 3.4 BUSINESS AND TECHNICAL SPECIFICATIONS 8.Priced Options Page 37	Can NCDOT spell out in greater detail what it means by Ruggedized Tablet?	The term Ruggedized refers to devices specifically designed to operate reliably in vehicles, harsh usage environments and conditions, such as strong vibrations, extreme temperatures and wet or dusty conditions. The rugged computers shall have features that include but shall not be limited to hardened casings, waterproof keyboards, sunlight-readable displays, and shock-mounted disk drives.
17	Priced Options Page 37	Is NCDOT willing to purchase the all the mentioned hardware through the vendor? If yes, can you confirm the total number for each type of hardware required for this project?	Potentially, as this is an optional category, NCDOT retains the ability to award at our discretion.
18	Onboard Hardware, Data Communications, and Installation (Option) Page 39	Is NCDOT willing to purchase all the mentioned Onboard Hardware, Data Communications, and Installation through the vendor? If yes, can the vendor include these costs in the price proposal?	Potentially, as this is an optional category, NCDOT retains the ability to award at our discretion. Yes, vendor can provide costs with proposal.
19	Section 6.3 Instructions For Offer Submission Page 46	With respect to the section: Can NCDOT confirm whether there is a page limit for vendor proposals?	No page limit requirements.

20	Section 6.3.2 OFFER ORGANIZATION Page #47 ATTACHMENT E: COST FORM RESERVED Page 86	With reference to this section under cost of Vendor offer: Can the vendor send the pricing in its own format?	Submissions must be formatted as detailed within Section 6.3.2 however there is no specific template mandated by NCDOT to submit pricing.
21	Section 6.3.2 OFFER ORGANIZATION Page 47 ATTACHMENT E: COST FORM RESERVED Page 86	Is there any preferred format for "ATTACHMENT E: COST FORM RESERVED?" If yes, please provide the preferred format.	Submissions must be formatted as detailed within Section 6.3.2 however there is no specific template mandated by NCDOT to submit pricing.
22	Attachment I: Financial Review Form Page 90	With reference to this form: it asks to attach a link to annual reports with financial statements and management discussion for the past three complete fiscal years. Can the vendor share the link separately through the email?	Please review page 50, Section 7.2, Financial Statements.
23	Section 1.0 Anticipated Procurement Schedule Page 3	Can NCDOT kindly extend the submission deadline to allow vendors to provide more responsive and informative proposals?	NCDOT does not intend to extend the bid submission deadline at this time.
24	Section - 2.4 AGENCY BACKGROUND Page 4	Can the Agency please share the budget for this project for the first year, and subsequent years?	There is no projected budget for this project at this time.
25	6.3.2 OFFER ORGANIZATION Page 47	Will NCDOT accept electronic signatures on the forms and letters?	NCDOT will accept electronic signatures where applicable.
26	2.5 Problem Statement Page 5	Does NCDOT only want pricing for a hosted solution, or would they like to see pricing for on-premise installations as well?	Please refer to the Problem Statement, the Business and Technical Specifications, Section 3 Demand Response Software and Section 6.2.6 for Alternate Offers.
27	2.5 Problem Statement Page 5	Does NCDOT only want SaaS pricing, or would they like to see pricing for both SaaS and a license and maintenance model?	Please refer to the Problem Statement, the Business and Technical Specifications, Section 3 Demand Response Software and Section 6.2.6 for Alternate Offers.

28	2.5 Problem Statement Page 5	NCDOT talks about fare payment integration within the RFP, please elaborate on which faring solutions they would like to see integrations with?	NCDOT prefers to keep these items open ended to allow for as many potential submissions as possible since this is intended as a multi-vendor contract
29	6.3 Instruction for Offer Submission Page 46	Would the NCDOT consider an extension to the proposal submission due date to accommodate the complexity of this RFP?	NCDOT does not intend to extend the bid submission deadline at this time.
30	2.0 Purpose of RFP Page 4	Will agencies have the ability to select from any of the awarded vendors for their solution? Will any factors limit certain agencies from selecting particular vendors?	If ultimately there is a multi-vendor award from this bid, agencies will have the opportunity to select from any awarded vendors; No inherent factors should block a prospective system from utilizing an awarded vendor.
31	3.0 RFP Requirements and Specifications Page 5	Does not providing or meeting Advanced/Optional specs/items affect evaluation of award?	NCDOT will deem any submissions that are compliant with “Core” specifications as being a complete bid.
32	8 Priced Options Page 37	Will the agency be willing to purchase the hardware from a separate vendor or does the vendor need to provide optional pricing? If yes, can you confirm the total number of hardware units required for this project?	The proposing vendor will be responsible for providing the optional pricing; NCDOT does not intend on awarding an subcontractors or vendors outside of the bid submitter.
33	Attachment E Page 86	Attachment E – Cost Form has not been provided in the RFP. Is there a prescribed form or is the vendor able to provide pricing in its own format?	Refer to Section 4.0 Cost of Vendor’s Offer, Page 40
34	Attachment E Page 86	What criteria should be considered for accurate pricing for this program (specific number of vehicles, number of users, max trips per day, etc.)?	Refer to Section 4.0 Cost of Vendor’s Offer, Page 40
35		What is the overall budget of this program?	No overall budget has been set for this project at this time.
36		What is the funding source for this project? What are the funding deadlines/timelines for this project, i.e., when does the money need to be spent?	Funding sources will be dependent on who is procuring but generally speaking it will be a combination of federal, state and local transit funds. NC state fiscal year runs from July to June.

37		Is there a page limit for the proposal responses?	No, there are no page limits to the responses.
38		Are there any hard deadlines to project deployments / launches?	Deadlines have not been determined at this time.
39		What is the anticipated launch date of the first project kick-off?	NCDOT projects that transit systems could potentially begin procuring from the awarded contract as early as NC Fiscal Year 2024.
40		Will NCDOT accept electronic signatures on the forms and proposal?	Yes, NCDOT will accept a wet signature or DocuSign signature on the proposal.
41	2.5 Problem Statement Page 5	Does NCDOT have a minimum agency target Productivity (Passengers per Vehicle Hour) for agency Demand Response Services?	Not at this time.
42		Are there any benchmark data points that can be shared and targeted as goals? (i.e., Cost/Passenger, Ridership, PVH, etc.).	Not at this time.
43		Is there a DBE requirement/goal for this project?	NCDOT IMD's DBE goal is currently 4.31%
44	RFP Section 2.5 Problem Statement Page Number 5	Key Objective #2 states, "simplified scheduling and new payment options." Could NCDOT clarify what is being requested as far as new payment options? There does not appear to be specs around payment options listed in the RFP.	"New payment options" for the purposes of this solicitation refers to fare payments.
45	RFP Section 2.5 Problem Statement Page Number 5	Key Objective #6 states, "turnkey transportation services." Can NCDOT clarify what "turnkey transportation services" are to be proposed. If turnkey services are required, will vendors be given flexibility to price separately for those agencies at a later time?	NCDOT prefers to keep these items open ended to allow for as many potential submissions as possible since this is intended as a multi-vendor contract

46	RFP Section 2.a-1 Page 12	“The system uses APIs to share data and connect with third-party applications as required by the DROs. The Vendor provides documentation describing all API calls, data formats, and communication and security protocols used to support the system interfaces.” Can NCDOT provide examples of third-party applications required by the DROs?	NCDOT prefers to keep these items open ended to allow for as many potential submissions as possible since this is intended as a multi-vendor contract
47	RFP Section 3.b-4 Page 15	“A system that allows authorized users to query tables of riders, reservations, and trips based on user-defined search parameters.” For what purpose?	Generally speaking, the purpose would be to provide ridership reports and/or destination reports.
48	RFP Section 3.c-10 Page 17	“Vendor provides explanations of any limitations for scheduling rides including limitations for the number of vehicles and/or passenger trips that can be scheduled.” Can NCDOT clarify this specification further? Is this referencing specific agency service parameters (i.e., if passengers are eligible for service, or if wheelchair accessible vehicles are required).	Yes, the intent was to provide vehicle and/or trip parameters.
49	RFP Section 3.c-16 Page 17	“The system allows a user to book disconnected legs of a trip.” Can NCDOT clarify what is meant by disconnected legs of a trip?	A disconnected leg in this case would refer to a trip that doesn’t necessarily travel back to the point of origin from the trip destination but rather an alternative destination.
50	RFP Section 3.d-2 Page 18	“The system allows for trips to or from same origins, or to same destinations, to be combined to eliminate duplicate trips.” Can NCDOT clarify what is meant by this specification?	The intent here was to identify duplication of trips for riders who share a common point of origin or destination IE multiple riders going from one assisted point of origin to the same destination at the same time but having been split up onto multiple vehicles.

51	RFP Section 3.d-8 Page 19	“The system allows users to view maps that illustrate fixed route bus routes and bus stops relative to trip origins and destinations.” Are users being referred to as agency staff or riders? Can NCDOT clarify what the purpose of this functionality will be?	“Users” in this case refers to Demand Response Operators.
52	RFP Section 3.d-20 Page 20	“The system allows the DRO to easily add, remove, and modify service boundaries based on service type and driver.” As an alternative, if a Project Manager is required to make this change on behalf of the DRO, is there a desired SLA?	NCDOT prefers to keep these items open ended to allow for as many potential submissions as possible since this is intended as a multi-vendor contract.
53	RFP Section 3.e-3 Page 20	“The system allows for a specific driver to be assigned to a route and allows the dispatcher to change a vehicle number.” What is meant by assigned to a route?	NCDOT prefers to keep these items open ended to allow for as many potential submissions as possible since this is intended as a multi-vendor contract.
54	RFP Section 3.g-2 Page 23	“The system includes tariff management tools to administer all fare price and fare structure. The Agencies will establish the price of fares.” Will NCDOT elaborate on what is meant by tariff management tools?	NCDOT prefers to keep these items open ended to allow for as many potential submissions as possible since this is intended as a multi-vendor contract.
55	RFP Section 3.g-3 Page 23	“The system handles billing and invoicing functions for riders/trips.” What kinds of invoicing functions are required here?	NCDOT prefers to keep these items open ended to allow for as many potential submissions as possible since this is intended as a multi-vendor contract
56	RFP Section 3.d-7 Page 19	“ The system prints vehicle manifests on a daily basis. The system formats printed manifests in a manner that minimizes paper waste, in a	NCDOT prefers to keep these items open ended to allow for as many potential submissions as possible since this is intended as a multi-vendor contract.

		legible font size suitable for drivers to reference while enroute, and only includes minimal information (e.g., client name, pick up/drop off address, scheduled window, etc.). Printed manifest details and layout will be defined during design review.” Is an active and dynamic digital manifest displayed on a driver-facing application a suitable replacement for paper-based manifests?	
57	RFP Section 3.d-16 Page 19	“The system allows the user to mark specific trips as “critical” or exempt from automated modification. If a critical trip must be modified manually, the system provides sufficient controls or notifications to the dispatcher.” In what situation would a trip need to be marked as "Critical?"	NCDOT prefers to keep these items open ended to allow for as many potential submissions as possible since this is intended as a multi-vendor contract.
58	RFP Section 3.e-13 Page 21	“ The system displays all dispatch activity for any route and allow the dispatcher to add dispatch activity notes.” What type of notes would be added by dispatchers to specific routes?	NCDOT prefers to keep these items open ended to allow for as many potential submissions as possible since this is intended as a multi-vendor contract.
59	RFP Section 3.e-19 Page 21	“ The system provides the DROs with two-way text messaging from dispatch to DRO. Messages shall be saved or archived in the system for future reference.” What would be the typical content of these text messages? Would recorded radio messages be a suitable alternative?	NCDOT prefers to keep these items open ended to allow for as many potential submissions as possible since this is intended as a multi-vendor contract.
60	RFP Section 3.f-9 Page 22	“ The system allows drivers to provide pickup and drop-off comments for each trip. The	NCDOT prefers to keep these items open ended to allow for as many potential submissions as possible since this is intended as a multi-vendor contract.

		system synchronizes with the client record and is available for future passenger trips.” What type of information would drivers need to include in pick-up and drop-off comments?	
61		Will the State of North Carolina please address the funding source for this project?	Funding sources will be dependent on who is procuring but generally speaking it will be a combination of federal, state and local transit funds. NC state fiscal year runs from July to June.
62		Does the State of North Carolina desire to have the vendors master service agreement included with their proposal?	Yes, NCDOT would support including the vendor master agreements with their proposal.
63		If a vendor does not supply their own hardware but rather offers a BYOD (bring your own device) approach, does the State of North Carolina desire to have estimated costs for hardware (tablets, cases, mounts) and data plans that would be purchased from the DORs local cellular provider of choice?	Additional priced options such as hardware are Advanced specifications for the purposes of this bid and are therefore not a requirement to be deemed a complete proposal.
64		Does this RFP potentially include providing preventative vehicle maintenance software if a vendor has such technology directly integrated with their own platform?	Not at this time.

Failure to acknowledge receipt of this addendum may result in rejection of the response.

Check ONE of the following options:

- ☒ Bid has not been mailed. Any changes resulting from this addendum are included in our bid response.
- ☐ Bid has been mailed. No changes resulted from this addendum.
- ☐ Bid has been mailed. Changes resulting from this addendum are as follows:

Execute Addendum:

Offeror: Spare Labs Inc.

Authorized Signature:



Name and Titled (Typed):

Kristoffer Vik Hansen, CEO

Date:

June 1, 2023

Appendix B - Project Deliverables Specifications

TEMPLATE
Spare Labs Quality Assurance Plan
[Project Name]

Spare Labs (Spare) and the [client name] entered into Contract Number [number] on [date]. Per [contract reference] of this agreement, Spare agreed with [client name] to [state reason for operating software]. [contract reference] states that it is Spare's [insert Spare's responsibility if stated]. Additionally, Spare [insert reference to quality assurance plan.] This document serves to fulfill this contractual obligation stated in [contract reference].

The Quality Assurance Plan will be broken into 4 sections: People, Service, Vehicles, and Data. These sections will contain details of contractual requirements, policies and procedures for both Spare and its subcontractor(s), Spare's monitoring procedures and corrective actions to subcontractor(s), and how these items will be reported to [client name].

PEOPLE

Call Center Agents

Spare has subcontracted Call Center services to Telelink. The Telelink Call Center is open 24/7 to book trips and provide trip status information to customers.

Spare will meet with Telelink staff no less than monthly for performance reviews and will monitor Telelink performance based on the policies and procedures below:

Prime Contract Reference	Spare Policy	Subcontractor Procedure	Spare Monitoring Procedure	Corrective Action
[insert]	All call center operations will be monitored by Spare.	Telelink will be expected to follow all Standard Operating	Spare will perform quality checks on random phone calls	Any issues identified by Spare will be communicated to

		Procedures outlined by Spare. Telelink will provide access to their virtual phone system to Spare.	no less than monthly. Spare will ensure all procedures are being followed as expected.	Telelink. It is the expectation that Telelink take steps to retrain and re-educate the agent on proper procedures.
[insert]	Spare will provide training and retraining to call center agents upon request	Telelink can request training or retraining at any time	Spare will monitor complaints and ensure the Telelink team is highly trained and retrained.	Provide training to Telelink agents

Drivers

Spare has currently subcontracted with [number of] operations providers: [insert names of operators]. While these subcontractors are responsible for the hiring, management, and training of all drivers, Spare will hold each subcontractor accountable to the following policies and procedures, as applicable:

Prime Contract Reference	Spare Policy	Subcontractor Procedure	Spare Monitoring Procedure	Corrective Action
[insert]	Drivers shall not have three (3) or more verified complaints	Subcontractors will be provided any driver complaints for further investigation. Subcontractor will report findings within 3 business days.	Spare will monitor the automated ticketing system from Telelink and communications from [client name] for complaints. Spare will conduct its own complaint investigation and provide the complaint to the subcontractor.	Subcontractor shall document any driver discipline taken in response to any verified complaint. Driver may be removed following 3 verified complaints.

[insert]	[insert]	[insert]	[insert]	[insert]

In addition to above requirements, subcontractors are required to perform training on the following areas, per [contract reference of the Prime Contract:

- [Insert items]

VEHICLES

As part of this contract, all of Spare's subcontractors will be responsible for maintaining vehicle cleanliness and vehicle maintenance. Spare policies and procedures will be broken down by those three categories below: Vehicle Interior Cleanliness, Vehicle Exterior Cleanliness, and Vehicle Maintenance.

Vehicle Interior Cleanliness

Prime Contract Reference	Spare Policy	Subcontractor Procedure	Spare Monitoring Procedure	Corrective Action
[insert]	Daily, subcontractors shall sweep, dust, and mop vehicle floors as appropriate to ensure	Ensure floors of the interior of each vehicle are clean daily, and mop, dust, or sweep as	No less than quarterly, Spare reserves the ability to physically inspect any vehicle	Subcontractor will mop / dust / sweep the floor of any non-compliant vehicle(s) prior to

	vehicle floors are clean.	needed to ensure floor cleanliness.	for cleanliness at any time, including in-service spot check and out of service audit inspections.	returning the vehicle(s) to service.
[insert]	Weekly, vehicle interiors will be washed, including all windows, seats, floor, stanchions, and grab rails.	Ensure all components of vehicle interior is thoroughly cleaned weekly, including all windows, seats, floor, stanchions, and grab rails.	No less than quarterly, Spare reserves the ability to physically inspect any vehicle for cleanliness at any time, including in-service spot check and out of service audit inspections.	Subcontractor will fully clean the interior of the vehicle(s) of any non-compliant vehicle(s) prior to returning it to service.
[insert]	Monthly, floors will be waxed once per month with a non-stick wax, and ceilings and walls will be thoroughly cleaned.	Ensure vehicle floors are waxed with non-stick wax at least monthly, and ensure ceilings and walls are thoroughly cleaned monthly	No less than quarterly, Spare reserves the ability to physically inspect any vehicle for cleanliness at any time, including in-service spot check and out of service audit inspections.	Subcontractor will wax and/or fully clean the ceilings and/or walls of the vehicle of any non-compliant vehicle(s) prior to returning it to service.
[insert]	As needed, vehicles will be kept free of litter and debris, interior glass shall be leaned to maintain clean appearance and visibility, and exterminate all vermin and insects within the vehicle.	Ensure vehicle interiors are kept clean throughout the service day. This includes litter and debris, interior glass and surfaces, and removal of vermin and/or insects as needed.	No less than quarterly, Spare reserves the ability to physically inspect any vehicle for cleanliness at any time, including in-service spot check and out of service audit inspections.	Subcontractor will remove litter and/or debris, or fully clean any interior glass, or exterminate vermin and/or insects in any non-compliant vehicle(s) prior to returning it to service.

Vehicle Exterior Cleanliness

Prime Contract	Spare Policy	Subcontractor Procedure	Spare Monitoring Procedure	Corrective Action

Reference				
[insert]	Within 24 hours, all graffiti and/or dirt on vehicle exterior shall be removed	Ensure graffiti or dirt is removed as soon as possible, no longer than 24 hours after it is first noticed	No less than quarterly, Spare reserves the ability to physically inspect any vehicle for cleanliness at any time, including in-service spot check and out of service audit inspections.	Subcontractor will remove graffiti and/or dirt from non-compliant vehicle(s) prior to returning the vehicle to service.
[insert]	Daily, vehicle exterior shall be rinsed. Twice per week at minimum, vehicle exteriors shall be washed, including the entire vehicle body, windows, and wheels	Ensure vehicles are rinsed daily and washed twice a week. Vehicle washing is expected to occur more frequently as needed so that vehicle exteriors consistently are as clean as possible	No less than quarterly, Spare reserves the ability to physically inspect any vehicle for cleanliness at any time, including in-service spot check and out of service audit inspections.	Subcontractor will rinse and/or wash non-compliant vehicle(s) prior to returning the vehicle to service.
[insert]	Monthly, rubber or vinyl components (tires, bumper fascia, fender skirts, door edge guards, etc.) shall be cleaned and treated with a preservative	Ensure rubber or vinyl components of vehicle exterior are cleaned and treated with a preservative monthly	No less than quarterly, Spare reserves the ability to physically inspect any vehicle for cleanliness at any time, including in-service spot check and out of service audit inspections.	Subcontractor will clean and/or apply preservative to non-compliant vehicle(s) components prior to returning the vehicle to service.

Vehicle Maintenance

Prime Contract Reference	Spare Policy	Subcontractor Procedure	Spare Monitoring Procedure	Corrective Action
[insert]	Subcontractors will adopt and adhere to a Preventative Maintenance Inspection (PMI)	Ensure a PMI plan is in place and all PMI intervals are completed and documented.	No less than quarterly, Spare intends to inspect maintenance records for any vehicle at any	Subcontractor will be required to complete a missed PMI on the vehicle(s) prior to returning

	inter	Perform each interval within 500 miles past the interval. Provide Spare a copy of the PMI plan that will be followed. PMI intervals are not a reason to defer maintenance at any time.	time. Spare may schedule a time to view records or arrive unannounced for inspection.	the vehicle to service.
[insert]	Contractor is expected to utilize heating and cooling systems at all necessary times. Prime contract requires air conditioning be operated at any air temperature 76 degree or warmer.	Ensure drivers are instructed on vehicle heating and cooling policy.	No less than quarterly, Spare reserves the ability to physically perform in-service, vehicle operations spot checks. Spare will check that the interior of the vehicle is climate controlled while in service.	Driver(s) will be required to turn on the heating or cooling system.
[insert]	Interior of the vehicle should be free from exhaust at all times.	Ensure exhaust systems are working properly.	During an in-service, vehicle operations spot check, Spare will observe if the interior is free from exhaust. Spare will monitor customer feedback and inform subcontractor(s) of any report of exhaust in the vehicle.	Upon reporting of exhaust smell, inspect vehicle exhaust systems and perform any necessary maintenance prior to vehicle returning to service.
[insert]	In the event a vehicle must be out of service for longer than 5 business days, subcontractor will notify Spare in writing.	Ensure Spare is notified in the event a vehicle will be out of service for longer than 5 business days.	Spare continuously monitors service and expects to maintain a consistent line of communication with each subcontractor. Should Spare notice a vehicle out of service for more than 5 days in a row without prior notification, Spare will confirm vehicle status with	Confirm vehicle status with subcontractor and provide any urgent updates to [client] at the earliest moment possible.

			the subcontractor.	

SERVICE

Spare will be responsible for ensuring all subcontractors and Spare itself has service operations, contingency, and emergency plans. Spare policies around service plans are as follows:

Prime Contract Reference	Spare Policy	Subcontractor Procedure	Spare Monitoring Procedure	Corrective Action
[insert]	Every subcontractor must have a contingency plan for spare capacity.	Ensure a contingency plan is in place for spare capacity in the event of a service issue or service expansion. Provide Spare the contingency plan.	Spare will document and review contingency plans. Spare will ask subcontractor(s) to update plans as service expands.	Spare will request, review, and document a contingency plan
[insert]	Every subcontractor will keep a list of vehicles for dedicated service, including Vehicle Number, Make and Model, VIN, Maximum Capacity, and contact number for driving practice reporting	Ensure a list of vehicles dedicated to service exists and is provided to Spare.	Spare will review and document any vehicles that are not within policy.	Spare will request an updated list of vehicles.
[insert]	Dispatch service will be provided at all times that directly operated revenue service is being provided.	Provide dispatch services and log any events by electronic ticketing system	Spare will monitor service throughout the day, and will constantly monitor ticket queues for any escalated electronic service ticket.	Spare will remain in consistent contact with the subcontracted call center to ensure dispatching services are performed.
[insert]	Subcontractors shall develop, implement, and maintain procedures to respond to emergencies and routine operating problems.	Ensure procedures are documented and implemented as needed. Provide copies of operational problem and emergency procedures to Spare.	Review procedures and ensure they are followed at all times during each separate problem or emergency.	Spare will review the problem and/or emergency response for a given situation and provide guidance for future incidents.

[insert]	In the event of a declared emergency, subcontractors shall deploy dedicated accessible vehicle as directed by [client] Project Manager and work closely with other [client] staff as necessary to respond to rapidly changing conditions	Ensure plan is in place for declared emergencies. Communicate directly with Spare's Transit Operations Manager throughout the course of the emergency event.	Spare will review the declared emergency plan with subcontractor(s). Spare will facilitate provision of service that occurs during a declared emergency among all subcontractors.	Spare will request and review a declared emergency plan.

DATA

Spare is responsible for ensuring secure and accurate data as well as timely reporting. Below is Spare's plan for data and reporting:

Prime Contract Reference	Report Information	Report Delivery Frequency	Spare's Method of Delivery	Note / Corrective Action
[insert]	NTD Reporting	NTD reporting is available on request to [client] users in Spare Analyze. Typical NTD Reporting timelines are monthly and annually.	Electronic, either by self service in Spare Analyze, or by email	Upon notification of potential NTD data error, Spare will promptly investigate and resolve.
[insert]	Daily Work Roster Includes duty number, name of operator, scheduled and actual pull out time, scheduled and actual pull in time, vehicle numbers assigned to run,	Daily	Electronic, by self service in Spare Analyze	This information is available in Spare Analyze, and individually in Spare Launch

	revenue collected, and daily mileage			
[insert]	Daily Dispatch Log, if available Includes time, duty number, and issue (schedule delay of 15 minutes or longer, missed trips, in-service vehicle breakdown, vehicle or driver relief, accidents, wheelchair lift/ramp assisted passenger boardings)	Daily	Electronic, by self service in Spare Analyze	Spare is currently developing additional trip timeline tools that will outline all actions taken on each trip.
[insert]	Daily Ridership Report	Daily	Electronic, by self service in Spare Analyze	This information is available in Spare Analyze
[insert]	Daily Customer Service Report	Daily	Electronic, by email or other agreed upon means	This information will be gathered by Spare staff and provided to [client]
[insert]	Accident and Incident Reports Any accident or incident causing injury to contractor, [client], or any 3rd Party shall be immediately recorded and investigated	As Needed Immediate Phone Notification, email report provided	Phone, email	Spare will gather information from subcontractor(s) and provide to [client]
[insert]	Weekly Key Performance Indicators Report	Weekly	Electronic, by email	This information is automatically sent to users by email
[insert]	Monthly Operational Reports, including: Current and historical number of dedicated drivers, max	Monthly	Electronic, either by self service in Spare Analyze, or by email	This information is available in Spare Analyze. Additional data may be emailed by Spare staff upon request.

	dedicated accessible vehicles in a day, total boardings by service, hours and mile by vehicle and service, and total fares and passes sold, by type			
[insert]	Monthly Customer Service Report, including: Contact type and medium, Distributions of commendations, complaints, and requests by category and resolution status, and List of unresolved complaints pending resolution	Monthly	Electronic, by email	Spare staff will compile and provide a monthly customer service report to [client] by email
[insert]	Monthly Statistics, including: Number and percentage of missed trips, accident rate (total accidents, in service accidents, preventable accidents, NTD passenger accident ratios), On Time Performance, invoicing, and dedicated vehicle inspection and repair histories	Monthly	Electronic, by email	This information will be compiled by Spare and provided to [client]
[insert]	Quarterly Reports and Performance Reviews, including: Roster sheets, ridership trends, customer satisfaction and feedback, On Time	Monthly	Electronic, by email	This information will be compiled by Spare and provided to [client]

	Performance, Service Performance, cost per mile, revenue hours, service interruptions, and accidents.			
[insert]	Annual reporting including: Maintenance, Safety, Ridership Statistics, NTD, and cost performance reports	Annual	Electronic, by email	This information will be compiled by Spare and provided to [client]

Spare Labs

815 W Hastings St
Suite 810
Vancouver, BC
V6C 1B4

[client] Implementation Risk Report

[date]

Purpose

This Risk Management Plan (RMP) identifies, analyzes and defines responses to risk events to help ensure that the consequences of adverse events to project scope, schedule and budget are minimized or mitigated. It assigns specific responsibilities for risk management and prescribes the documenting, monitoring, and reporting processes to be followed. The Risk Registry is used to perform the RMP processes.

We will continue to update this working document as any additional risks arise or additional steps are taken to mitigate risks.

Objective

Ensure that the risks of the project are consistent with [client]'s overall project and agency goals and objectives using the Risk Registry;

Define the processes that will be used to identify, analyze and manage risks throughout the project;

Identify the frequency with which risks will be reviewed and who will be responsible for conducting the review;

Define the roles and responsibilities of individuals in managing risk; and

Initially identify the major risks, strategies for mitigating those risks and who will be responsible for implementing the mitigation.

Risk Identification

Risk identification is the first step in the risk management process. Its purpose is to determine those critical events that could prevent the project from achieving its objectives. All identified risks are documented in this section, with a statement of the risk and a description of the conditions or situations causing concern.

Risk Analysis

Risk analysis is the second step in the risk management process. Probability of the risk occurring is assigned a percentage rating between 10% for very low to 90% for very high. Impact is given a numeric rating between 1 for very low to 9 for very high. Probability is multiplied by Impact to assign a Risk Score between .1 and 8.1. A Risk Score between 0.1 and 1.5 results in a Low Risk Indicator; 1.8 and 4.2, Medium; and 4.2 to 8.1, High.

The Risk Indicator levels indicate the level of risk management mitigation and response activity required:

Low Risk: Risk can be controlled within normal project activities performed in the course of task performance and schedule, AIL and Risk Matrix reviews during project team meetings.

Medium Risk: Special action and management attention will be required to control acceptable risk.

High Risk: Significant additional action and high priority management attention will be required to control acceptable risk.

Risk Response Plan

Development of the risk response plan is the third step in the risk management process. In this step, mitigation actions are developed for each risk to prevent the risk event from occurring and to minimize the impact on the project. Risk responses are planned should the risk event actually occur.

Risk Roles and Responsibilities

The table below identifies the roles and responsibilities of all participants in the Risk Management process.

Risk Management Roles and Responsibilities Table	
Contractors	[client] Project Manager, Team and Steering Committee
Identify Risks	Identify Risks
Risk Ownership	Risk Ownership
Develop Mitigating Strategies	Develop Mitigating Strategies
Develop Contingency Plans	Develop Contingency Plans
Respond to Risk Events	Respond to Risk Events
Authority to change risk levels	Authority to change risk levels
	Monitor Risk Status
	Communication of Risk Status

The [client] Project Managers will coordinate with Contractors and Project Team Members to review the status of all risk mitigation efforts, review the exposure assessments for any new risk items, and update the project's Risk Matrix on a regular basis.

Risk Assessment

A monthly contractor and interdepartmental Risk meeting is held to assess risk level.

Risk Identification

New Product Specifications

1. [item]

Risk Analysis:

[description of risk]

Risk Response Plan:

- [Details of Spare's approach].

Existing Product Fit

1. [item]

Risk Analysis:

[description of risk]

Risk Response Plan:

- [Details of Spare's approach].

Implementation Risks

1. [item]

Risk Analysis:

[description of risk]

Risk Response Plan:

- [Details of Spare's approach].

Testing Methodology

As a software, Spare believes in our product and follows a testing procedure that includes internal and beta testing. We are problem solvers and we strive to build the best product to suit [ClientName]'s needs. There are milestones and tasks for testing as part of our implementation plan. Following is a walkthrough of our procedures for integrations, system acceptance, and operability performance testing.

Integration Testing

Spare uses a combination of role-based permissions and individual product permissions to manage user access to the administrative/staff platform. Spare can support single-sign on (SSO) for the staff platform through an integration with WorkOS.

Spare has iOS and Android apps for Spare Rider and Spare Driver—we have no issues integrating these apps into the existing tablets and phones used by [ClientName].

Any change to Spare's code base goes through the following process:

1. The Engineer pushes their changes to our source code repository, in a feature branch
2. A comprehensive suite of automated tests runs against the feature branch
 - A very large number of "unit tests", a moderate number of "integration tests", and a small number of "end to end" tests, in accordance with a standard [test pyramid](#) approach
 - If the change involves a "database migration" (altering the structure of the database, or the data within it), all tests run with both the new and old versions of the code, to ensure the database changes are compatible with both
3. The branch is reviewed by at least one other developer - at least two for higher risk changes
 - The change itself will, in almost all cases, include new automated tests covering the new/changed behavior
4. If approved, and all tests pass, the branch is merged into the primary branch
5. The change is then automatically rolled out to a staging environment
 - In most cases, the rollout is slowly ramped up over a 15-30 minute period
 - If error rates rise during the rollout, it is automatically rolled back, and Engineers are alerted
 - We also have a bot that continuously performs key workflows against the staging environment, "Spare Monitor". If any of them fail, the rollout is automatically rolled back, and Engineers are alerted

- This environment is similar to our true production, that customers use, but customers do not use it
 - The rollout process is gradual, with automated monitoring:
- 6. If the staging deploy succeeds without issue, a production deploy (releasing to customers) is possible
 - By default, changes will be automatically deployed to production the day after a successful staging deployment
 - However, if necessary, Engineers can manually trigger a production deploy before this (for example, to fix an urgent bug)
- 7. The production deploy goes through the same steps as the staging deploy
 - See step 5 above (automated monitoring/rollback)
- 8. Once the change is in production, a comprehensive set of alerts will page on-call Engineers if any issues are detected
 - Primarily we monitor for increases in error rates or latencies
 - The bot described in step 5 will also alert if any key workflows do not function properly
 - There are always Engineers on call, 24/7

The above applies to even the smallest change. The above applies to even the smallest change.

For higher risk changes, or significant new features, all of the above occurs, as well as extra measures to ensure quality:

1. The Engineer(s) working on the change run a manual QA process
 - We have a set of manual QA “scripts” for specific types of changes
 - For many changes, Engineers will produce a script specific to this change, to ensure very specific new functionality works as intended
2. The change itself is gated by a “feature flag”
 - This allows it to be enabled for a single organization at a time
 - At first, the change is enabled only for internal testing organizations
3. A non-Engineer stakeholder, often a Product Manager or Designer, will themselves manually test the change on an internal test organization, to ensure it meets all requirements
 - If not, changes will be made before rolling out to any customers
4. The change will then be enabled for a small number of customers
 - The most common process for determining candidate customers is for Spare’s Partner Success team to nominate customers (generally ones eagerly awaiting the feature), reach out to the customers, and roll it out with their approval to be an early adopter
5. Feedback is collected from early adopters
 - Release blocking bugs or functionality changes are incorporated before rolling out further
6. The rollout is gradually expanded to more customers, and finally all customers
 - Depending on the change, this can happen over a period of days, weeks, or even months
 - When fully released, the feature flag is removed

- The only exception is certain features that not all customers will want - in these cases the feature flag is left long term, so the feature can be enabled/disabled on a customer by customer basis

System Acceptance Testing

The system acceptance testing speaks to the testing of Spare's products and features to ensure uninterrupted functionality for [ClientName]. Our approach includes:

Automated Testing for Continuous Improvement. Spare uses automated test-driven development techniques to ensure that as we develop new features, they are being tested on the fly and as completed. Upon completion of a feature, but prior to release, automated testing is completed as discussed, then manual testing is completed by a variety of engineers on the team to ensure the product is ready to be staged. Spare also maintains a continuous monitoring system to alert engineers if any issues are identified. With Spare's 24/7 on-call schedule, we can guarantee an engineer will be ready at a moment's notice in the event of an emergency.

Quality Checks at Every Stage. Spare uses Google Cloud Platform for its cloud environment. We have a testing, staging and production environment, and every feature or database update or release will go through each environment prior to being shipped. Additionally, automated monitoring processes notify the engineering operations team if anything is out of the ordinary. Spare's Partner Success team is also actively observing systems every day to ensure a high quality of service.

Operability Performance Testing

We will work closely with [ClientName]'s project team to craft a tailored end-to-end testing plan that ensures the service design and Spare's platform configurations align with [ClientName]'s objectives and service goals. This will be set at the beginning of the project and will work as the project's North Star.

Testing can be done in the sandbox/testing and production environments, based on the specific characteristics of what is being tested and [ClientName]'s desired testing approach. These are a few of the different types of operability testing we do:

Desk testing. This involves booking fake trips with fake rider profiles and fake driver duties/trips. This is completed by [ClientName]'s project team members.

Specific user workflow testing. This testing is done by the Admin, Dispatcher/Scheduler, Driver, Customer Service Representative, and Data Analyst. Similarly described in our [Training](#) section, this is completed by specific end users to mirror real world operations. This testing involves all the steps for:

- **Admin:** Adding a platform user, adding admin notifications, adding a custom field, editing a custom field, deleting a custom field, creating a service, adding a new zone, adding service settings, adding a stop zone, adding time rules, adding a fleet, creating a new group/membership, creating an announcement, creating a fare rule, adding a fixed fare rule, and adding a per rider (variable) fare rule.
- **Dispatcher/Scheduler:** Creating a duty, duplicating a duty, deleting a duty, canceling a duty, changing a driver, changing a vehicle, extending duty hours, changing a vehicle (down for maintenance), simulating a vehicle incident (short term vehicle issue), simulating a vehicle incident (long term vehicle issue), adding a driver, adding a vehicle, adding a fleet, monitoring live requests, view requests by hour, view requests by driver, and view requests by service.
- **Driver App:** Creating a duty, downloading the Spare Driver App, logging into Spare Driver, starting a duty, booking a request to your duty, new requests, changing navigation view, viewing navigation by directions, viewing rider/request details, canceling a trip, simulating pick up, viewing all upcoming stops, and simulating a "no show".
- **Customer Service Representative:** Create a "leave as soon as possible" request, cancel a trip, create a scheduled request, create a return request, edit an existing request, arrive by request, create a duplicate request, recurring trip, adding a rider, adding default request preferences, adding a favorite location, adding a membership, adding a payment method, lifting a rider ban early, booking to the paratransit service, booking to the on-request service, booking trips - troubleshooting, outside of the service zone, rider not added to group, and ride requested outside of service hours.
- **Rider App / Web Booker:** Downloading the app, logging into the app / web booker, location settings, booking a trip, changing the trip type (leave at / arrive by), change the amount of riders, adding accessibility feature, adding a payment method, confirm booking, finding upcoming trips, canceling a trip, updating your profile, viewing past trips, adding a credit card, make payment type the default, remove a credit card, add a favorite location, and signing out.

End-to-end dry run testing. The holistic approach involves the vehicles on the road with all user classes (e.g. dispatcher, reservationist, driver, etc.), booking and completing live trips, though not necessarily with real riders. This is essentially a soft launch of the services. Dry run testing involves:

- Spare Rider App Testing
 - Account Creation (Register & Verification Code): Registration, log in, log out, notification permission, location permission, announcements.
 - Booking Trips: Available services in the area, service selection, finding and viewing trip destinations, booking screen display, after requesting a ride.

- Post-Ride Experience: Leave a review and/or a tip.
 - Extras: Edit profile, showing organization and nearby available ones, fare passes, payments, promos, past trips, group memberships, settings, legal, sign out.
- Spare Launch (Admin Panel) Testing
 - Booking trips: Select a rider, set pickup and dropoff locations, select the service, set the leave time, set passenger and accessibility preferences, select payment method, enter driver notes.
 - Pausing Duties & Rematching Trips.
 - Execute Vehicle Disruption Process: in the case of vehicle breakdown.
- Spare Driver App Testing
 - Perform the Pick-up & Drop-off of Riders.
 - Viewing Rider Trip Notes.
 - No-Shows & Cancellations.

If desired, [ClientName] can soft launch Spare in a subsection of its operating area and/or subsection of riders to work out any remaining kinks before launching the full service. However, for paratransit services, this is generally not recommended as there are risks associated with running two systems in parallel. It would be difficult if the system is segmented into two parts as users would need to use two systems. This would be prone to errors, trips slipping through cracks, and can lead to poor efficiency as two different software systems do not integrate nor speak with one another.

📞 Calling Sebastian Vettel

- ✓ Card number
- ✓ Expiry date
- Postal code
- CVC



Spare Booking Agent Guide

Visit sparelabs.com
815 W Hastings St Suite 810,
Vancouver, BC V6C 1B4
© Spare 2022

Table of Contents

1. Getting started	3
1.1. Accessing Your Account.....	4
1.2. Main Dashboard Overview.....	5
2. Service Monitoring with Spare Live Map	6
2.1. Access Spare Live Map.....	7
2.2. Investigate Vehicle/Duty Activity	8
3. Viewing Request History.....	9
3.1. Access the Request Panel.....	10
3.2. View Request Details.....	11
3.3. Investigate Trips with Activity Log.....	12
4. Managing Single Trip Requests	13
4.1. Create a New Request.....	14
4.2. Request Status and Troubleshooting.....	18
4.3. Edit Requests.....	19
5. Managing Recurring Trip Requests	21
5.1. Create a Recurring Trip Request.....	22
5.2. Edit a Recurring Trip Request.....	23
6. Managing Riders.....	24
6.1. View Rider Information.....	25
6.2. Edit Rider Information.....	26
6.3. Add Favourite Locations.....	27
6.4. Add Riders to Groups	28
7. Managing Payments.....	30
7.1. View Existing Fare Information.....	31
7.2. Apply Promo Codes.....	32
7.3. Set Up IVR Pay.....	34
8. Viewing Service, Fleet, and Duty Information.....	35
8.1. View Existing Service Settings.....	36
8.2. View Duties and Fleets.....	37
9. Administrator Notifications.....	38
9.1. Set up Platform Notifications.....	39
10. Help and Troubleshooting.....	40
10.1. How to Reach out for Support.....	41

Calling Sebastian Vettel

- ☒ Card number
- ☒ Expiry date
- ☐ Postal code
- ☐ CVC



[1] Getting Started

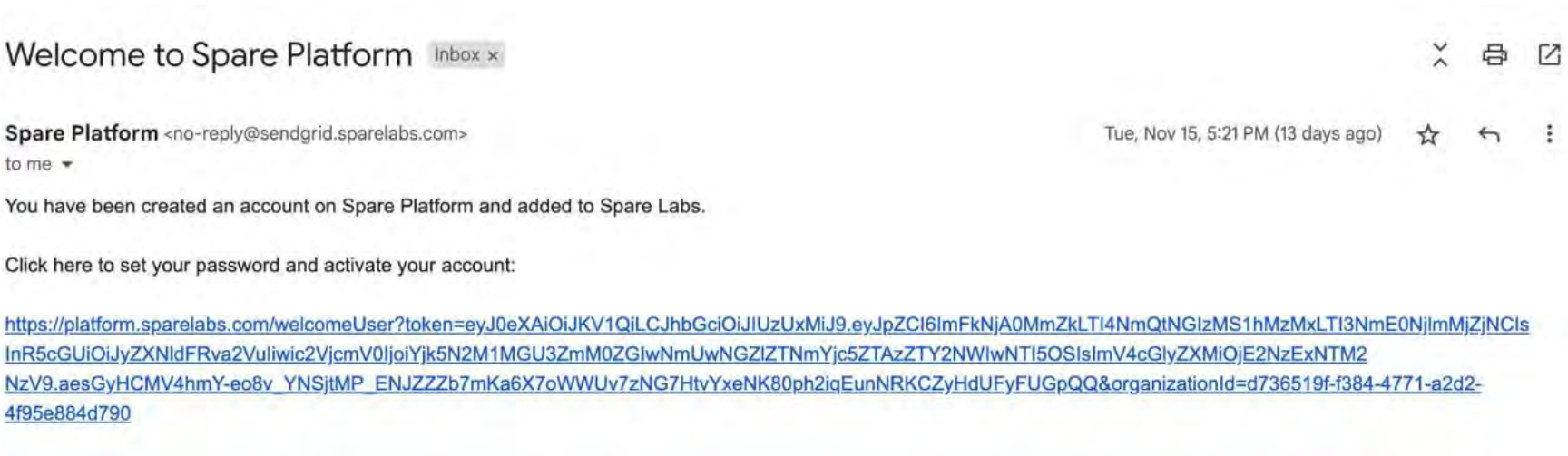
- Spare Platform Login Information
- Main Dashboards Overview

1.1. Accessing your Account

1 Setup your account

You should have received an invitation email from sparelabs.com.
An invitation link will redirect you to the Spare Platform and the account setup.

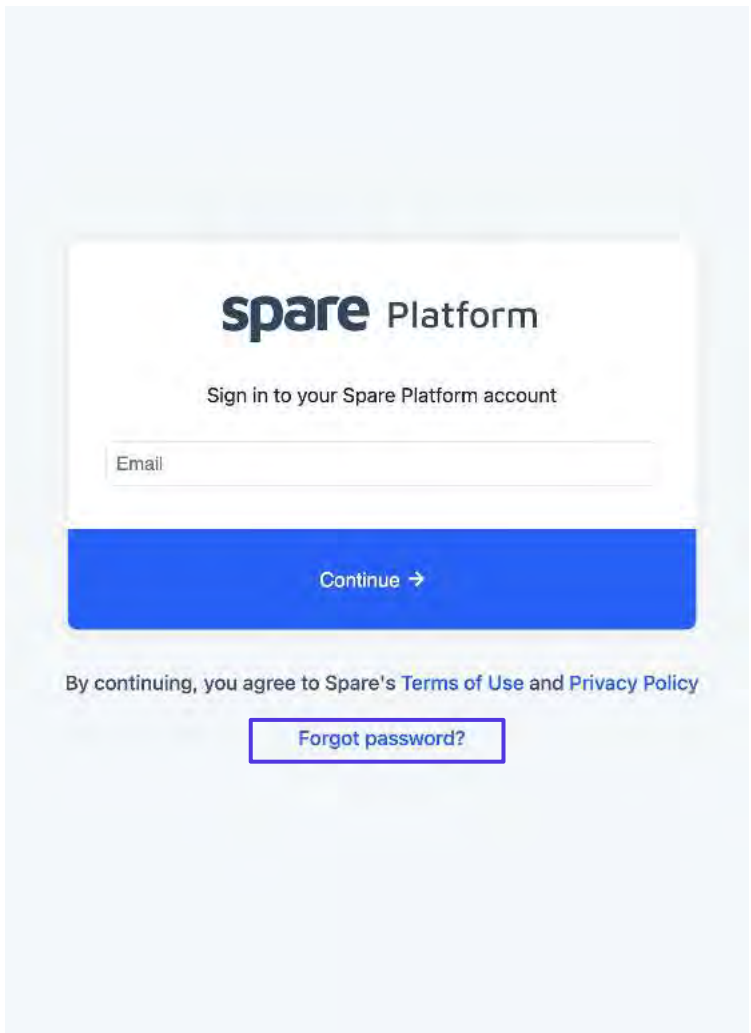
You can log into your account via your email and a password you will set the first time.



 Please contact your **administrator** if you don't have login credentials or did not receive a registration email.

2 Log in to your account

You can log into your account via your email and a password you will set at the first time.



Reset your password

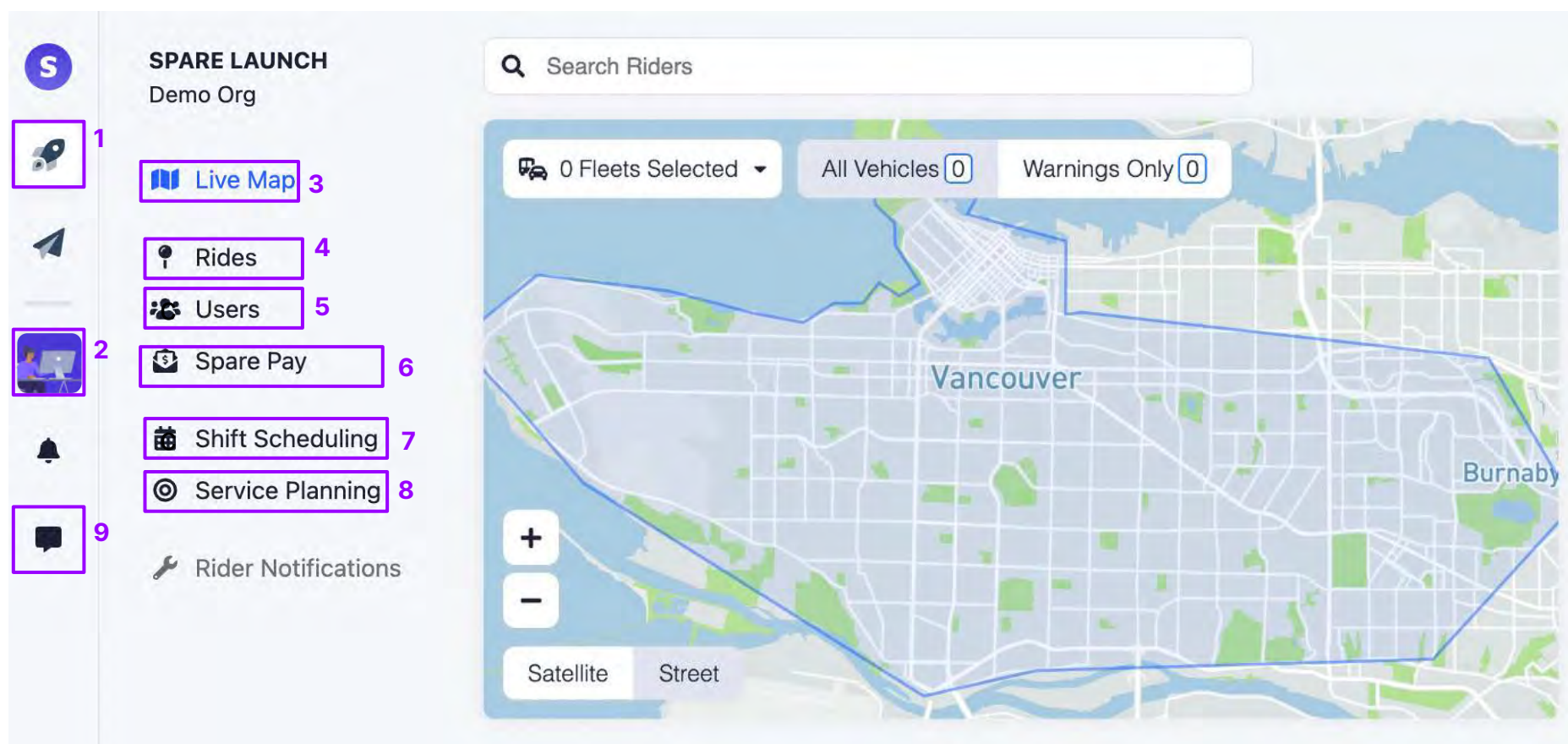
If you don't remember your password, you can tap on the **"Forgot Password?"** button. You will receive an email with a password reset link.

If you request a password reset too many times, the system might no longer send you a password reset email. Please get in touch with your administrator instead.

 Remember to follow your manager's instructions and **log out** after your duty if instructed to do so.

1.2. Main Dashboards Overview

Here is what you will see when you first log in to Spare Platform. Below are the key areas you'll learn to navigate as a Booking Agent:



[1] Spare Launch is Spare's core service where all the rides happen. This is your main working space.

[2] Your Spare Account is where you can access your account settings and help resources.

[3] Spare Live Map is a living representation of the service on-demand operations.

[4] Rides section is where you create, edit, cancel, or investigate trip requests.

[5] Users section contains information about riders and drivers.

[6] Spare Pay allows you to view and edit current service fares and learn about current fare policies and passes (if applicable).

[7] Shift Scheduling is where you can view driver duties and vehicle information.

[8] Service Planning is where you can view current service settings.

There are several ways you can **access help resources**:

 By clicking on the **message icon[9]**: it will redirect you to Spare's Tech Support chat.

 By going to your **Spare Account [2]** and selecting **Help**: it will redirect you to Spare's Help Center.

📞 Calling Sebastian Vettel

✓ Card number

✓ Expiry date

○ Postal code

● CVC



[2] Service Monitoring with Spare Live Map

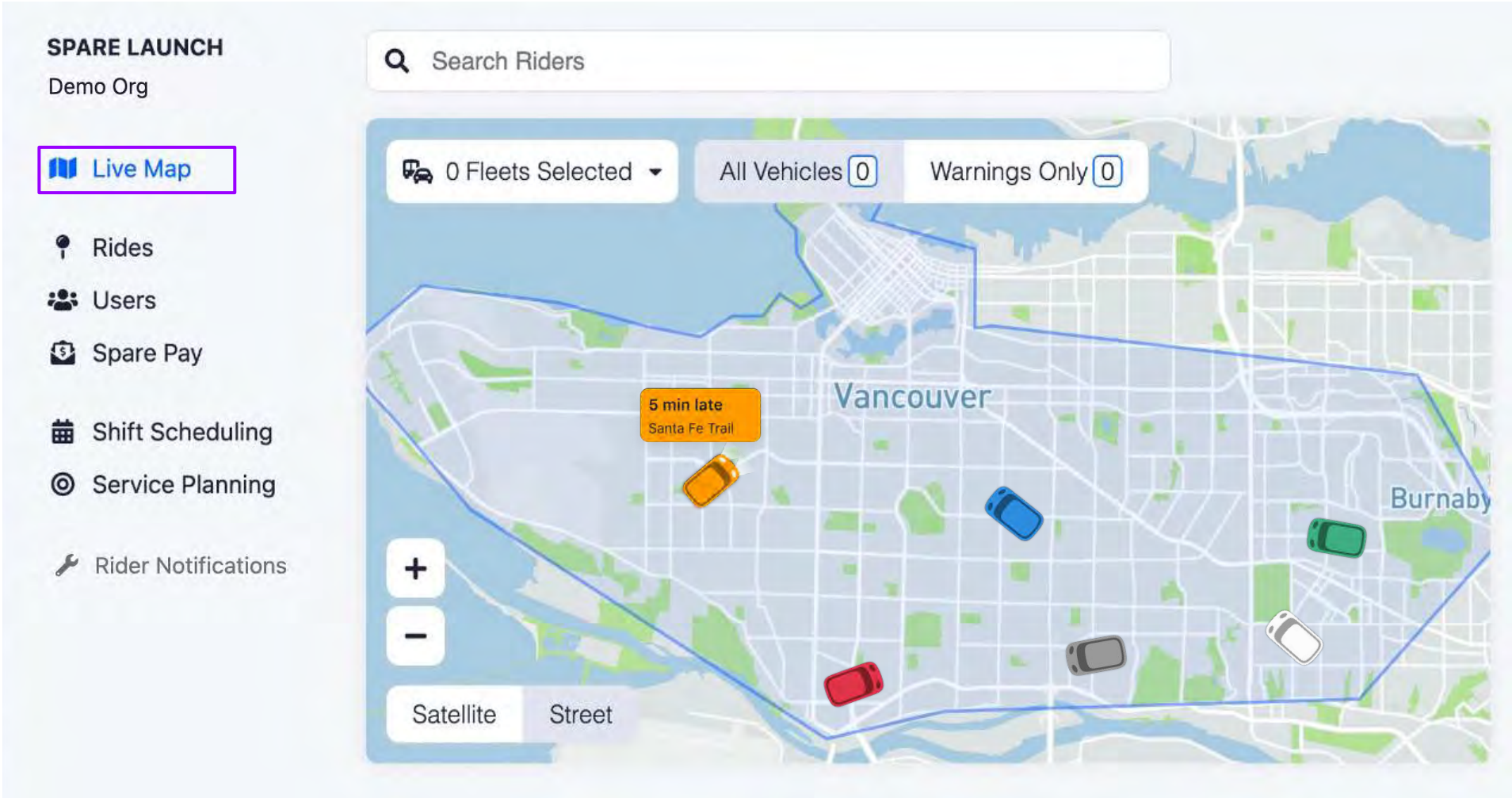
→ Access Spare Live Map

→ Investigate Vehicle/Duty Activity

2.1. How to Use the Live Map



The Live Map is where you can view your entire operations or take a closer look at specific services. The dark blue area represents your service zone(s), and the vehicles represent the drivers that you currently have on duty. Where the vehicles are on the Live Map accurately reflect where they are in real life.



1 Vehicle Color & Information

Vehicle Color	Vehicle Status
Green	The vehicle/duty/driver is currently operating normally and is on time.
Yellow	The vehicle/duty/driver is between 2-10 minutes late to their next pickup/dropoff, or a vehicle has not updated its location (no connection) for 1-2 minutes.
Red	The vehicle/duty/driver is over 10 minutes late to their next pickup or dropoff or has not updated its location (no connection) in over 2 minutes and so is now unmatchable.
Blue	The vehicle is “Idle” and currently has no trips booked to its manifest.
Grey	The vehicle has been paused and is unmatchable.
White	The vehicle is on a driver break.

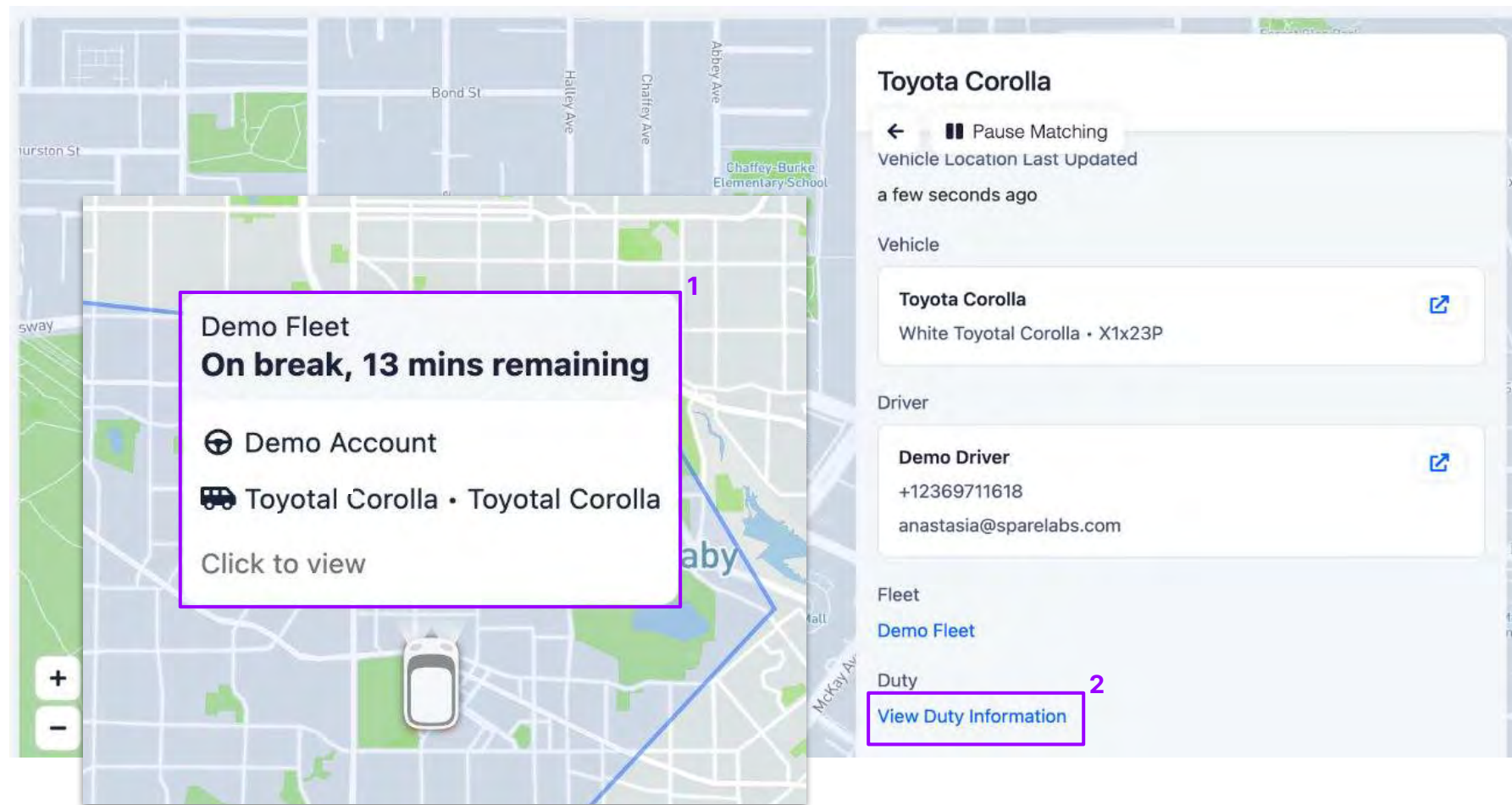


Hovering over or clicking on a vehicle will give you more information on the duty's status and trip manifest.

2.2. How to View Vehicle's Past & Future Activity

1 Vehicle/Duty Details Screen

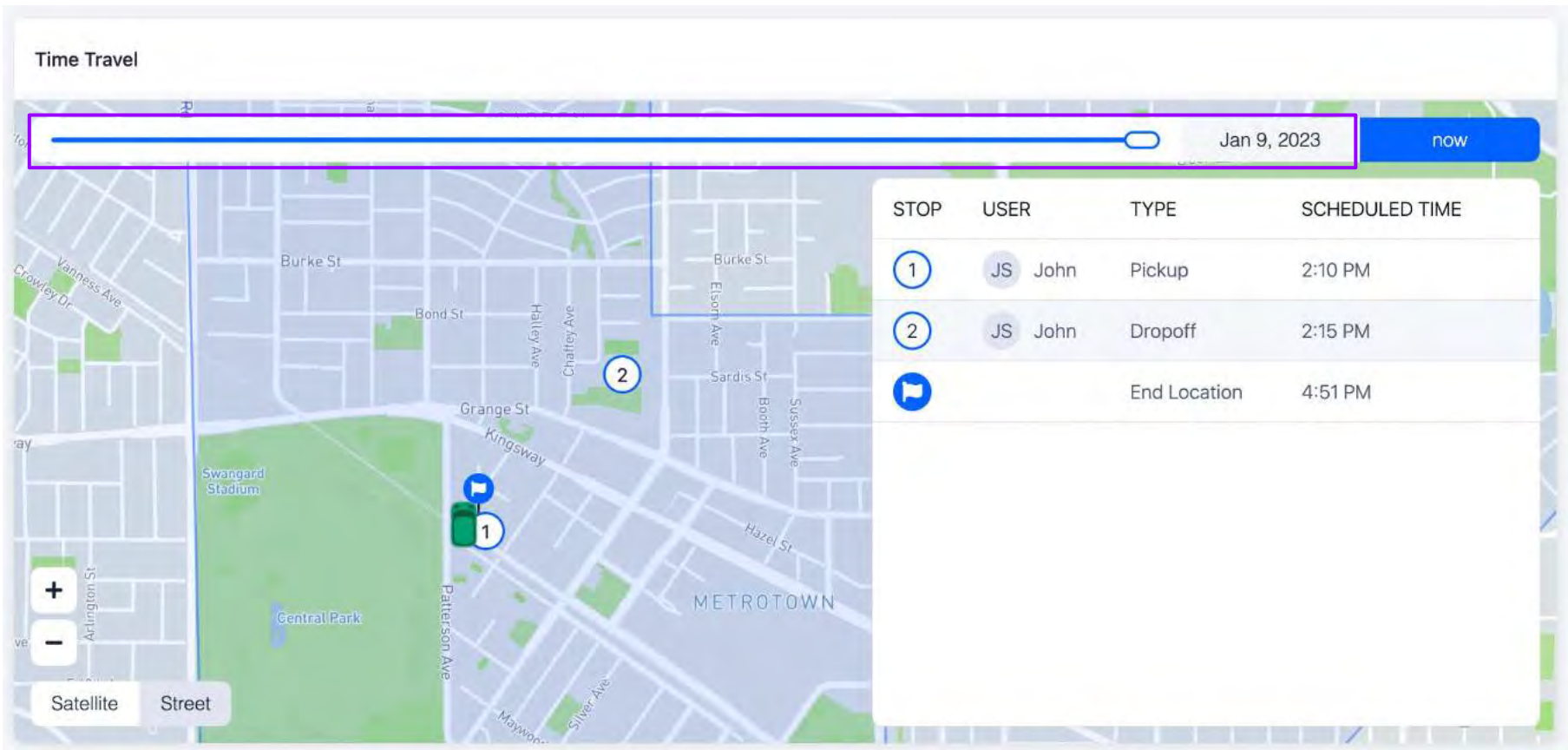
On the **Vehicle Information Card [1]** of the Live Map you will see such information as current status (e.g., “On break”); vehicle name; driver name; duty name. Click on the card to view the details.



i The **Vehicle Details screen** can be extremely useful in diagnosing operational problems and answering questions, such as the current capacity of a vehicle or its current route.

All of the vehicle’s currently **assigned pickups and dropoffs** are shown in a list which is then represented on the map by the chronological stops and the vehicle path. You can also click on **View Duty Information[2]** to see details about that request.

By using the **Time Travel** feature ↓, you can see the status of a vehicle at a specific point in time. This is useful for answering questions from Riders.



📞 Calling Sebastian Vettel

✓ Card number

✓ Expiry date

○ Postal code

● CVC



[3] Viewing Requests History

- Access the Request Panel
- View Request Details
- Investigate with Activity Log

3.1. How to View Requests History

1 Access the Request Panel

To access the requests panel, navigate to **Spare Launch**[1] on the left-hand side of your screen. Select **Rides** [2], then **Requests** [3]. The Requests panel includes all of the requests that have been made in your organization to date.

The screenshot displays the 'SPARE LAUNCH' interface for 'Demo Org'. On the left sidebar, navigation options include Live Map, Rides, Requests, Recurring Trips, Reviews, Users, Spare Pay, Shift Scheduling, Service Planning, and Rider Notifications. The 'Requests' option is highlighted. The main area features a search bar labeled 'Search Riders' and a 'Requests' header. Below the header, there are links for 'Filter', 'Import Requests', and 'Add Request'. A table lists various requests with columns for STATUS, RIDER, DRIVER, PASSENGERS, REQUESTED PICKUP TIME, and CREATED INTERFACE.

STATUS	RIDER	DRIVER	PASSENGERS	REQUESTED PICKUP TIME	CREATED INTERFACE
Accepted	Julie Liu	Demo Driver	1 Adult, 1 Child	Thu, Jan 12, 2023 11:57 AM	Admin Panel
Completed	John Smith	Demo Driver	1 Adult	Mon, Jan 9, 2023 2:10 PM	Admin Panel
Completed	John Smith	Demo Driver	1 Adult	Tue, Dec 20, 2022 10:15 AM	Admin Panel
Completed	Ellie Smith	Demo Driver	1 Adult	Mon, Dec 19, 2022 2:40 PM	Admin Panel
Cancelled	Julie Liu	Demo Driver	1 Adult	Fri, Dec 16, 2022 11:56 AM	Rider Mobile App
Accepted	Ellie Smith	-	1 Person with disabilities	Thu, Dec 15, 2022 12:50 PM	Admin Panel
Completed	Ellie Smith	Demo Driver	1 Person with disabilities	Wed, Dec 14, 2022 6:20 PM	Admin Panel
Completed	Julie Liu	Demo Driver	1 Adult, 1 Child	Tue, Dec 13, 2022 1:04 PM	Driver App

 You can **filter requests[4]** by clicking on the corresponding button at the top of the page.

2 Filter Results

There are many filter options that you can select from. For example, if you would like to filter your requests by Rider, **select 'Rider', type the rider's name** you would like to filter for, then click **'Done'**. You can also select 'Clear' to clear your filter search.



SPARE LAUNCH

Demo Org

 Live Map

 Rides

 Requests

 Recurring Trips

 Reviews

 Users

 Spare Pay

 Shift Scheduling

 Service Planning

 Rider Notifications

Clear

Filters

Done

☐ Created At

☐ Requested Pickup Time

☐ Status

☐ Driver

☒ Rider

☐ Service

☐ Request Cancellation Reason

☐ Created Interface

☐ Stranded Request

Import Requests

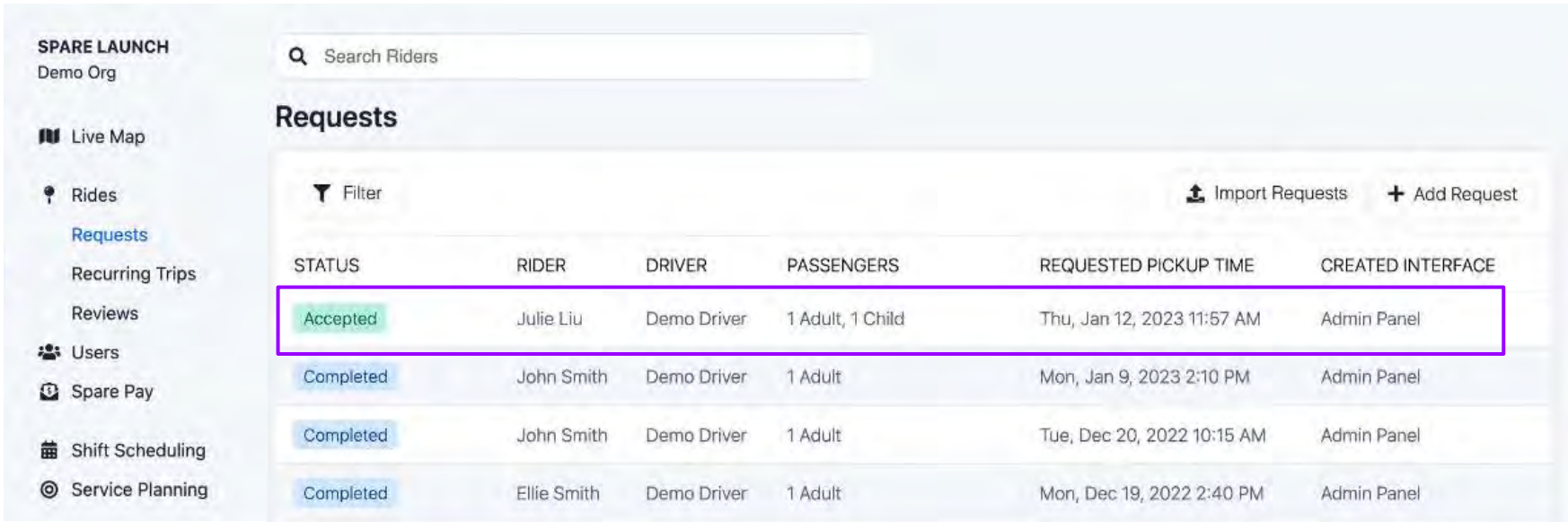
Add Request

PASSENGERS	REQUESTED PICKUP TIME	CREATED INTERFACE
1 Adult, 1 Child	Wed, Jan 18, 2023 11:57 AM	Admin Panel
1 Adult, 1 Child	Mon, Jan 16, 2023 11:57 AM	Admin Panel
1 Adult, 1 Child	Thu, Jan 12, 2023 11:57 AM	Admin Panel
1 Adult	Mon, Jan 9, 2023 2:10 PM	Admin Panel
1 Adult	Tue, Dec 20, 2022 10:15 AM	Admin Panel

3.2. How to View Request Details

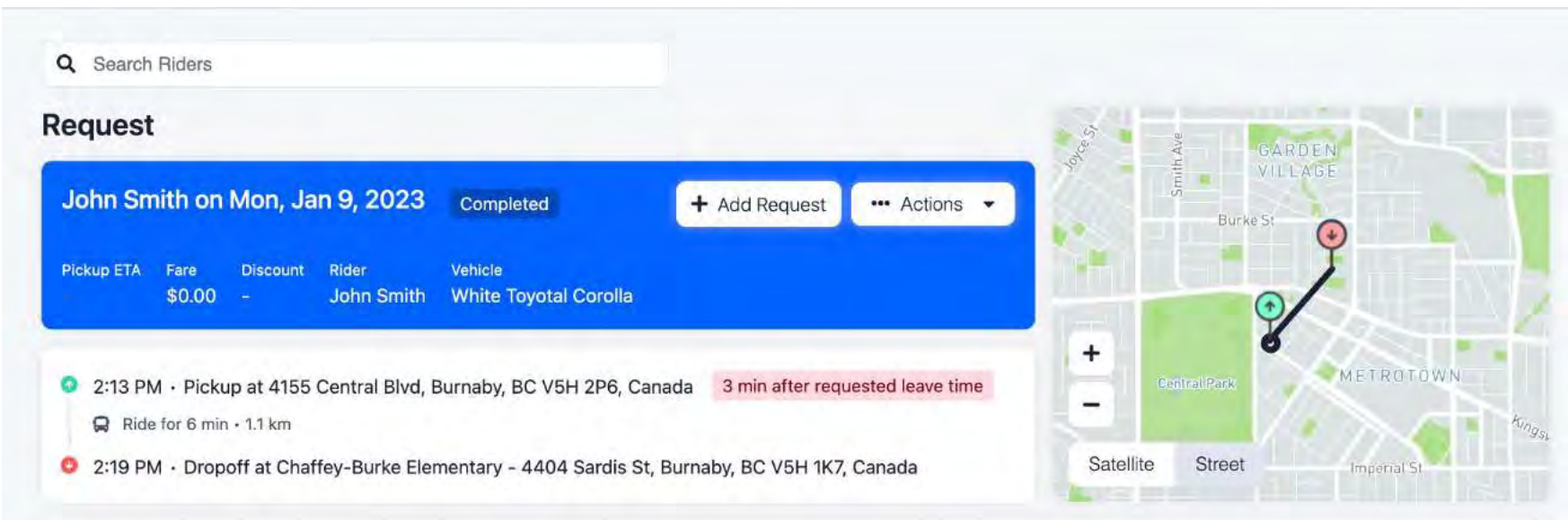
1 Open the Request Information Page

From the requests panel, click on the **request record line** you want to view.



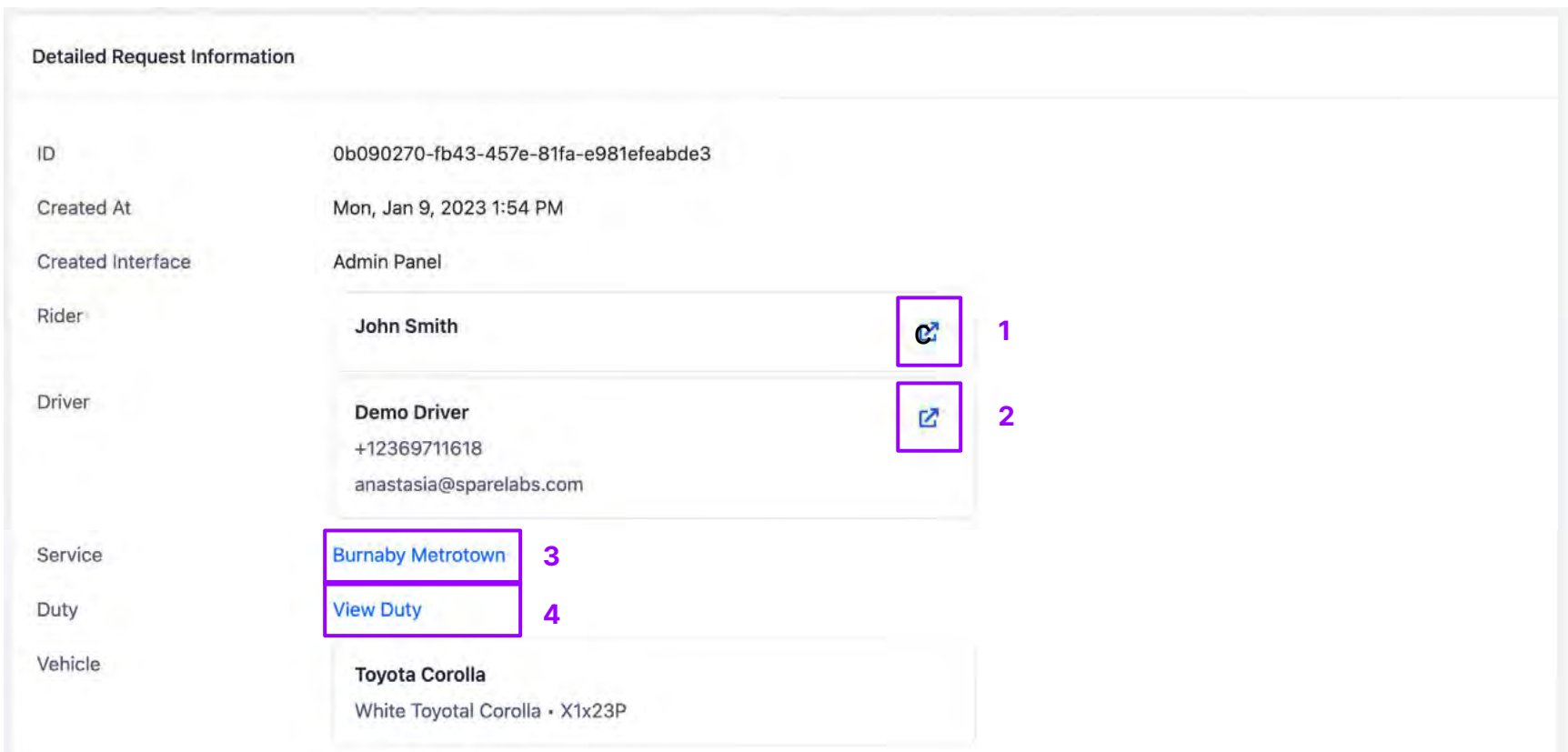
2 View Request Status Summary

On the top of the information page, you will see the request summary with the key metrics.



3 Explore Associated Users & Vehicles

Scroll down to see the detailed information. Click on the **Rider [1], Driver [2], Service [3], or Duty[4] hyperlink** to get transferred to the linked pages.



3.2. How to Investigate with Activity Log

4 View Status Changes

Scroll down the Request Information Page to see status changes and their timestamps for the specific request. Status changes are displayed in chronological order.

Status Changes	
STATUS	TIME
Processing	Mon, Jan 9, 2023 1:54 PM
Accepted	Mon, Jan 9, 2023 1:54 PM
Service Disruption	Mon, Jan 9, 2023 2:09 PM
Accepted	Mon, Jan 9, 2023 2:09 PM
Driver Arriving	Mon, Jan 9, 2023 2:11 PM
In Progress	Mon, Jan 9, 2023 2:13 PM
Completed	Mon, Jan 9, 2023 2:19 PM

5 View Activity Log



An Activity Log is a **written record of all recent activities** that happened on a specific object. Activity logs help you **track any minor changes** and save time recreating the sequence of events.

Here is what Spare Platform is **currently tracking**:

Estimate Generated | Request Created | Request Accepted | Request Rematched | Duty Cancelled | Request Edited | Notification Sent to the Rider;

Each **Activity Log record** is clickable and contains **detailed information** about the changes.

Activity Log		
TIME	ACTIVITY	CREATED INTERFACE
Mon, Jan 9, 2023 1:54 PM	Estimate Created	Admin Interface
Mon, Jan 9, 2023 1:54 PM	Request Created	Admin Interface
Mon, Jan 9, 2023 1:54 PM	Request Accepted	Spare Engine
Mon, Jan 9, 2023 2:09 PM	Request Edited	Admin Interface
Mon, Jan 9, 2023 2:09 PM	Request Rematched	Admin Interface
Mon, Jan 9, 2023 2:09 PM	Request Accepted	Spare Engine

📞 Calling Sebastian Vettel

- ✓ Card number
- ✓ Expiry date
- Postal code
- CVC



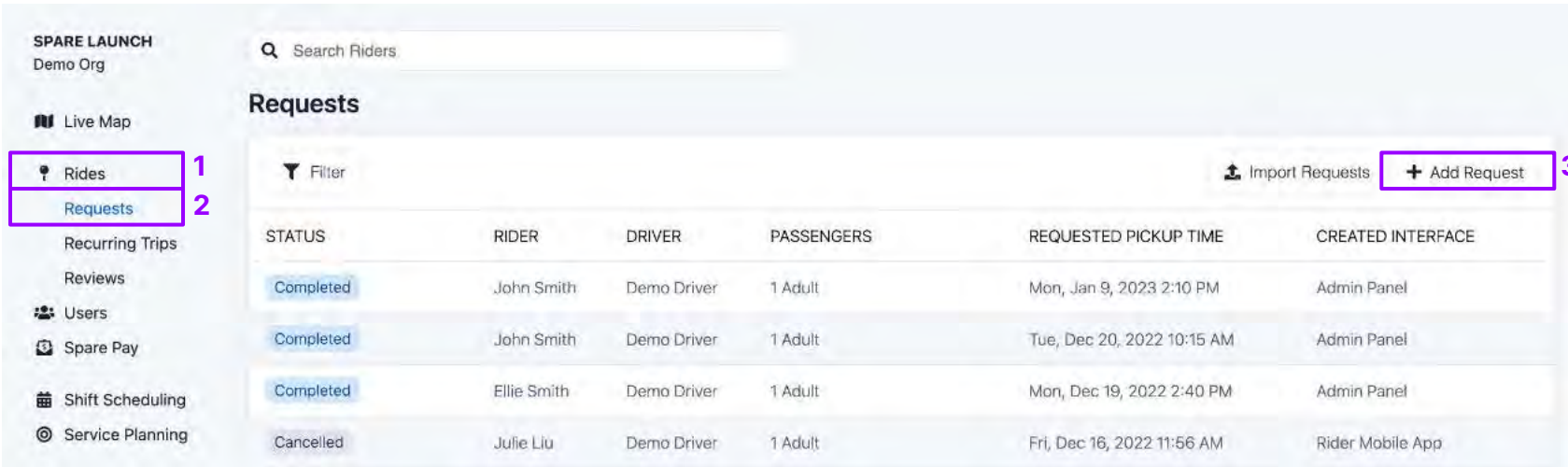
[4] Managing Single Trip Requests

- Create a Trip Request
- Request Status and Troubleshooting
- Edit a Trip Request
- Create a Return Trip Request
- Rematch the Request
- Lock Request to Duty

4.1. How to Create Requests

1 Add a New Request

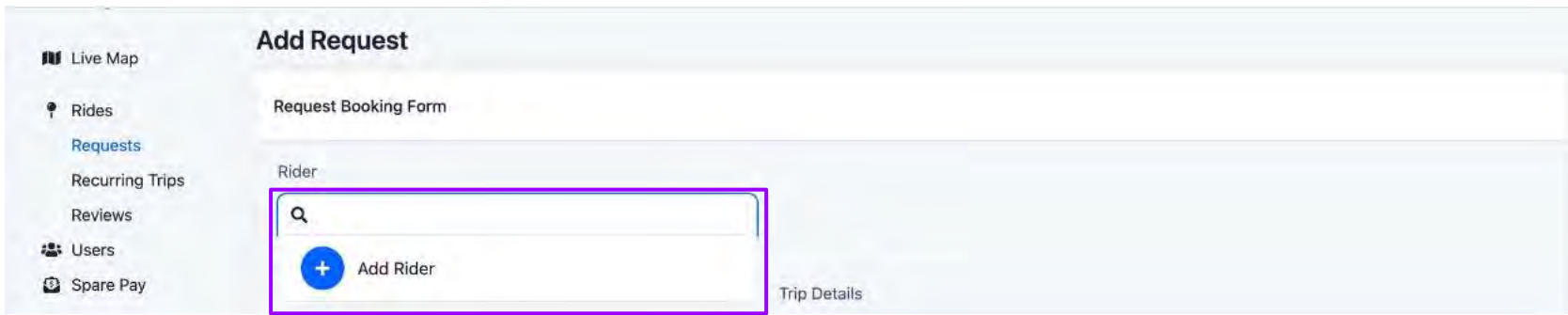
Go to the **Rides tab** [1] and select **Requests**[2]. Click **+Add Requests** [3]



2 Select a Rider

From the **Request Booking Form**, Find the rider by typing a *name or phone number* into the **Search riders field**[1] and select on the desired user in the dropdown menu.

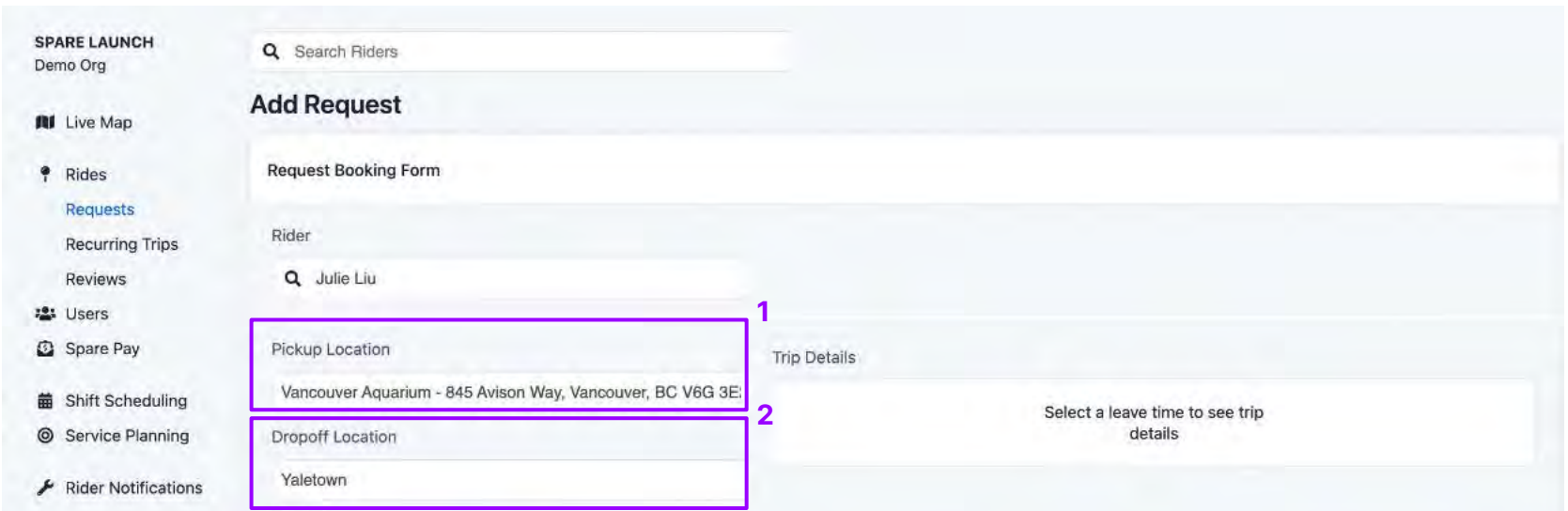
If the rider does not have a user profile, select **Add User** and enter in their details.



3 Select Pick-up & Drop-off Locations

In the **Pickup Location field** [1], type in the address of the riders pickup location and select the virtual stop or address in the dropdown menu.

Do the same for the **Dropoff Location** [2].

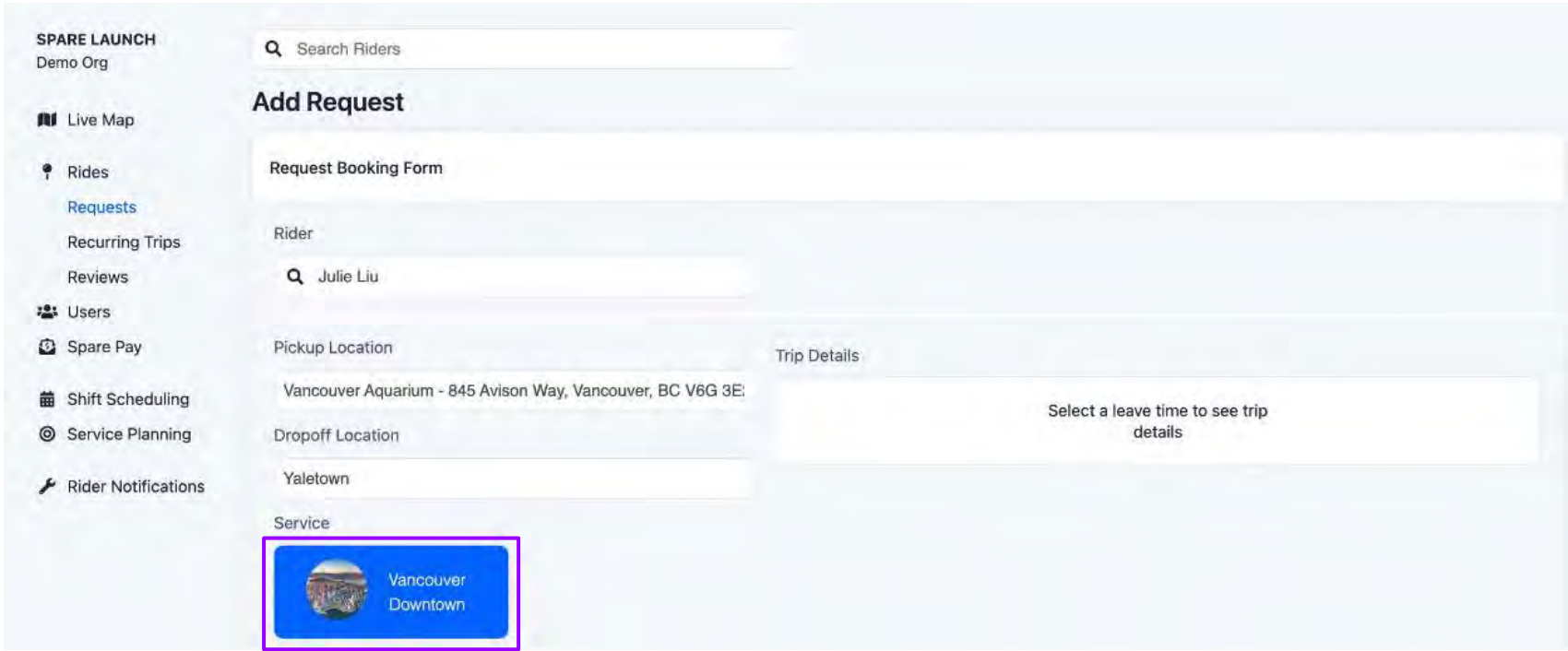


Pro Tip: Allow the browser to fetch your location. This will populate with relevant results faster. Click on the suggested result to accept it.

4.1. How to Create Requests

4 Select the Service

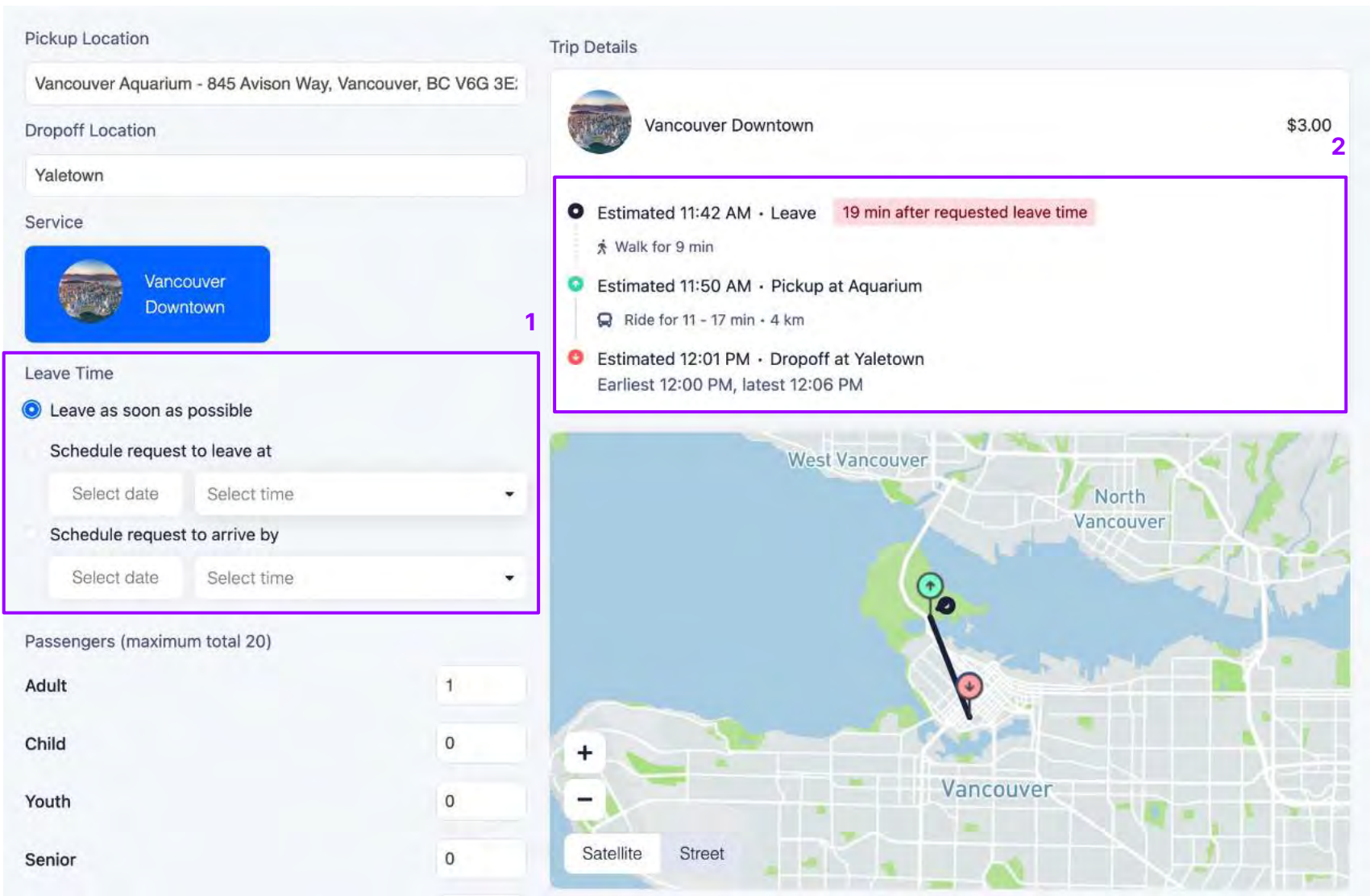
If both pickup and dropoff locations are within an active service zone, the applicable service(s) will show up. Select the service you would like to book the trip on by clicking on its name.



5 Set the Leave Time

The rider can either: **(a)** leave as soon as possible; **(b)** leave at a point in the future (if enabled); **(c)** (if enabled) set an arrive by a time;

Select the most relevant **leave time option[1]** for the rider. If there are available vehicles, **the request pickup and dropoff time estimates will appear [2]**.



4.1. How to Create Requests

6 Add Passenger(s) Information

Enter in the number of passengers along with any accessibility features required for the trip.

Pickup Location

Vancouver Aquarium - 845 Avison Way, Vancouver, BC V6G 3E

Dropoff Location

Yaletown

Service

Vancouver Downtown

Leave Time

Leave as soon as possible

Schedule request to leave at

Select date

Select time

Schedule request to arrive by

Select date

Select time

Passengers (maximum total 20)

Adult

1

Child

0

Youth

0

Senior

0

Trip Details

Vancouver Downtown

\$3.00

Estimated 11:42 AM • Leave

19 min after requested leave time

Walk for 9 min

Estimated 11:50 AM • Pickup at Aquarium

Ride for 11 - 17 min • 4 km

Estimated 12:01 PM • Dropoff at Yaletown

Earliest 12:00 PM, latest 12:06 PM

Map

West Vancouver

North Vancouver

Vancouver

Satellite

Street



Note: This will restrict the request to services and vehicles that can accommodate the passenger's accessibility needs.

7 Lock Request to Duty (Optional)

If for any reason there is a necessity that the request is to be assigned to a specific driver, you may do so by using the **Lock Request to Duty** feature. **Mark the checkbox[1]** and **select the driver[2]**. **Add a note [3]** for internal records about why you are locking the request to the duty.

Duty

Lock this request to a duty

Manually Select Duty

Select

Demo Driver, Toyota Corolla

Demo Driver 2, Toyota Yaris

Let others at your organization know why you assigned the request to this duty.

4.1. How to Create Requests

8 Select Payment Options

If payments are enabled for the service, select a relevant payment method for the user. Depending on payment options available, this could be **Cash**, **Credit Card**, or a **Mobile Ticketing** option.

If cash is not an option, and payment is required, select **Add Credit Card** with Spare Pay IVR. After selecting this option, an automated system will call the rider and request for them to input a credit card.

Payment Method

Cash

+ Add Payment Method

9 Add Driver Notes

Finally, **add any notes** you'd like to be visible for the driver. Click **Create Request** to book the trip.

Notes

Write your notes here

Ticket Number

0

Ticket Type

Please select value

Trip details created a few seconds ago. Refresh trip details

Create Request



When the request is created, a new pickup and dropoff time might appear. Sometimes it may be different from the original estimate as Spare Engine constantly attempts to increase fleet efficiency and improve the key metrics.

Request

Julie Liu on Thu, Jan 12, 2023

Accepted

+ Add Request

... Actions

Pickup ETA	Fare	Discount	Rider	Vehicle
12:09 PM	\$3.00	-	Julie Liu	White Toyotal Corolla

Estimated 12:09 PM - Pickup at Aquarium

13 min after requested leave time

Earliest 12:05 PM, latest 12:14 PM

Ride for 11 - 17 min - 4 km

Estimated 12:20 PM - Dropoff at Yaletown

Earliest 12:15 PM, latest 12:30 PM

Map of Vancouver showing pickup and dropoff locations

4.2. Request Status and Troubleshooting

Check the Request Status

Check the request status either from the **Requests tab** or from the **Request Information page**.

Status Changes	
STATUS	TIME
Processing	Thu, Jan 12, 2023 11:42 AM
Accepted	Thu, Jan 12, 2023 11:42 AM



What statuses can a trip request have?

Processing: The matching process is updating the request based on the latest information regarding driver availability.

No Drivers Available: The matching process did not find any drivers for the passenger to match with.

Accepted: The request has been accepted into a driver duty.

Driver Arriving: Driver is within a certain distance/time to the passenger pickup location. Note: that this status is only used for on-demand services.

Trip in Progress: Trip is in progress.

Cancelled: The request has been cancelled. To find more information about the specific cancellation reason, navigate to the detailed information regarding the specific request.

Trip Completed: The trip/request was completed by a driver.

Cannot Create a Request?

If you go through the enlisted steps and cannot get a trip estimate, there are a few possible reasons why.

If no service appears after you enter the pickup and dropoff addresses, the following are potential reasons why:

- 1. One or both of the addresses falls outside of the service zones of your organization’s services
- 2. The service you are trying to book for has been disabled

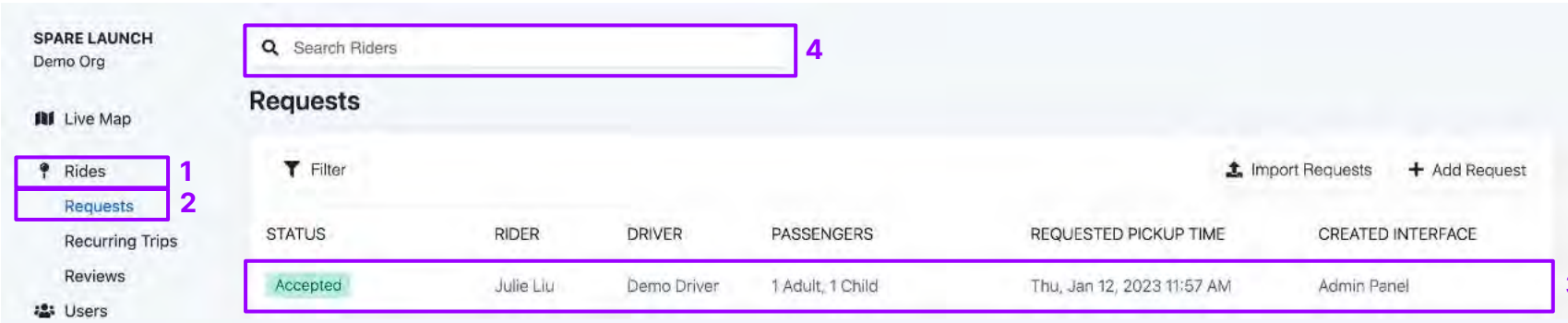
If after having entered the pickup and dropoff addresses, clicking on the respective service, and entering a desired leave time, **no trips can be found**, the following are potential reasons why:

- 1. The estimated pickup and/or dropoff time falls outside of the service’s operating hours
- 2. There are no duties scheduled for this service during the estimated pickup and/or dropoff time
- 3. An active vehicle has gone offline due to not updating its location and so has become unmatchable. Check the Live Map to confirm by clicking on the vehicles within the zone to check the status (red color indicates the vehicles is potentially unmatchable)
- 4. The number of passengers and/or accessibility features cannot be accommodated (either at this time due to other trips or generally by the service)

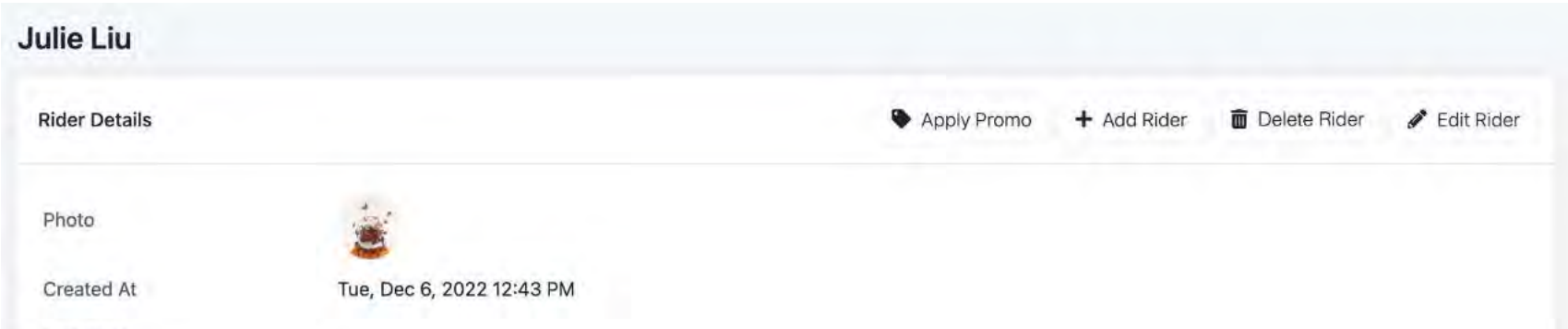
4.3. How to Edit Requests

1 Select the Request

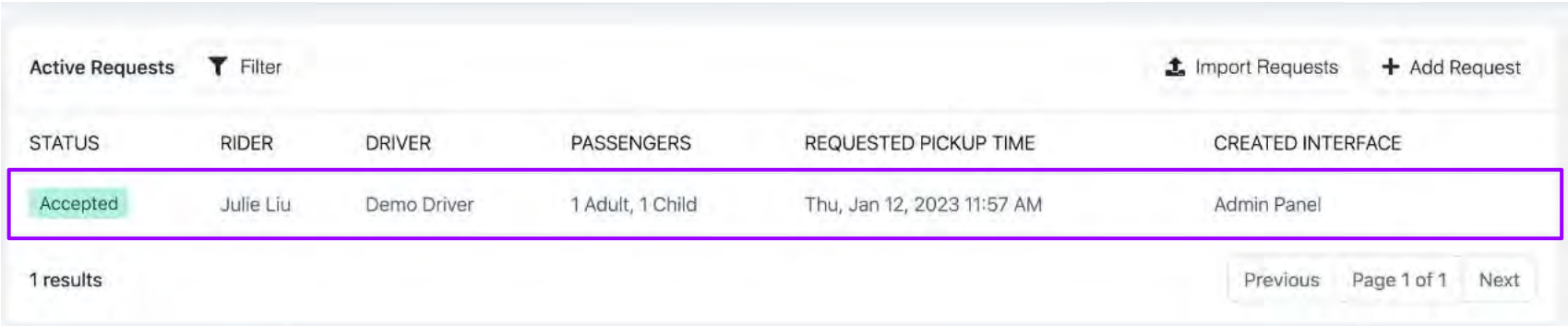
If you need to change an existing request, first, locate it in the Requests list. To do so, go to the **Rides tab**[1] and select **Requests**[2]. Click on the **request record**[3] you'd like to change.



You can also search the request by rider. Type the rider's name in the **search bar**[4] and select the rider card. Once in the **rider profile**, scroll down to their **requests history**. **Select the request** you'd like to change.

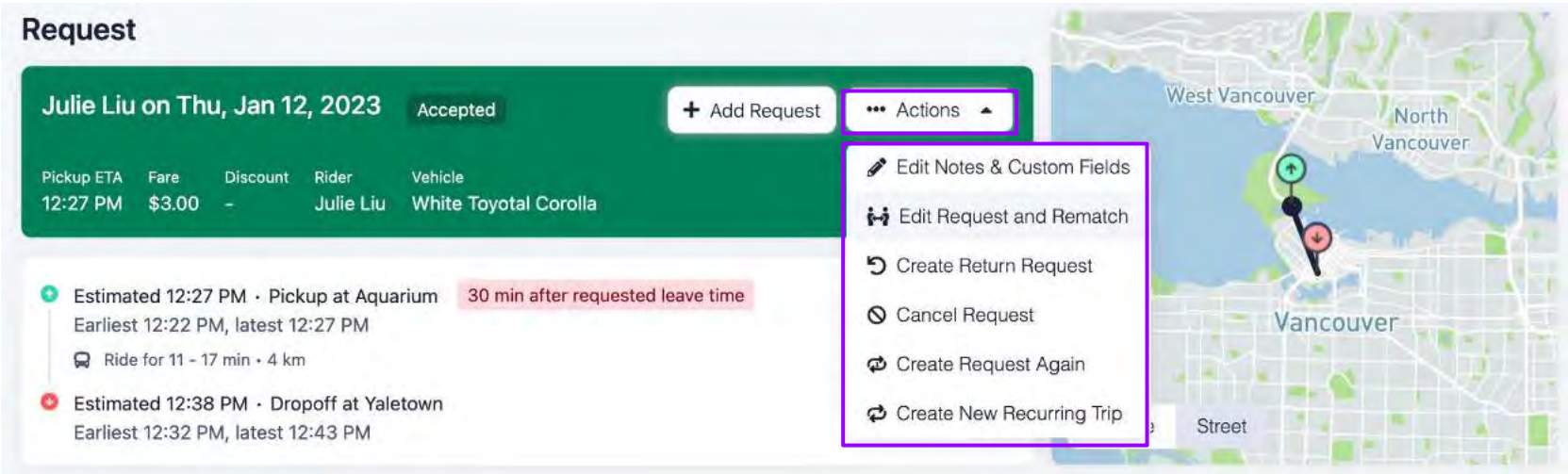


Scroll Down ↓



2 Edit or Cancel the Request

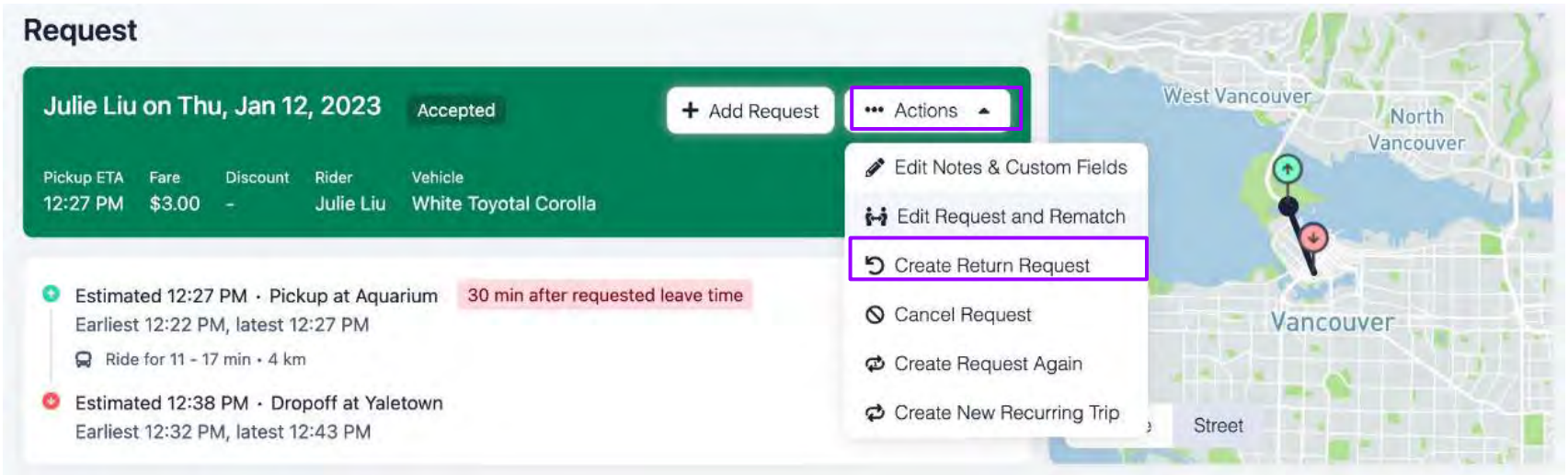
Once on the Request Information page, click **Actions** and **select one of the options** from the drop-down menu. **Save** the changes to apply them.



4.3. How to Edit Requests

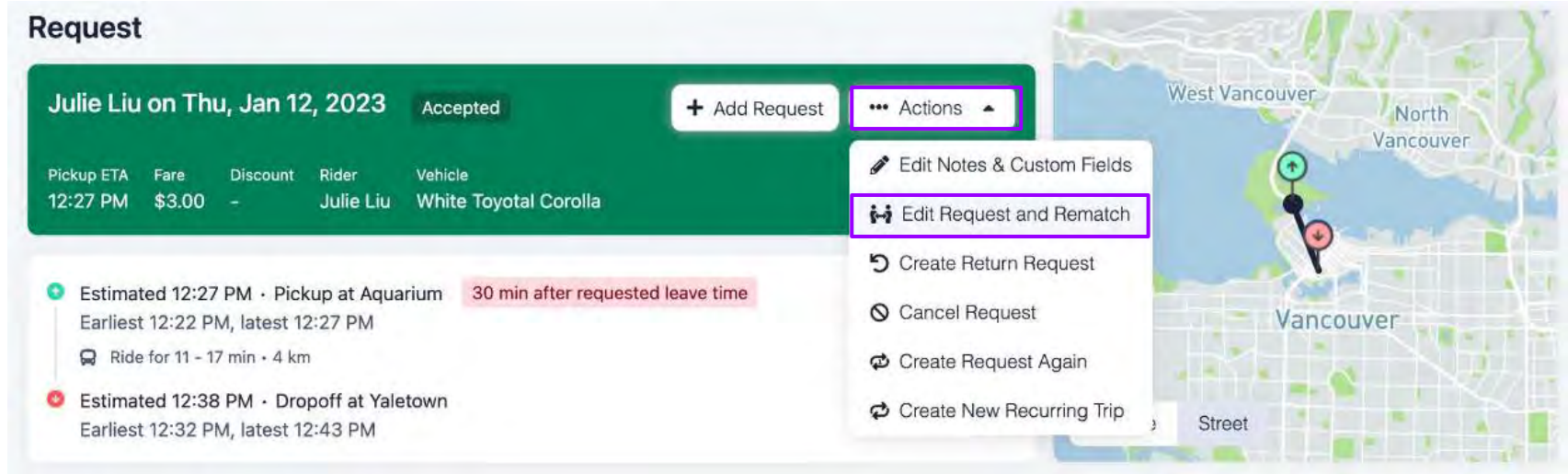
3 Create a Return Request

Selecting ‘Create Return Request’ will take you back to the booking screen. The rider’s pickup and dropoff locations will be reversed to reflect a return trip. If you would like to change one or both of the locations, you can do so by clicking into the field, entering an address or point-of-interest, and selecting the location.



4 Rematch the Request

Selecting ‘Rematch Request’ will remove a request from duty and rematch the request to the best possible duty based on the services set parameters.



i Remember that you can lock the request to a specific duty (driver). To do so, edit the request information page and check “Lock the request to duty”. Select the driver you’d like the request to be matched with. If the driver is available, the system will allow you to accept the changes. ↓



📞 Calling Sebastian Vettel

✓ Card number

✓ Expiry date

○ Postal code

● CVC



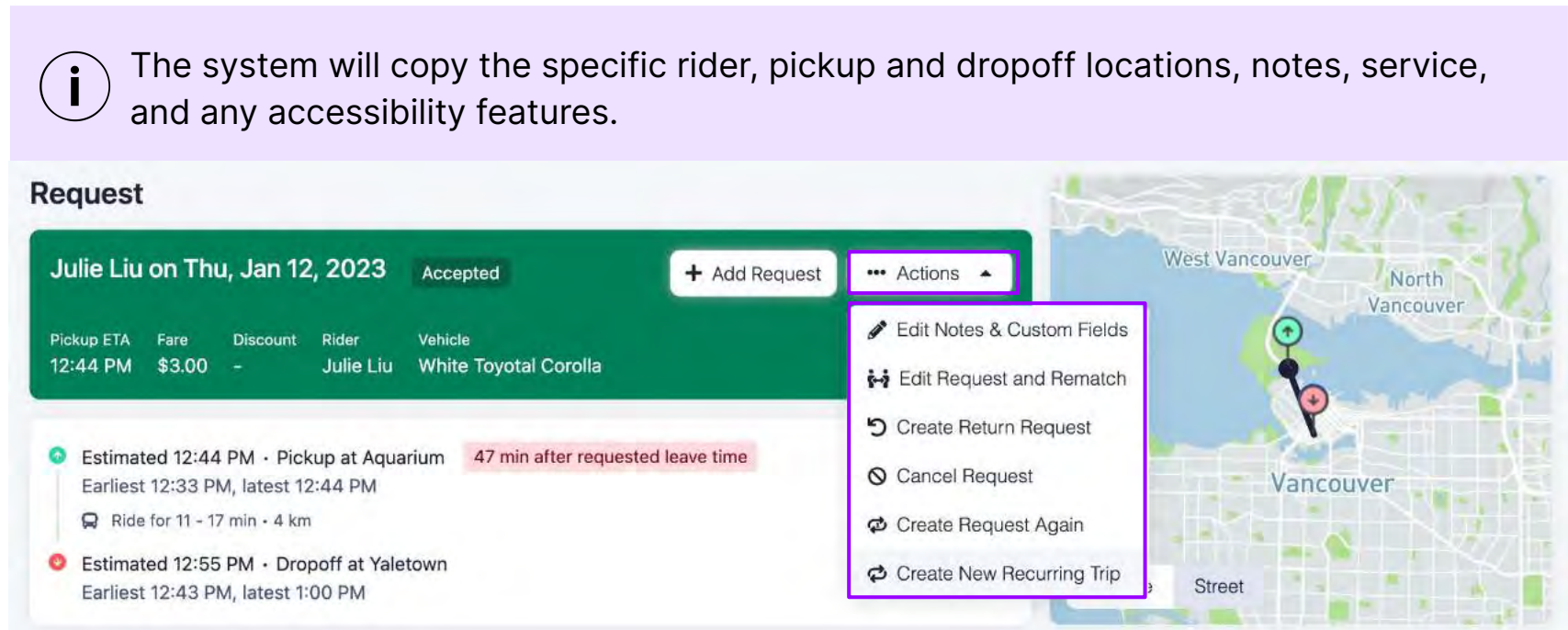
[5] Managing Recurring Trip Requests

- Create a Recurring Request
- Edit a Trip Request
- Create and Edit a Recurring Trip

5.1. How to Create Recurring Trip Requests

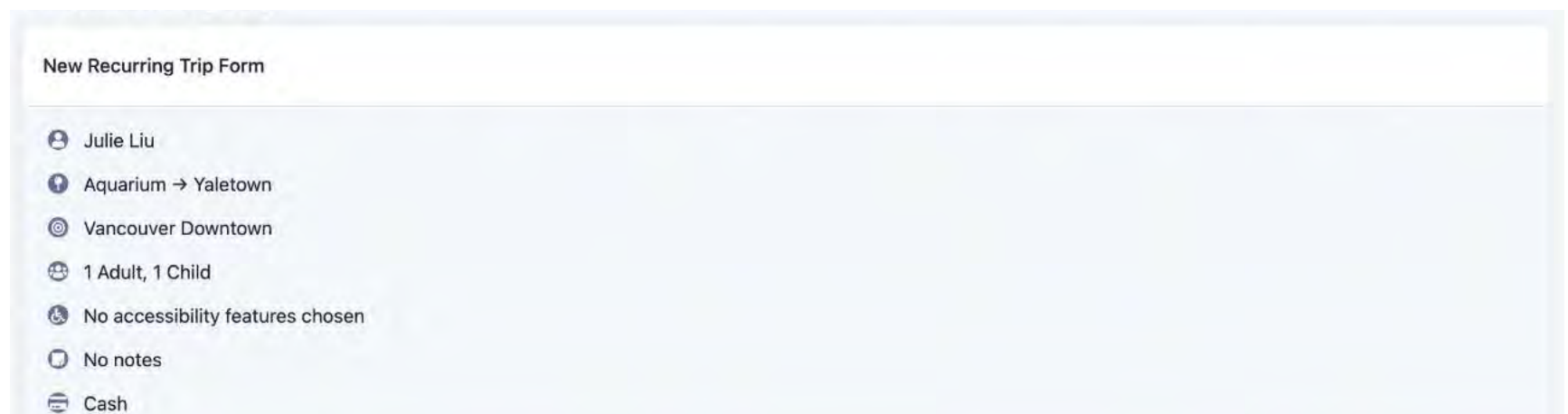
1 Locate the “BluePrint” Request

Find a trip to act as the "blueprint". You can either select an existing trip Request or create a new one.



2 Check Existing Details

Review all existing details that are populated to the New Recurring Trip Form.



3 Set Recurring Parameters

In the form, set the days of the week and the time period. Add exceptions, if necessary. Click **Create New Recurring Trip** to apply changes.

Repeat on

M

Tu

W

Th

F

Sa

Su

Select All

Begin on

2023-01-12

Repeat until

☒ Forever

Request Time

Leave at

11:57 AM

Departure time may occur between 11:57 AM and 12:57 PM.

Return Request Time

☒ No return request

Exceptions

DATE	OUTBOUND REQUEST	RETURN REQUEST
No exceptions have been added		

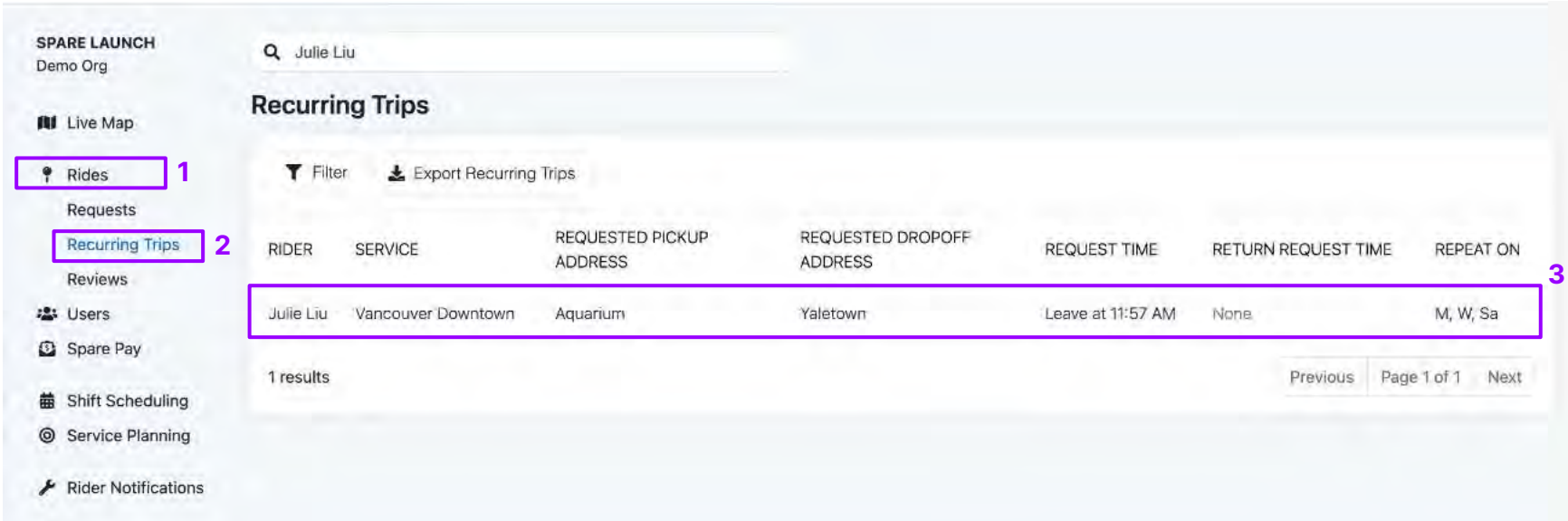
+ Add

 Adding an exception is necessary if the rider does not need an outbound or return request (or both) on a particular day.

5.2. How to Edit Recurring Trip Requests

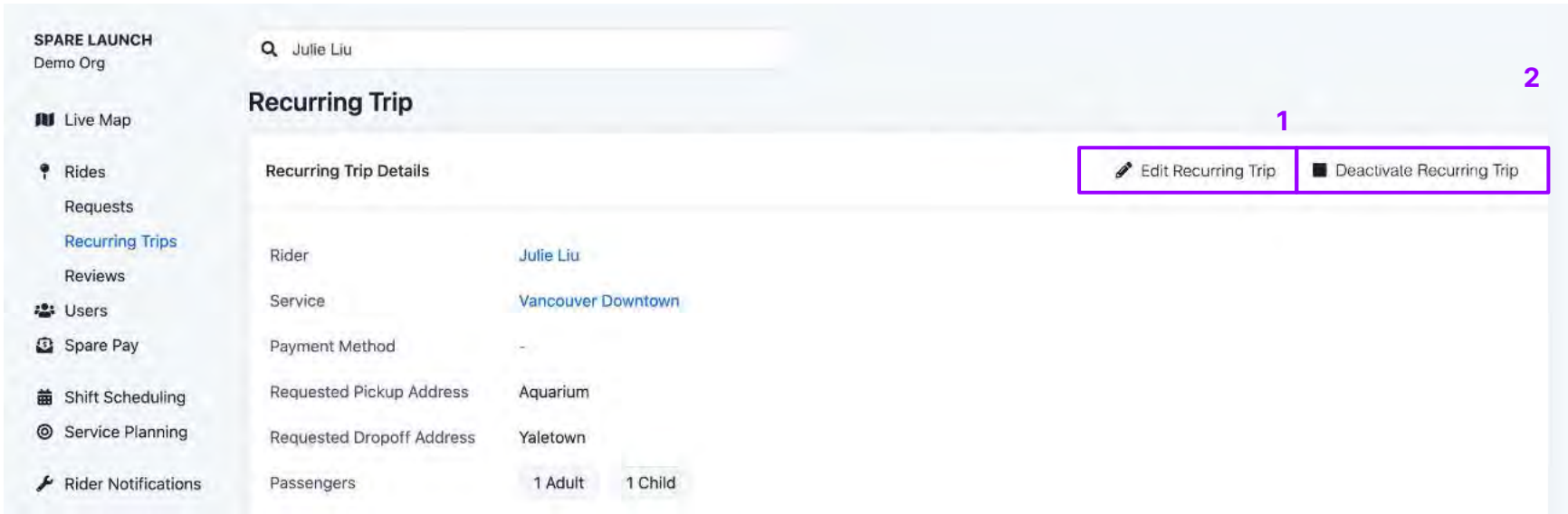
1 Open the Recurring Trip Information Page

If you need to change an existing recurring trip request, first, locate it in the Recurring Trips list. To do so, go to the **Rides tab**[1] and select **Recurring Trips**[2]. Click on the **request record**[3] you'd like to change.



2 Edit or Deactivate the Trip

From the Recurring Trip Information Page, **Edit**[1] or **Deactivate**[2] the trip. Follow the platform instructions to apply the changes.



Changes will apply to any requests created by the recurring trip from the moment of applying the new parameters. Any requests that have already been created will remain unchanged.

📞 Calling Sebastian Vettel

✓ Card number

✓ Expiry date

○ Postal code

● CVC



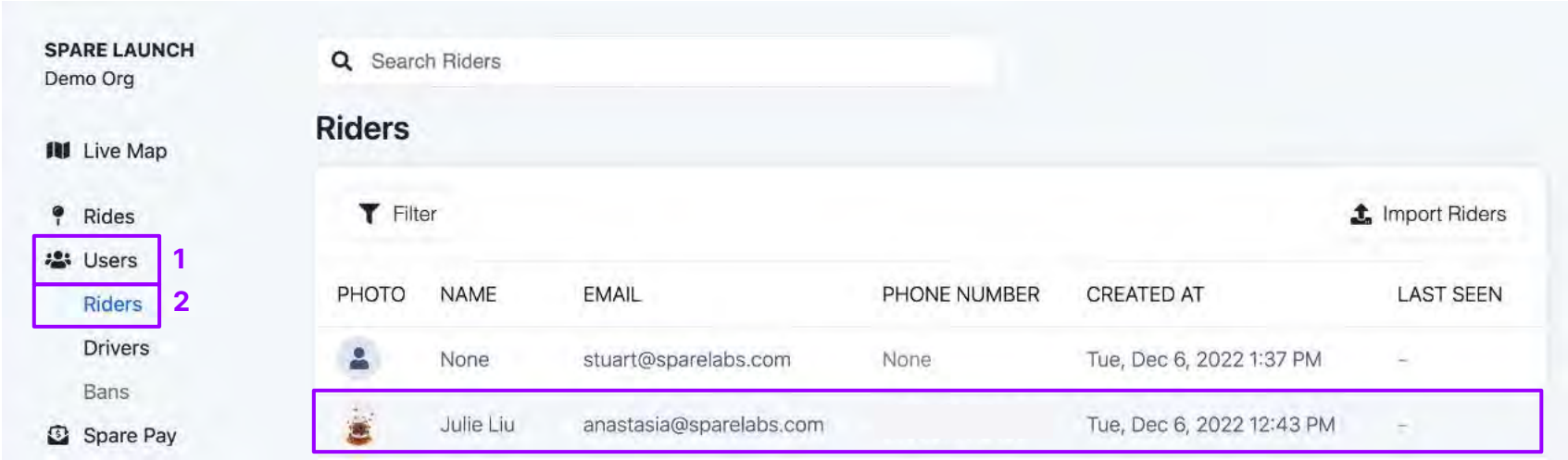
[6] Managing Riders

- View Rider Information
- Edit Rider Information
- Add Favourite Locations
- Add Riders to Groups

6.1. How to View Rider Information

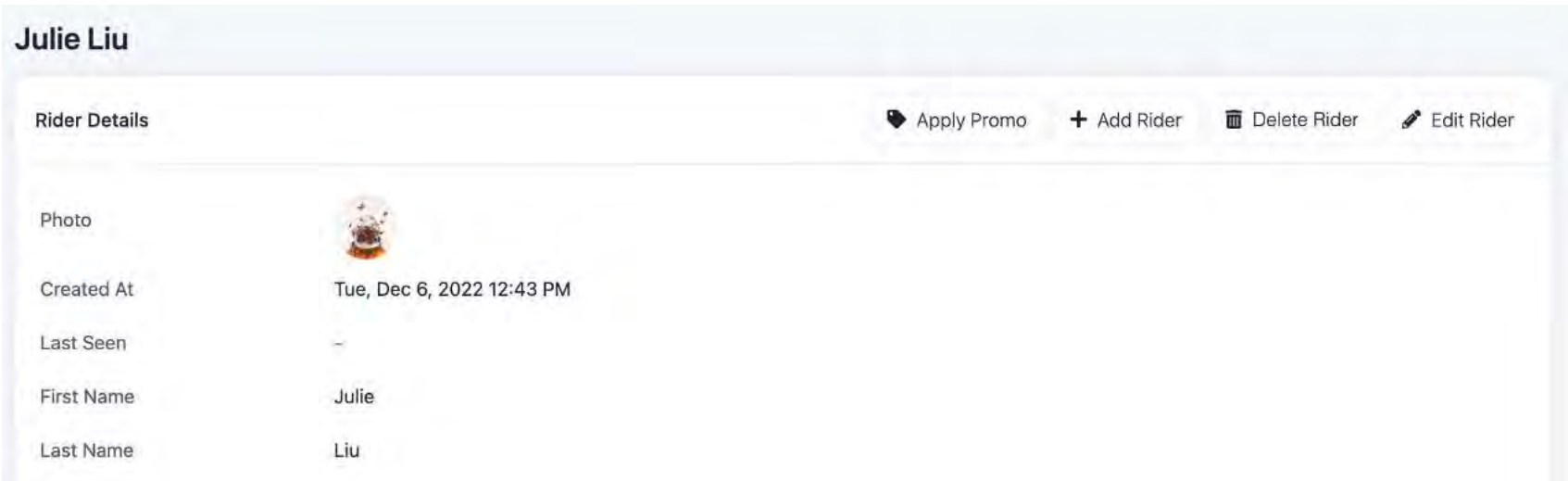
1 View Rider Information

You can see a list of all the Riders registered in the system by clicking **Users[1]** on the left side menu and then **Riders[2]**:



By clicking on a **Rider** you will be taken to the **Rider Details page** for that specific Rider. For each Rider you can see the follow details:

Contact Information	First name, Last name, Phone, Email (optional for Riders)
Default Request Preferences	You can set a default number (and type) of passengers or required accessibility features for the rider. The new defaults will automatically show up when you in the future create new trip requests for this specific rider.
Default Notes	You can also add default Notes for the Rider that will be shared with the Driver when picking up the Rider.
Favourite Locations	By adding favorite locations a booking agent can simply search for Home in the pickup location field and the saved Home address will show up.
Charges, Promos, Fare Passes, and Payment Methods	If your organization has these features enabled in the Spare Platform.
Requests	This is an overview of all the requests for the rider.



6.2. How to Edit Rider Information

2 Edit Rider Information

To edit rider information, click on the **Rider record** to open the Rider Information page and select **Edit Rider**. Click **Save** to apply the changes.

SPARE LAUNCH
Demo Org

Live Map

Rides

Users

Riders

Drivers

Bans

Spare Pay

Search Riders

Riders

Filter

Import Riders

PHOTO	NAME	EMAIL	PHONE NUMBER	CREATED AT	LAST SEEN
	None	stuart@sparelabs.com	None	Tue, Dec 6, 2022 1:37 PM	-
	Julie Liu	anastasia@sparelabs.com	+12369711618	Tue, Dec 6, 2022 12:43 PM	-

Julie Liu

Rider Details

Apply Promo

Add Rider

Delete Rider

Edit Rider

Photo

Created At

Tue, Dec 6, 2022 12:43 PM

Last Seen

-

First Name

Julie

Last Name

Liu

Save

3 Delete a Rider Record

To delete rider information, click on the **Rider record** to open the Rider Information page and select **Delete Rider**.

Julie Liu

Rider Details

Apply Promo

Add Rider

Delete Rider

Edit Rider

Photo

Created At

Tue, Dec 6, 2022 12:43 PM

Last Seen

-

First Name

Julie

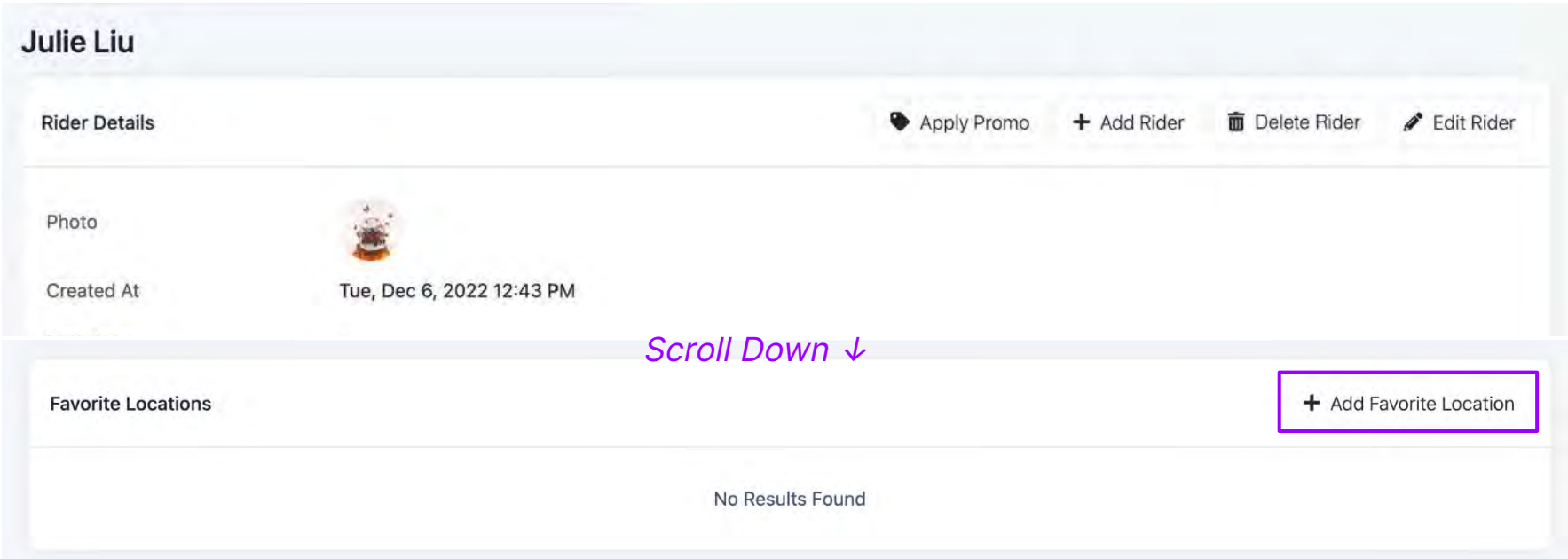
Last Name

Liu

6.3. How to Add Favourite Locations

1 Edit Rider Information

Favourite Locations are locations that a rider frequents often. You can add a Favourite Location(s) for riders by going to their **profile**, scrolling down to the 'Favourite Locations' section, and then selecting '**+ Add Favourite Location**'.



2 Fill in Location Details

In the Favourite Location card, fill in the details:
[1] Choose the **type of location** (work, leisure, sport, etc.);
[2] Type in **the address**;
[3] Create a **nickname** for the location;
Then click “**Create New Favourite Location**” to apply changes.



3 Apply when Booking the Next Trip

When you go to book requests for that rider in the future, you can either enter the address or point of interest or the name that represents the symbol you chose to denote their Favourite Location.

6.4. How to Add Riders to Groups



Groups are a function that can be used if your organization finds it necessary to restrict certain zones and services to specific sets of riders. For example, a paratransit service would be restricted only to those riders in the paratransit service group.

1

Edit Rider Information

To add a rider to a specific group, go to the **rider's profile**, scroll down to Group Memberships, and select **'+ Add Group Membership'**.

Julie Liu

Rider Details

Apply Promo

+ Add Rider

Delete Rider

Edit Rider

Photo

Created At

Tue, Dec 6, 2022 12:43 PM

Last Seen

-

First Name

Julie

Last Name

Liu

Scroll Down ↓

Memberships

Filter

+ Add Membership

No Results Found

2

Fill in Membership Details

In the Add Membership card, fill in the details:

- [1] Type in the name of the group;
 - [2] Check that the rider's name is correct;
 - [3] Set the expiry date or mark "Forever" if the membership is indefinite;
- Then click **"Create New Membership"** to apply changes.

Add Membership

New Membership Form

Group

para

Paratransit - Vancouver

Rider

☐ Forever

Valid until

2023-02-19

11:59 PM

Create New Membership

6.4. How to Add Riders to Groups

3 Edit or Archive the Membership

If you wish to edit or archive a rider’s membership, click on the membership record in their profile. You will then be navigated to the Membership Card.

By clicking **Edit [1]**, you will be able to change the expiry date of the membership;
By clicking **Archive[1]**, you will be able to disable the membership for the rider.

Memberships

Filter

+ Add Membership

GROUP	STATUS	CREATED AT	VALID UNTIL
Paratransit - Vancouver	Active	Thu, Jan 19, 2023 12:19 PM	-

Membership

12

Membership Details

Edit Membership

Archive Membership

Created At

Thu, Jan 19, 2023 12:19 PM

Status

Active

Group

Paratransit - Vancouver

Rider

Julie Liu

Valid until

-

4 View All Members of the Group

To view the list of current group members, go to the **Service Planning tab [1]** and select **Groups [2]**. Then click on the **group record line** to jump into its information page.

SPARE LAUNCH

Demo Org

Live Map

Rides

Users

Spare Pay

Shift Scheduling

Service Planning

Services

Groups

Announcements

Fleets

Time Rules

Routes

Rider Notifications

Search Riders

Paratransit - Vancouver

Group Details

Delete Group

Name

Paratransit - Vancouver

Created At

Wed, Dec 14, 2022 4:10 PM

Secret Code

0000

Description

None

Memberships

Filter

+ Add Membership

RIDER	STATUS	CREATED AT	VALID UNTIL
Julie Liu	Active	Thu, Jan 19, 2023 12:19 PM	-
Ellie Smith	Active	Wed, Dec 14, 2022 4:11 PM	-

Calling Sebastian Vettel

- ☒ Card number
- ☒ Expiry date
- ☐ Postal code
- ☐ CVC



[7] Managing Payments

- View Existing Fares
- Apply Promo Codes
- Set Up IVR

7.1. How to View Existing Fare Information



In most cases, payments are processed on the rider's side and don't require a Booking Agent's involvement. However, you can still view fare information, apply promo codes, and help the rider set up their IVR Payment, if applicable.

1 View Existing Fare Rules

To view existing fares per ride, go to the **Spare Pay tab**[1] and jump into **Fare Rules**[2]. From there,click on the **Fare Rule name**[3] to be transferred to the **Fare Information page**.

SPARE LAUNCH
Demo Org

Live Map

Rides

Users

Spare Pay

Charges

Payment Methods

Fare Rules

Tip Policies

Promos

Fare Passes

Search Riders

Fare Rules

Fare Rules

NAME

Paratransit

Basic

2 results

A • Per Rider

Adds together fares for each rider, based on the rider's type.

To control multiple rider types at once, rider types can be mapped to the Default value instead of a block.

Default	B • \$1.50 Fixed
Each Disabled	B • \$1.50 Fixed
Each Personal Care Attendant	Free
Each Other Rider	C • \$3.00 Fixed

1 View Existing Fare Passes

To view existing fare passes, go to the **Spare Pay tab**[1] and jump into **Fare Passes**[2]. From there,click on the **Fare Pass name**[3] to be transferred to the **Fare Pass Information page**.

SPARE LAUNCH
Demo Org

Live Map

Rides

Users

Spare Pay

Charges

Payment Methods

Fare Rules

Tip Policies

Promos

Fare Passes

Search Riders

Fare Passes

Filter

NAME	TYPE	STATUS	CURRENTLY ACTIVE
31 Day Adult Pass	Time Based	Draft	0

1 results

PreviousPage 1 of 1Next

Fare Pass Details

Edit Fare Pass

Status

Draft

Name

31 Day Adult Pass

Description

Unlimited rides during the period

Color

Type

Time Based

Number of Valid Days

31

Selling Price

\$20.00

Rider Type Restriction

Adult

Simple Terms Of Use

Non-refundable

Full Terms Of Use Link

https://www.google.com/

You will then be able to see the Fare Pass details, and any users with a currently active pass. →

7.2. How to Apply Promo Codes

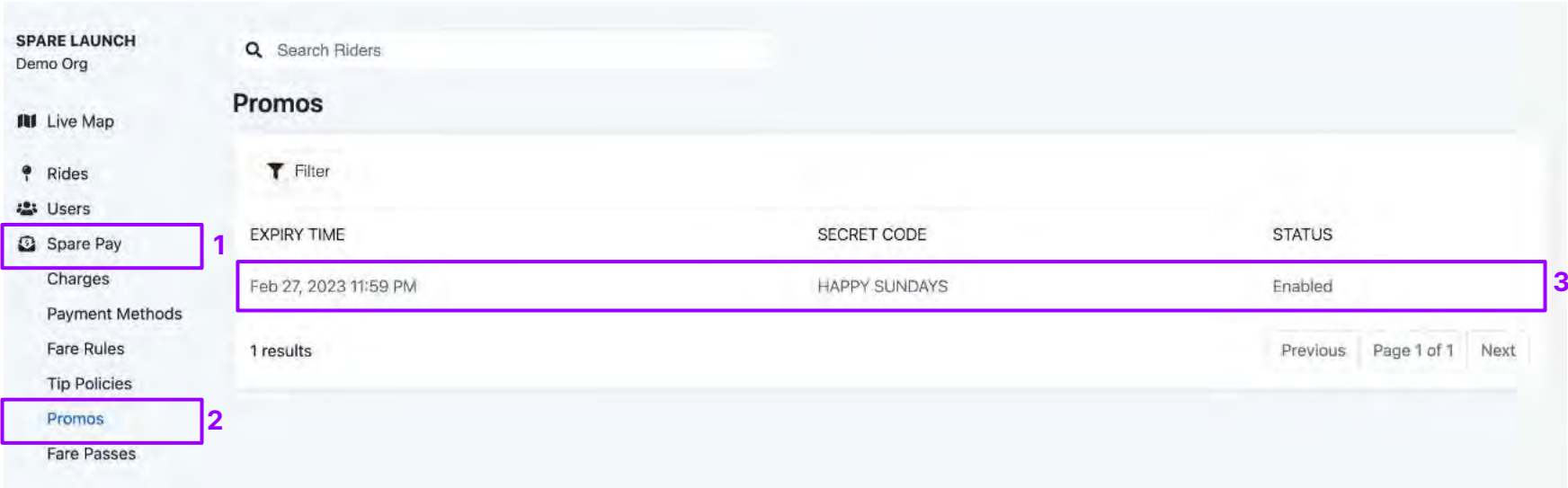


Promo Codes are a great way to market your service, build awareness, and push riders towards using the Rider App. Promo Codes are usually created by Service Administrators. However, promos can be viewed and applied by Booking Agents, too.

1

View Existing Promo Codes

To view existing promo codes, go to the **Spare Pay tab[1]** and jump into **Promos[2]**. From there,click on the **Promo Code name[3]** to be transferred to the **Promo Details page**.

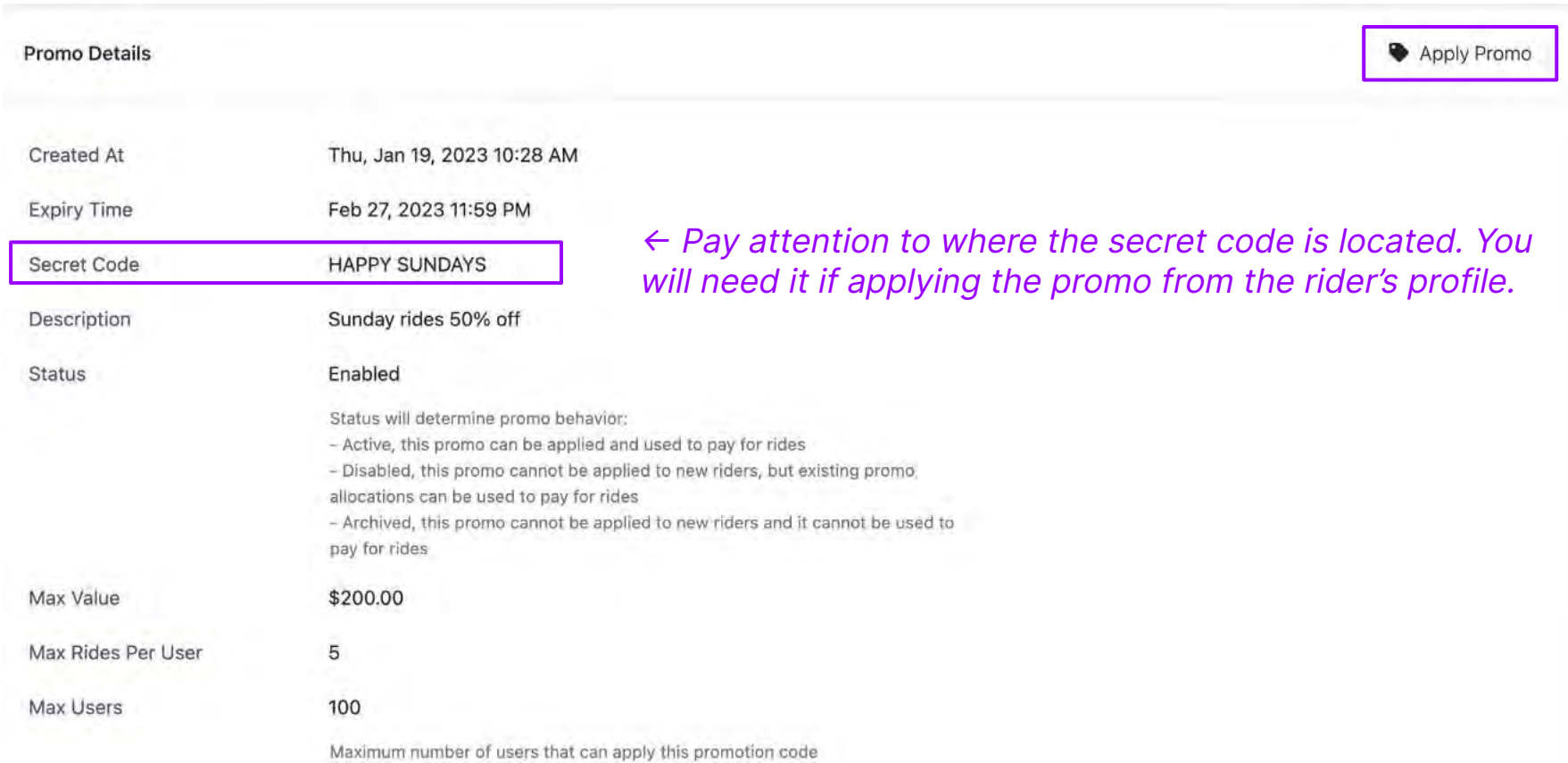


2

Apply Promo Codes - via Promos tab

If you click on a promo code, at the bottom of the page you will see if anyone has applied it to their profile and how much they've used/redeemed.

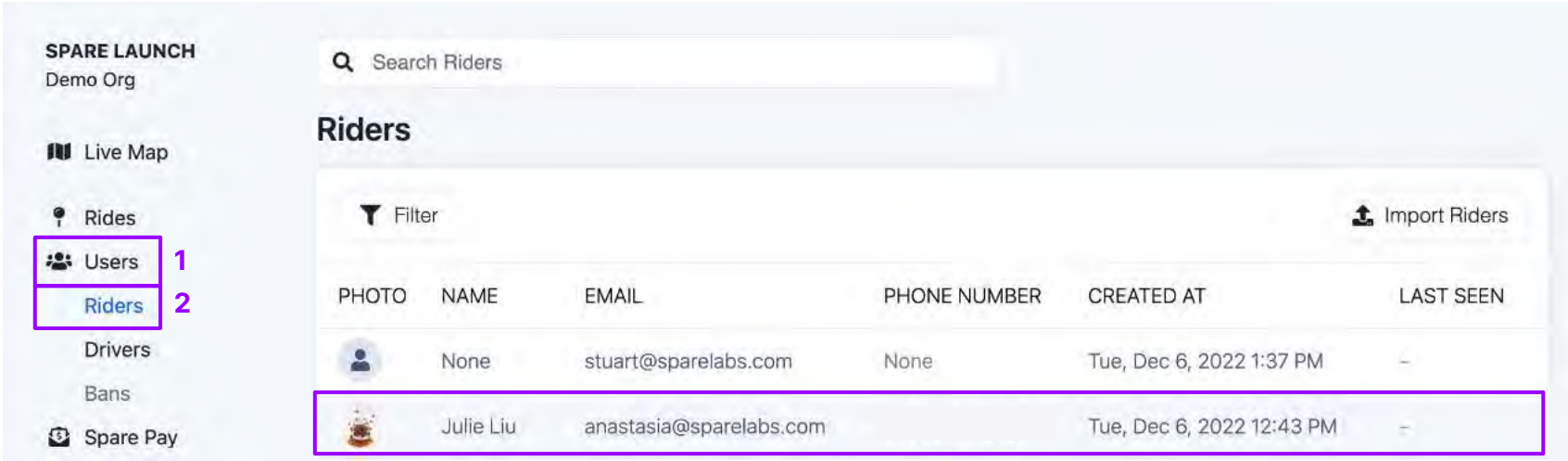
If you'd like to apply the promo code on behalf of the rider, click on **Apply Promo** and enter the **rider's name**. This will apply the promo code to **their account**.



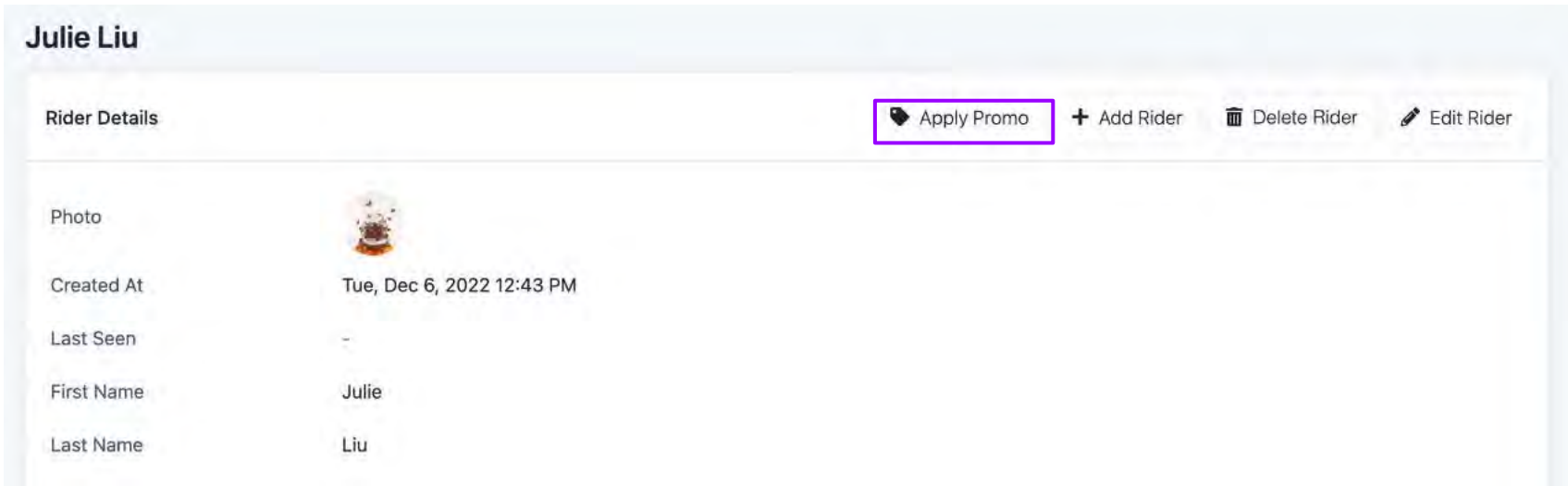
7.2. How to Apply Promo Codes

3 Apply Promo Codes - via Rider Profile

Alternatively to the step 2, you can apply a promo code right from the rider's profile. To do so, go to the **Users tab**[1] and select **Riders**[2]. **Locate the rider**[3] and open their profile.



Once in the rider profile, select **Apply Promo**. A promo card will appear.



Enter the **Secret Code** (you can find it on a Promo Details page) and click **Apply Promo** to enable the changes.

Apply Promo

Secret Code

User

Julie Liu

Apply Promo



Note that riders using Spare's rider app can apply the promo code from within the app by accessing the account menu in the top left of the home screen and then tapping **Promos** and entering the code.

7.3. How to Set Up IVR Pay

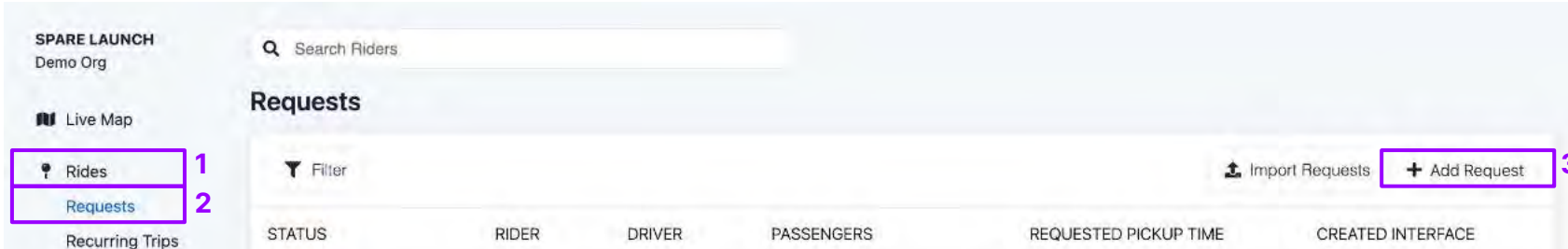


You are able to send an **IVR (Interactive Voice Response) phone call** to your riders for them to **register their credit card information** in their profile through the Spare platform and they can pay the fare by their **credit card** whenever booking.

Please **check first** if the IVR function is enabled.

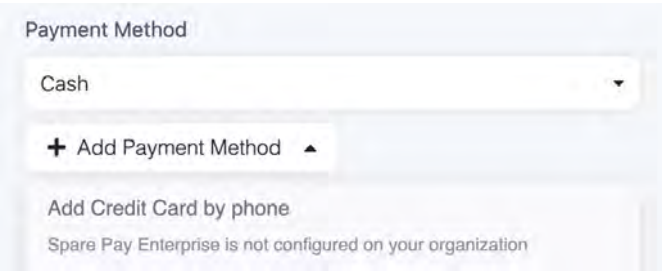
1 Create a Request

Go to the **Rides tab [1]** and select **Requests[2]**. Click **+Add Requests [3]**. Fill in the trip related information.



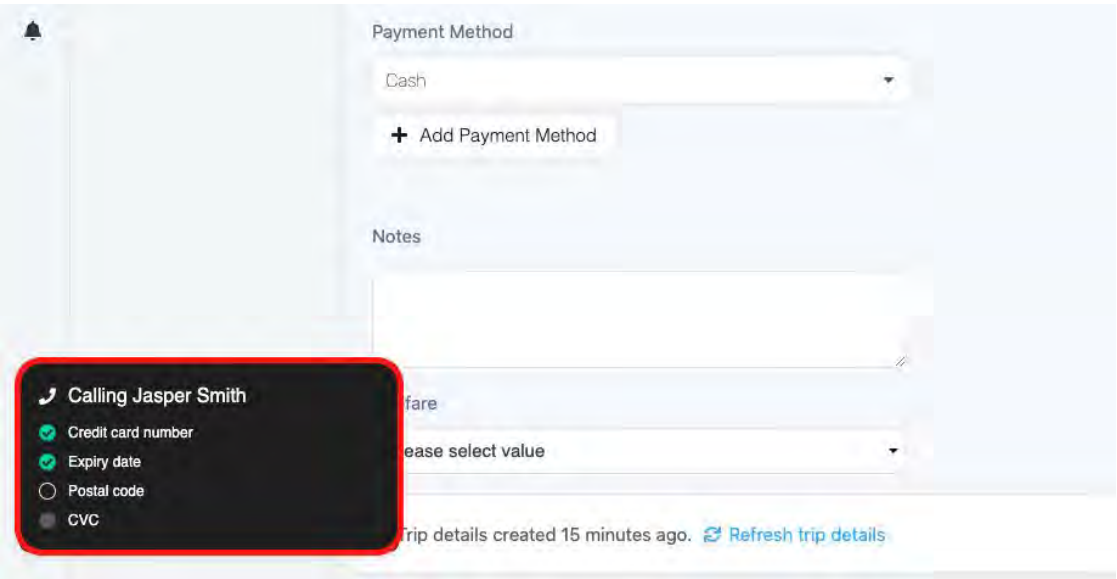
2 Add Payment Method

Click on **"Add Payment Method"** and **"Add Credit Card by phone"** to send an IVR phone call to the rider. You may want to give the rider heads-up that he/she is receiving a call from us and ask whether they want to hang up your call or put you on hold.



2 Rider to Input Credit Card Information

As soon as sending an IVR call to the rider, the rider receives a phone call and can input credit card information through the phone call. It will ask **credit card number, expiry date, postal code (only for US riders) and CVC**.



You can see the process of the input on the platform and once done, the rider's credit card information will appear as a payment method. Whenever you book a trip for this rider, the credit card will be there as a payment method.

📞 Calling Sebastian Vettel

✓ Card number

✓ Expiry date

○ Postal code

● CVC



[8] Viewing Service, Fleet, and Duty Details

- View Existing Service Settings
- View Scheduled Duties
- View Fleets and Associated Services

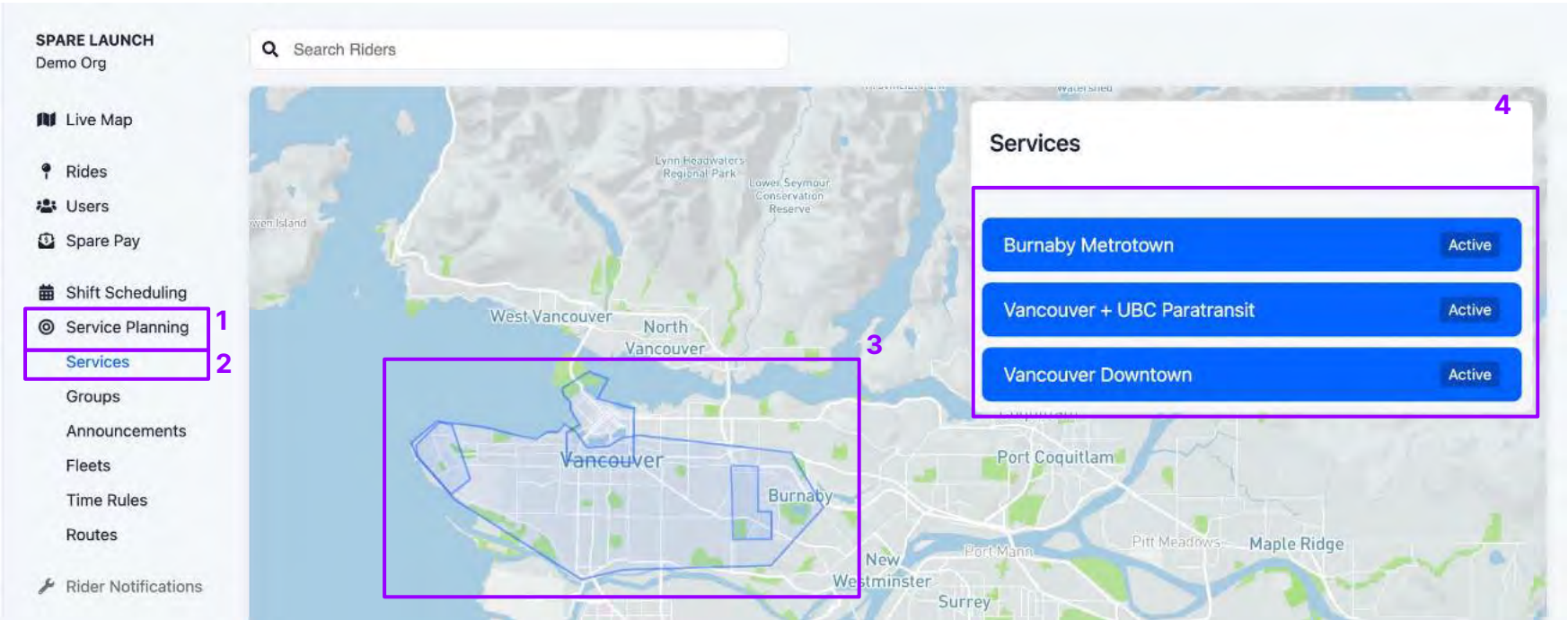
8.1. How to View Existing Service Settings



Being able to view Service Settings is useful when you want to learn about the existing service parameters, such as: driver breaks frequency and duration, service flexibilities (how much time a rider can spend on a vehicle, etc.)

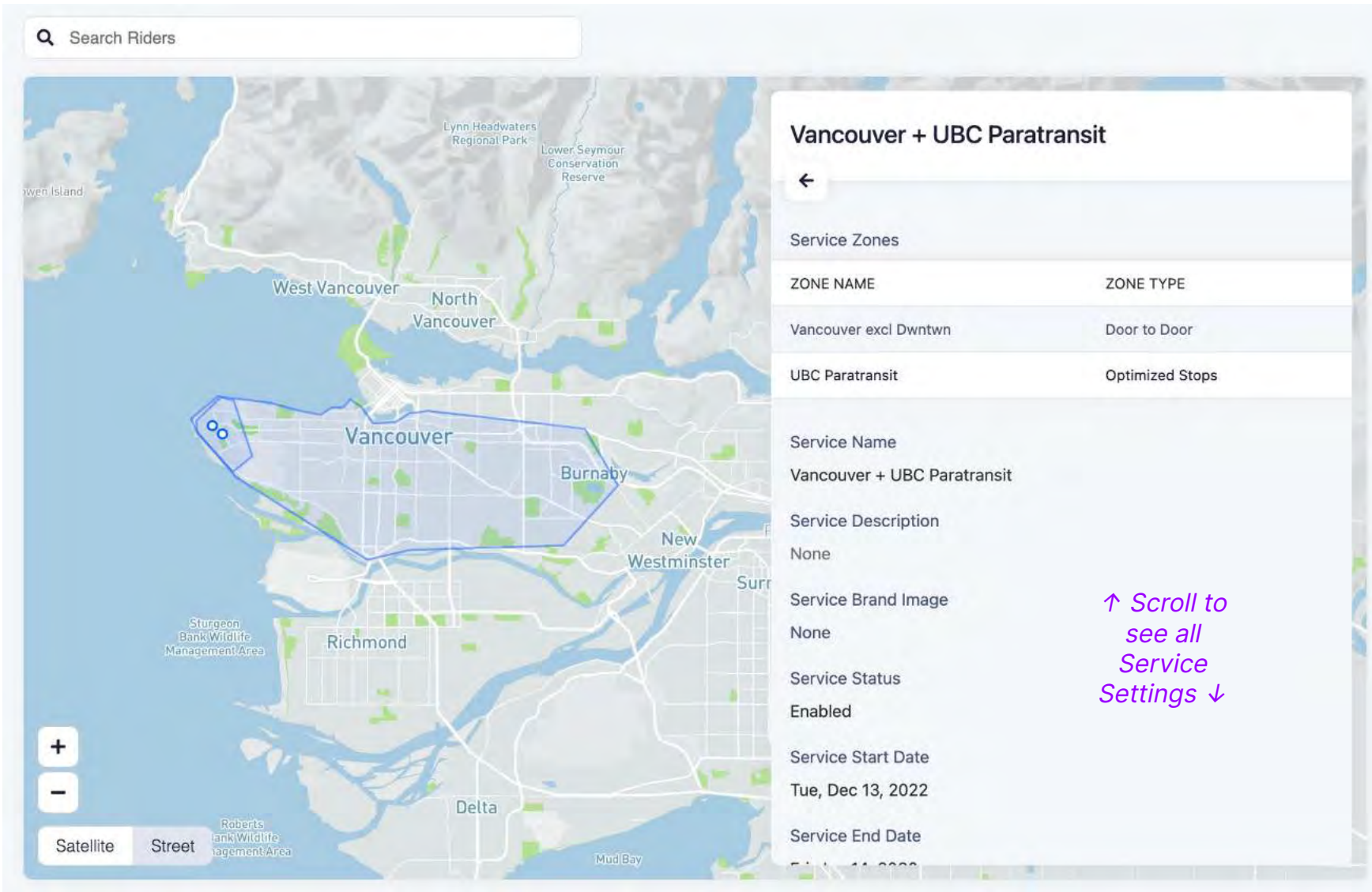
1 Identify Service Area and Status

From the **Service Planning** tab [1], go to **Services** [2]. You will see all **service inclusion zones** displayed on the map[3], as well as each service **name and its status**[4].



2 View Current Service Settings

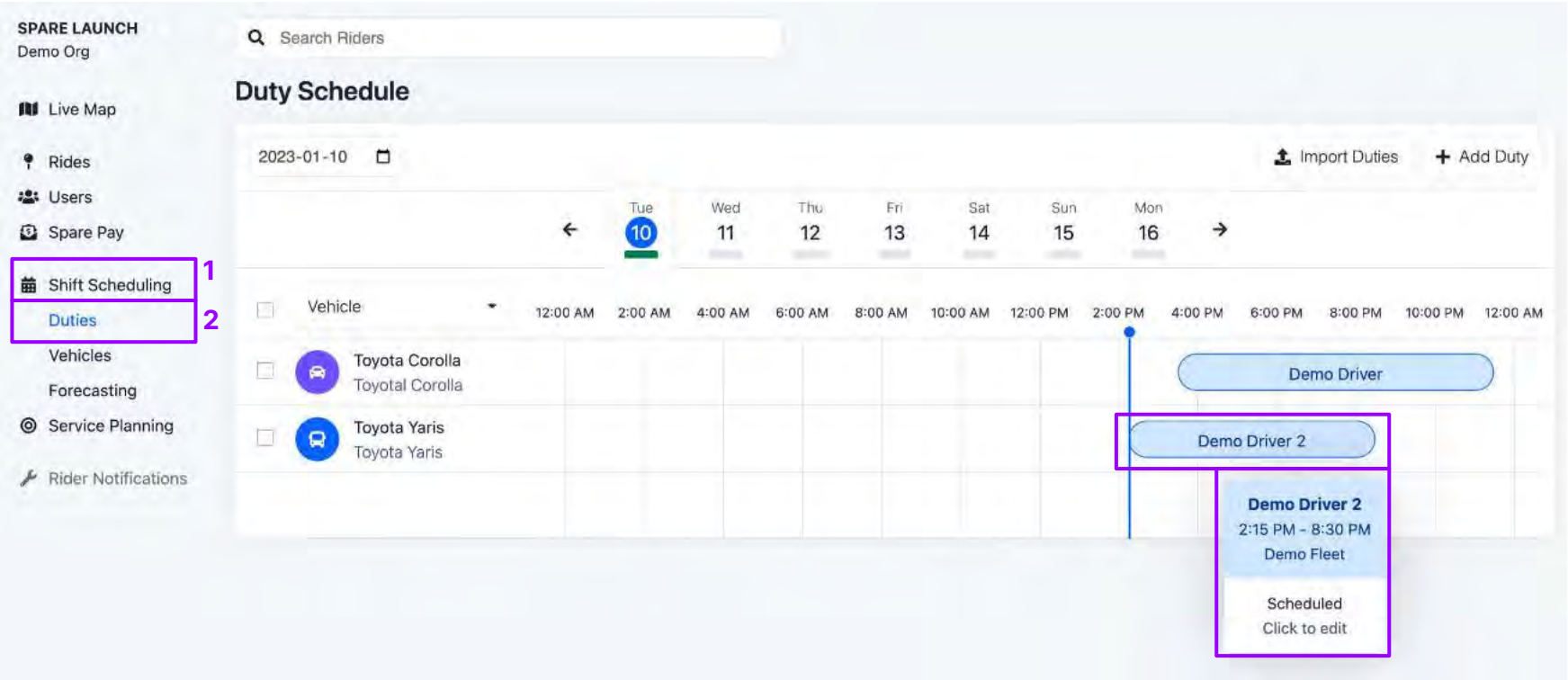
Click on the service name to get redirected to its information card.



8.2. How to View Duties and Fleets

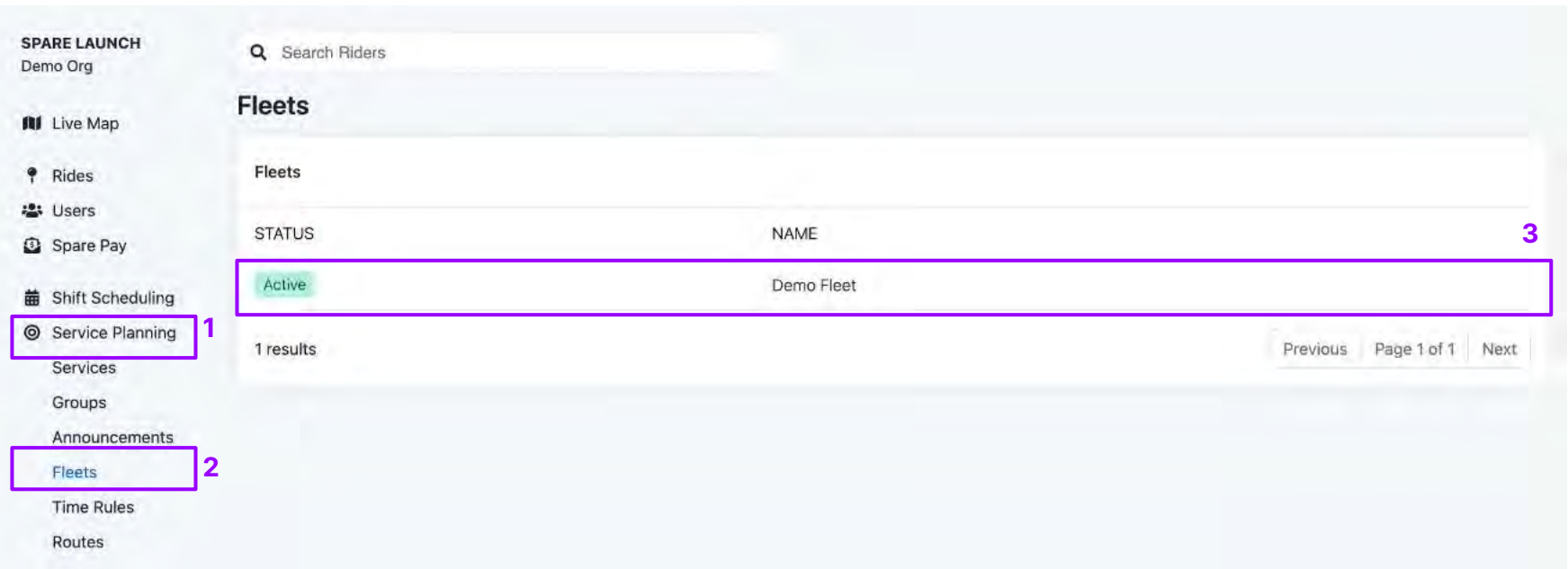
1 View Scheduled Duties

You can view scheduled duties by going to the **Shift Scheduling tab[1]**, and clicking **Duties[2]**. You will see a **calendar** with all currently scheduled (and cancelled) duties in it. **Hover over** the duty to view its information.



2 View Fleets and Associated Services

To view the drivers assigned to a specific fleet, go to the **Service Planning tab[1]** and jump into **Fleets [2]**. Then click on the **fleet record line[3]** to get redirected to the Fleet information page.



You will then be able to see the following information:

- [1] Driver Threshold:** how much time a driver should wait for the rider at the pickup location and after the scheduled pickup time before marking them as No-Show);
- [2] Break Policy:** how often automatic driver breaks occur and how long the breaks last;
- [3] Linked Services:** list of all services associated with the fleet;

📞 Calling Sebastian Vettel

✓ Card number

✓ Expiry date

○ Postal code

● CVC



[9] Admin Notifications

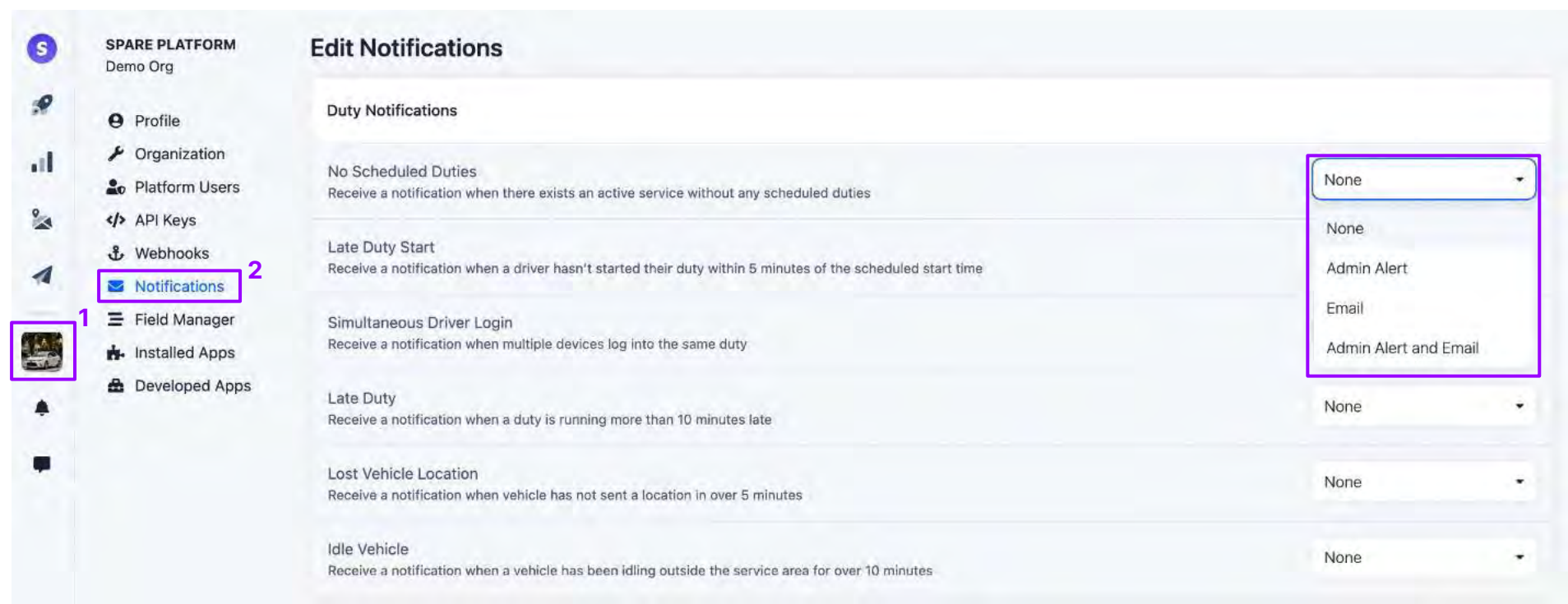
→ Set up Platform (Admin)
Notifications

9.1. How to Set Up Platform Notifications



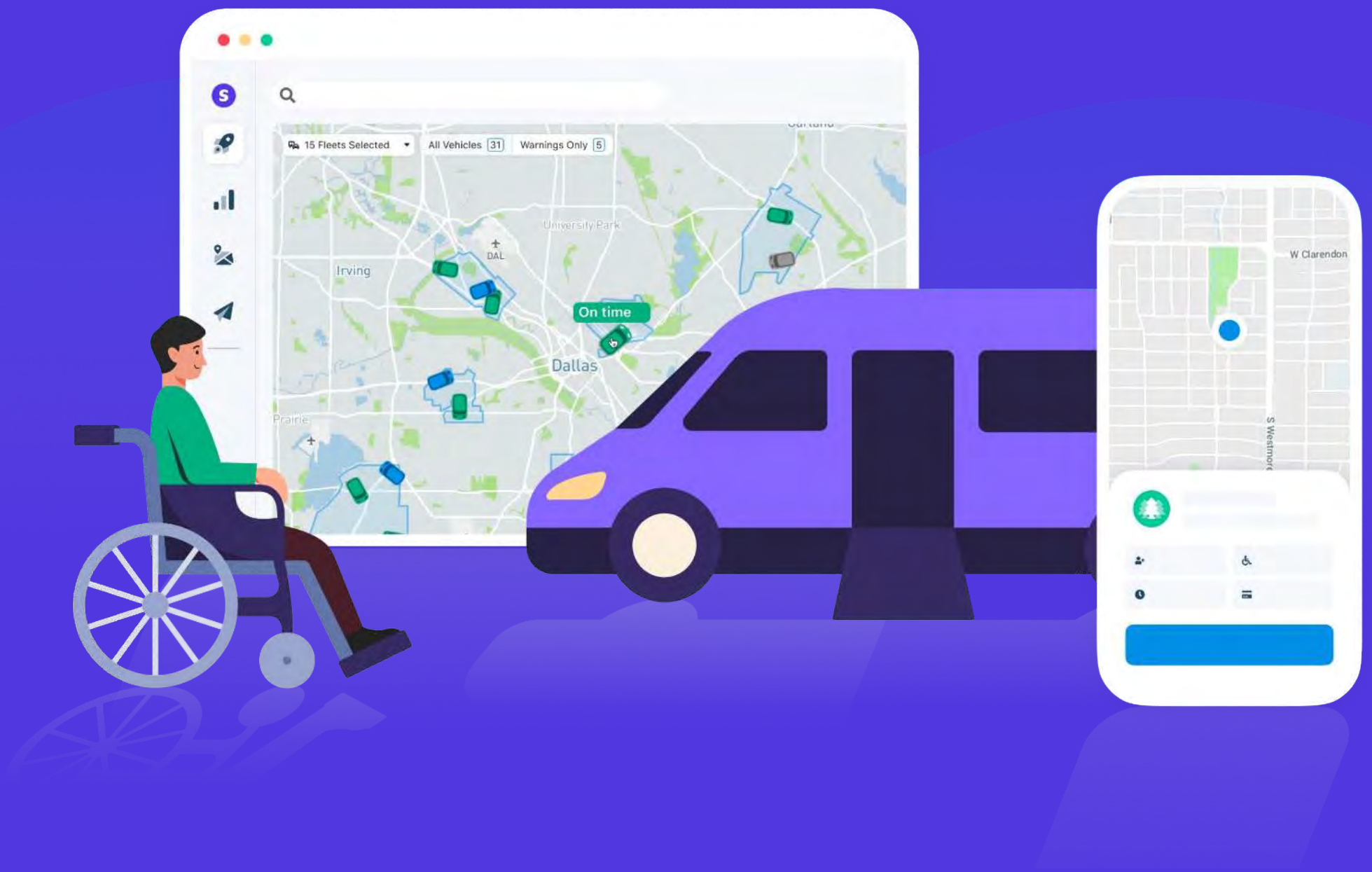
Administrator notifications provide information to platform users about events within the platform. Unlike the notifications in the Launch menu, which notify riders, the notifications in the Administrator menu notify your specific user profile either through in platform alerts, via email, or both.

To access the administrator notifications, select your **Account icon**[1] on the left-hand side of the screen, navigate to the **Settings** section, and then select **Notifications**[2].



There are currently 4 groups of notifications (see the table below. You can set up your preferred notification mode for each of them.

Notification Group	Notification Modes
Duty Notifications: No Scheduled Duties, Late Duty Start, Simultaneous Driver Login, Late Duty, Lost Vehicle Location, Idle Vehicle	☐ Admin Alert (in-platform) ☐ Email ☐ Admin Alert & Email ☐ None
Request Notifications: System at Capacity, No Drivers Available, No Show Cancellation, Recurring Trip Failure, Stranded Requests	☐ Admin Alert (in-platform) ☐ Email ☐ Admin Alert & Email ☐ None
Review Notifications: Negative Review Posted, Positive Review Posted with Comment	☐ Admin Alert (in-platform) ☐ Email ☐ Admin Alert & Email ☐ None
Engage Notifications (if applicable): Case Assignment	☐ Admin Alert (in-platform) ☐ Email ☐ Admin Alert & Email ☐ None



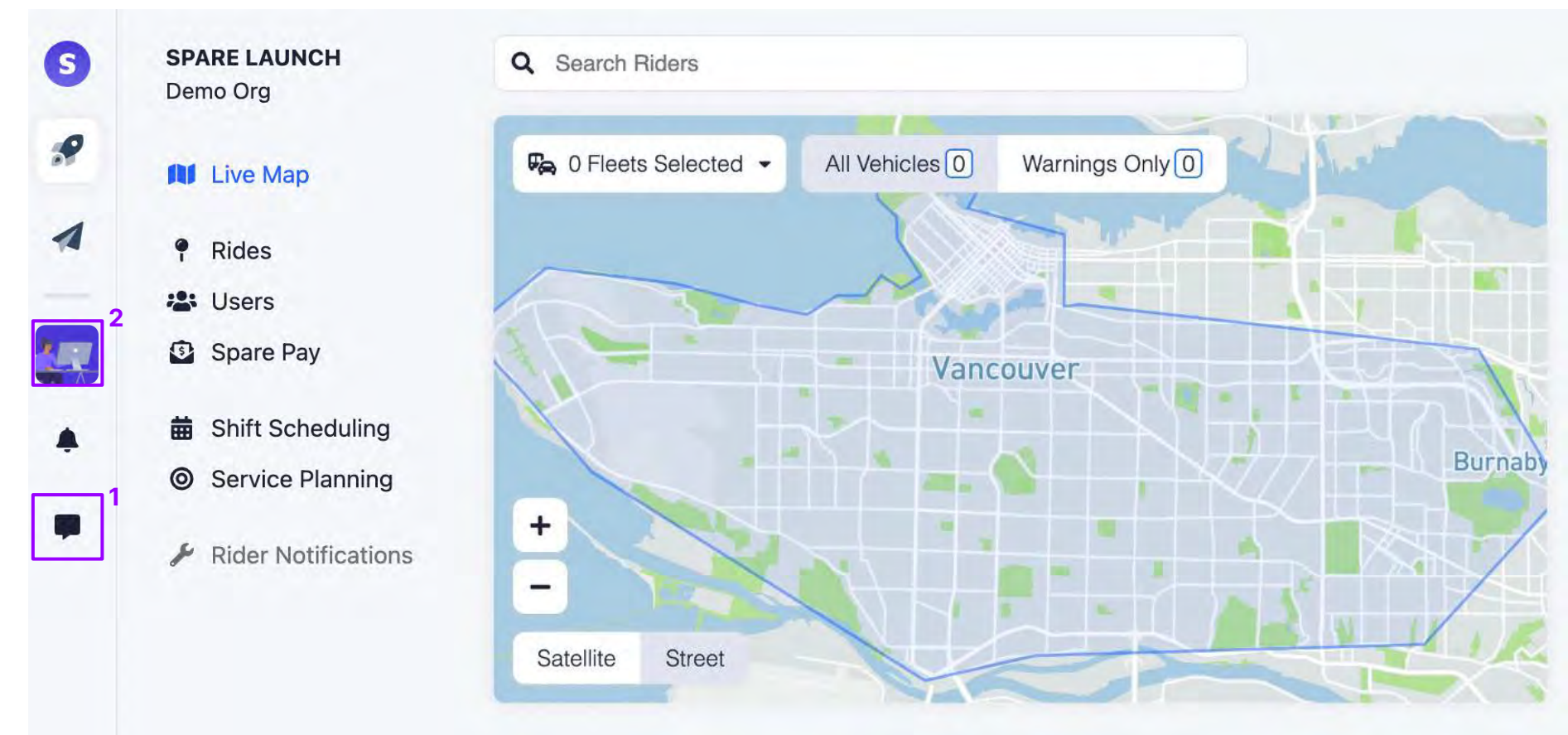
[10] Help & Troubleshooting

- Spare Help Centre
- Spare Tech Support

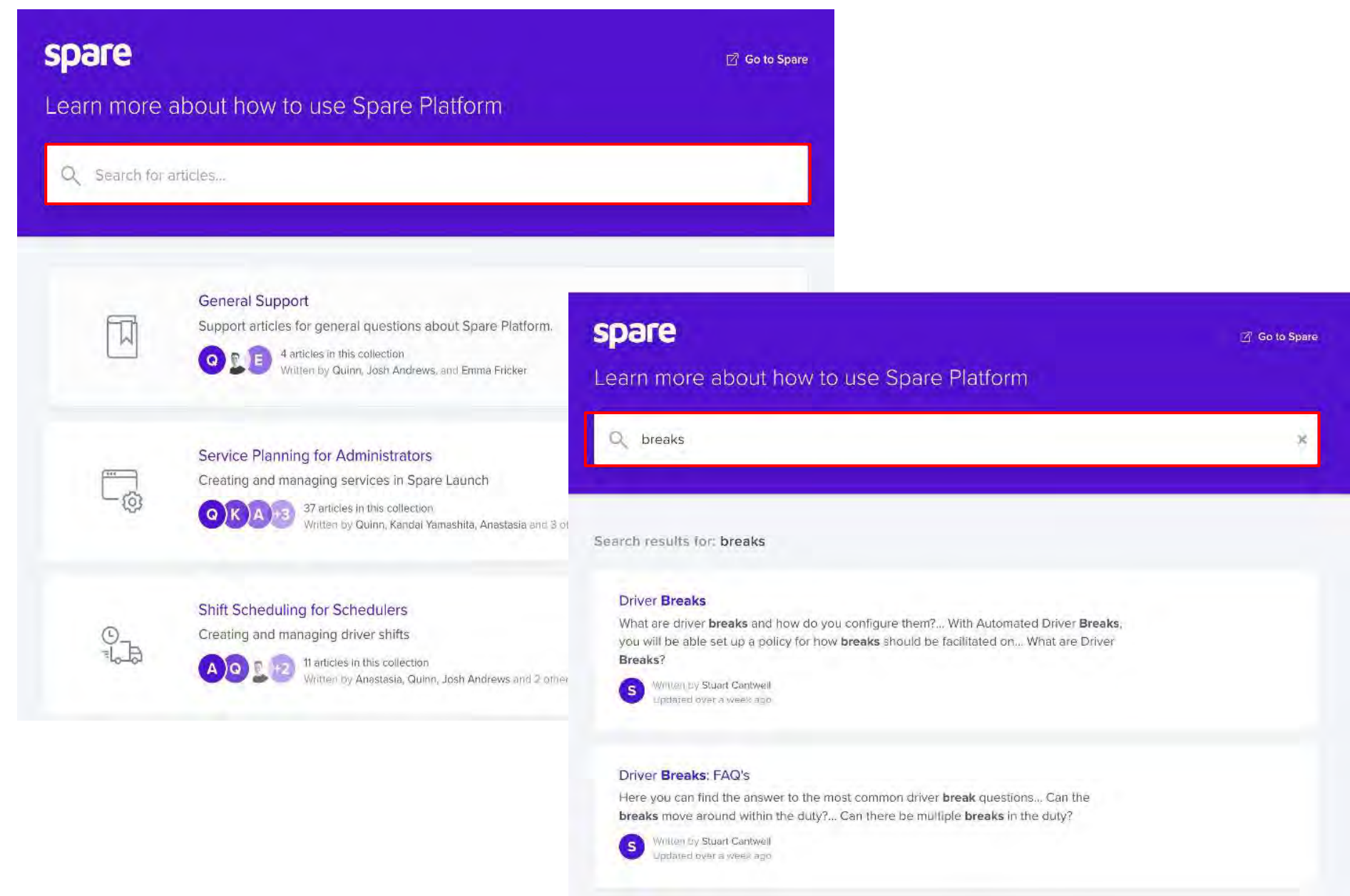
10.1. How to Reach out for Support

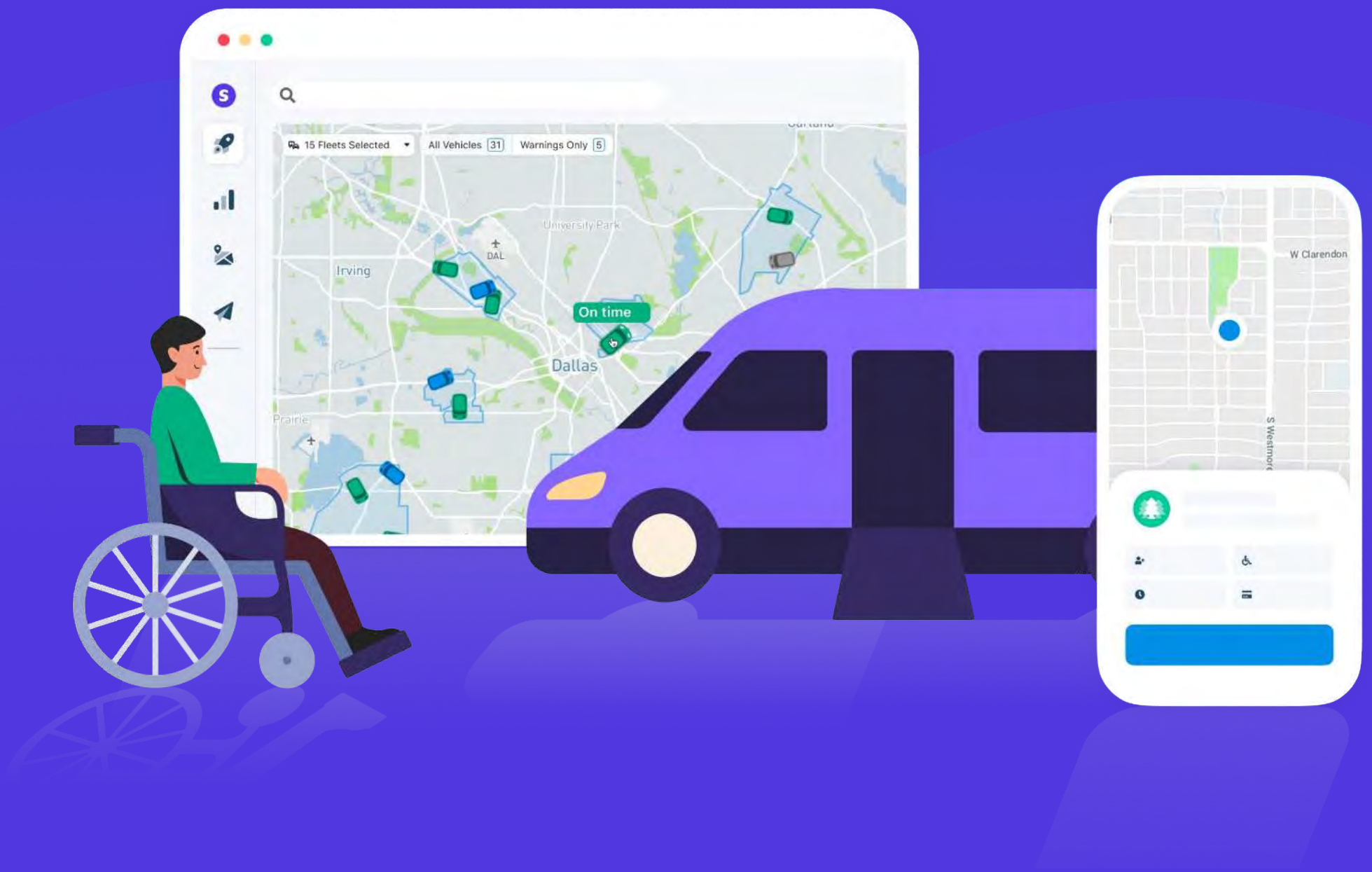
There are several ways you can **access help resources**:

- By clicking on the **message icon**[9]: it will redirect you to **Spare's Tech Support** chat.
- By going to your **Spare Account** [2] and selecting **Help**: it will redirect you to [Spare's Help Center](#).



If you are browsing Spare's Help Centre, feel free to type in the keywords in the search tab and click Enter to get all related results.



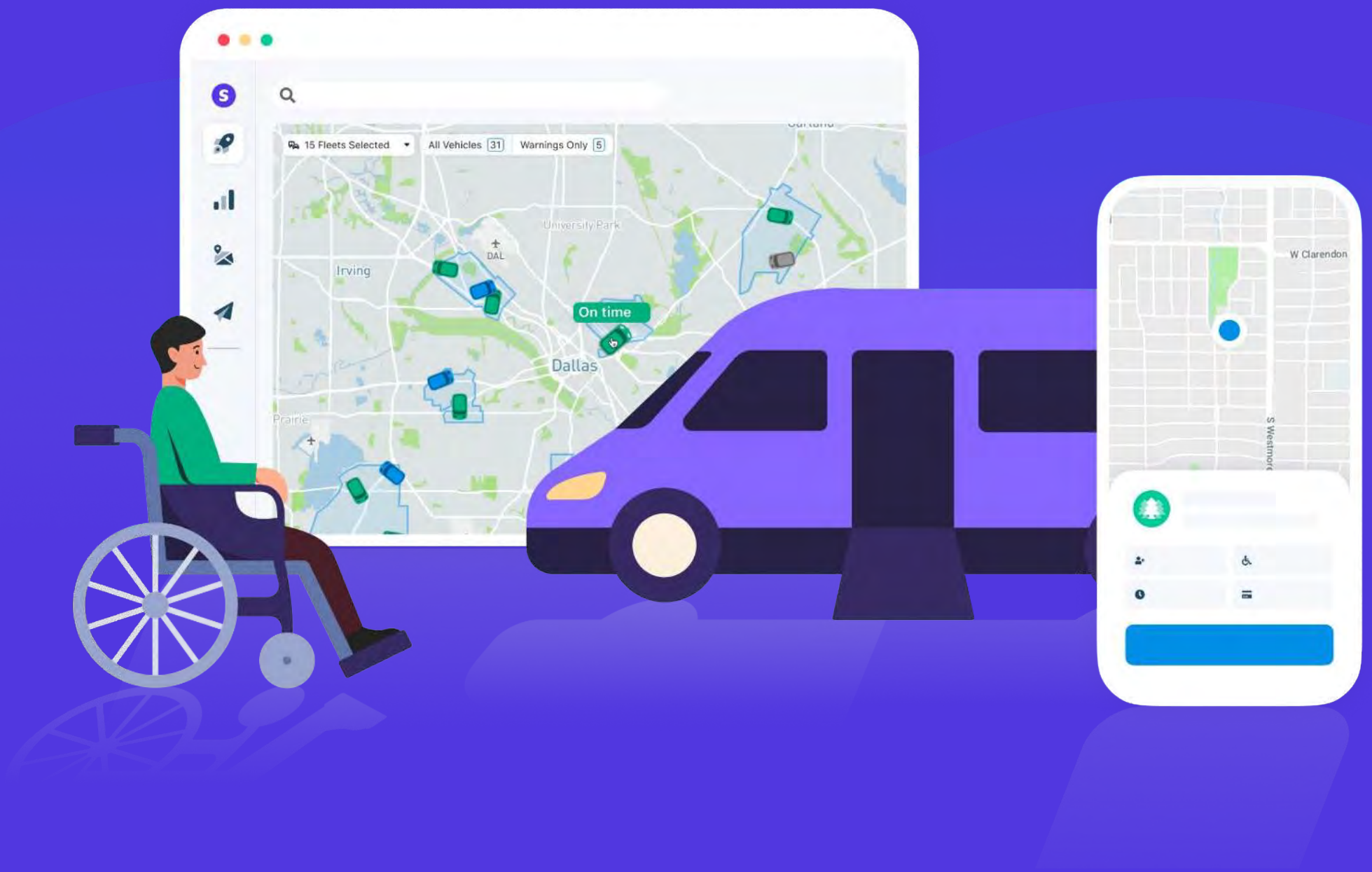


Spare Platform Dispatcher Guide

Visit sparelabs.com
815 W Hastings St Suite 810,
Vancouver, BC V6C 1B4
© Spare 2022

Table of Contents

1. Getting started	3
1.1. Accessing Your Account.....	4
1.2. Main Dashboard Overview.....	5
2. Service Monitoring with Spare Live Map	6
2.1. Access Spare Live Map.....	7
2.2. Investigate Vehicle/Duty Activity	8
3. Exploring Service Settings	9
3.1. View Existing Service Setting.....	10
4. Managing Drivers	12
4.1. Create a New Driver Record.....	13
4.2. Edit an Existing Driver Record.....	14
4.3. Investigate Drivers' Activity.....	15
5. Managing Vehicles	16
5.1. Add a New Vehicle.....	17
5.2. Edit an Existing Vehicle.....	18
6. Managing Driver Fleets	19
6.1. View Fleet Information.....	20
6.2. Re-Assign Drivers to Fleets.....	22
7. Managing Shifts/Duties.....	23
7.1. Schedule a New Duty.....	24
7.2. Edit an Existing Duty.....	26
8. Managing Riders.....	28
8.1. View Rider Information.....	29
8.2. Edit Rider Information.....	30
9. Managing Trip Requests.....	31
9.1. Create Requests.....	32
9.2. Request Status and Troubleshooting.....	36
9.3. Edit Requests.....	37
9.4. Create Recurring Trip Requests.....	38
9.5. Edit Recurring Trip Requests.....	39
10. Administrator Notifications.....	40
10.1. Set up Platform Notifications.....	41
11. Help and Troubleshooting.....	42
11.1. How to Reach out for Support.....	43



[1] Getting Started

- Spare Platform Login Information;
- Main Dashboards Overview;

1.1. Accessing your Account

1 Setup your account

You should have received an invitation email from sparelabs.com.
An invitation link will redirect you to the Spare Platform and the account setup.

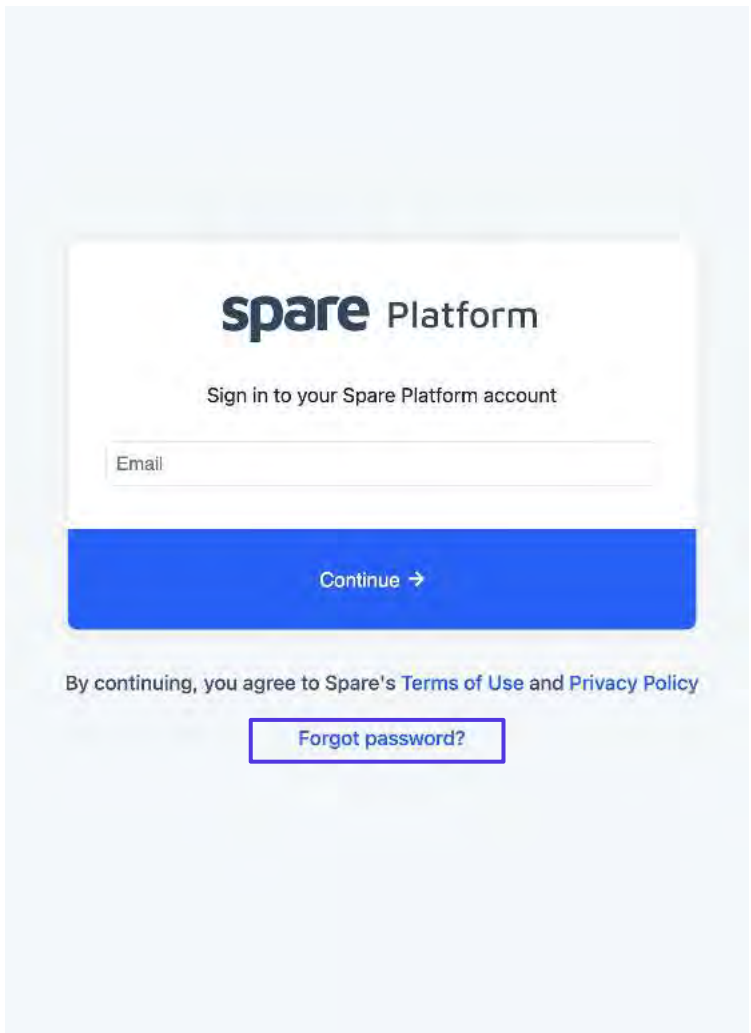
You can log into your account via your email and a password you will set the first time.



 Please contact your **administrator** if you don't have login credentials or did not receive a registration email.

2 Log in to your account

You can log into your account via your email and a password you will set at the first time.



Reset your password

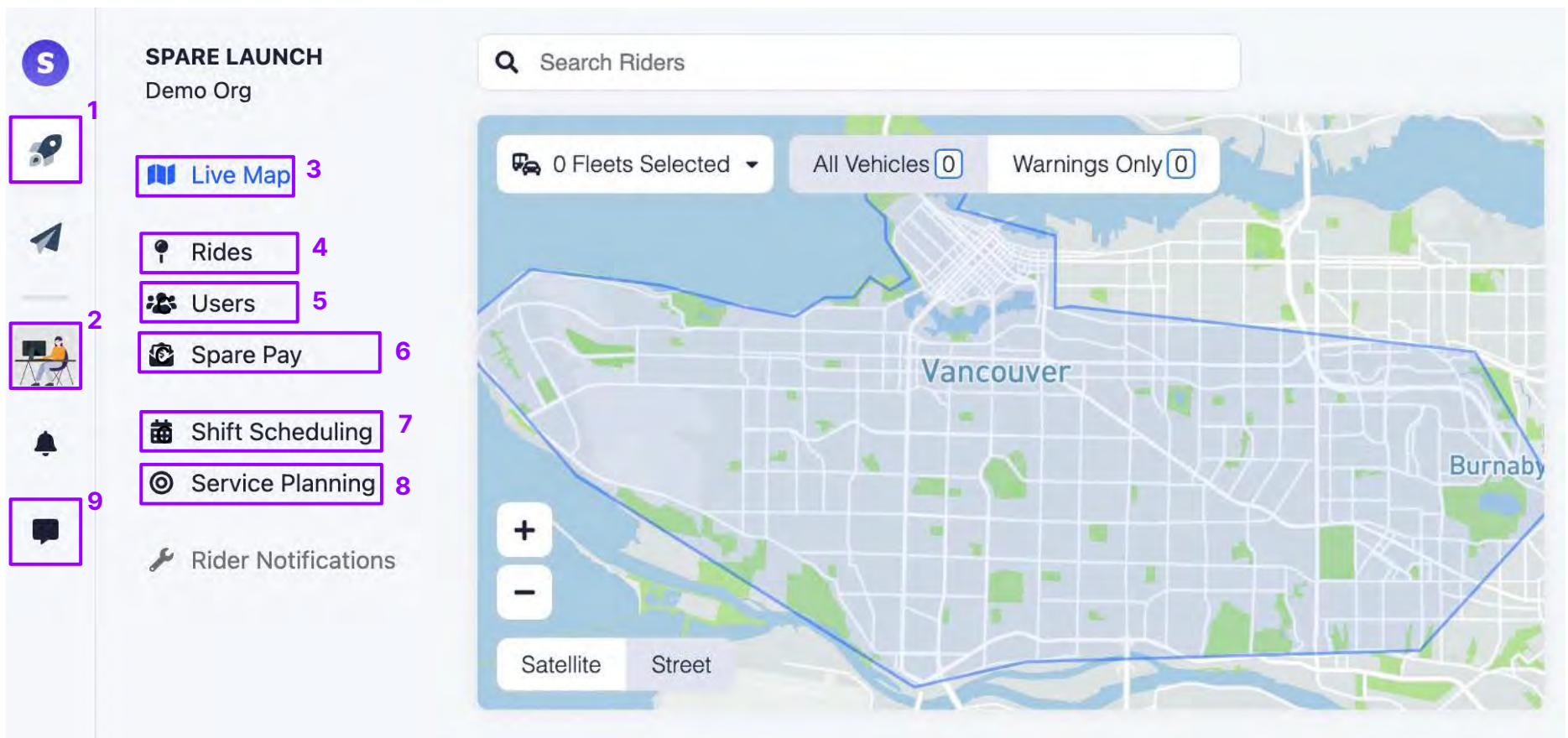
If you don't remember your password, you can tap on the **"Forgot Password?"** button. You will receive an email with a password reset link.

If you request a password reset too many times, the system might no longer send you a password reset email. Please get in touch with your administrator instead.

 Remember to follow your manager's instructions and **log out** after your duty if instructed to do so.

1.2. Main Dashboards Overview

Here is what you will see when you first log in to Spare Platform. Below are the key areas you'll learn to navigate as a Dispatcher/Scheduler:



[1] Spare Launch is Spare's core service where all the rides happen. This is your main working space.

[2] Your Spare Account is where you can access the account settings and help resources.

[3] Spare Live Map is a living representation of the service on-demand operations.

[4] Rides section is where you create, edit, cancel, or investigate trip requests.

[5] Users section contains information about riders and drivers.

[6] Spare Pay allows you to view and edit current service fares and learn about current fare policies and passes (if applicable).

[7] Shift Scheduling is where you can create/edit/cancel driver duties, or view vehicle information.

[8] Service Planning is where you can view current service settings and create routes.

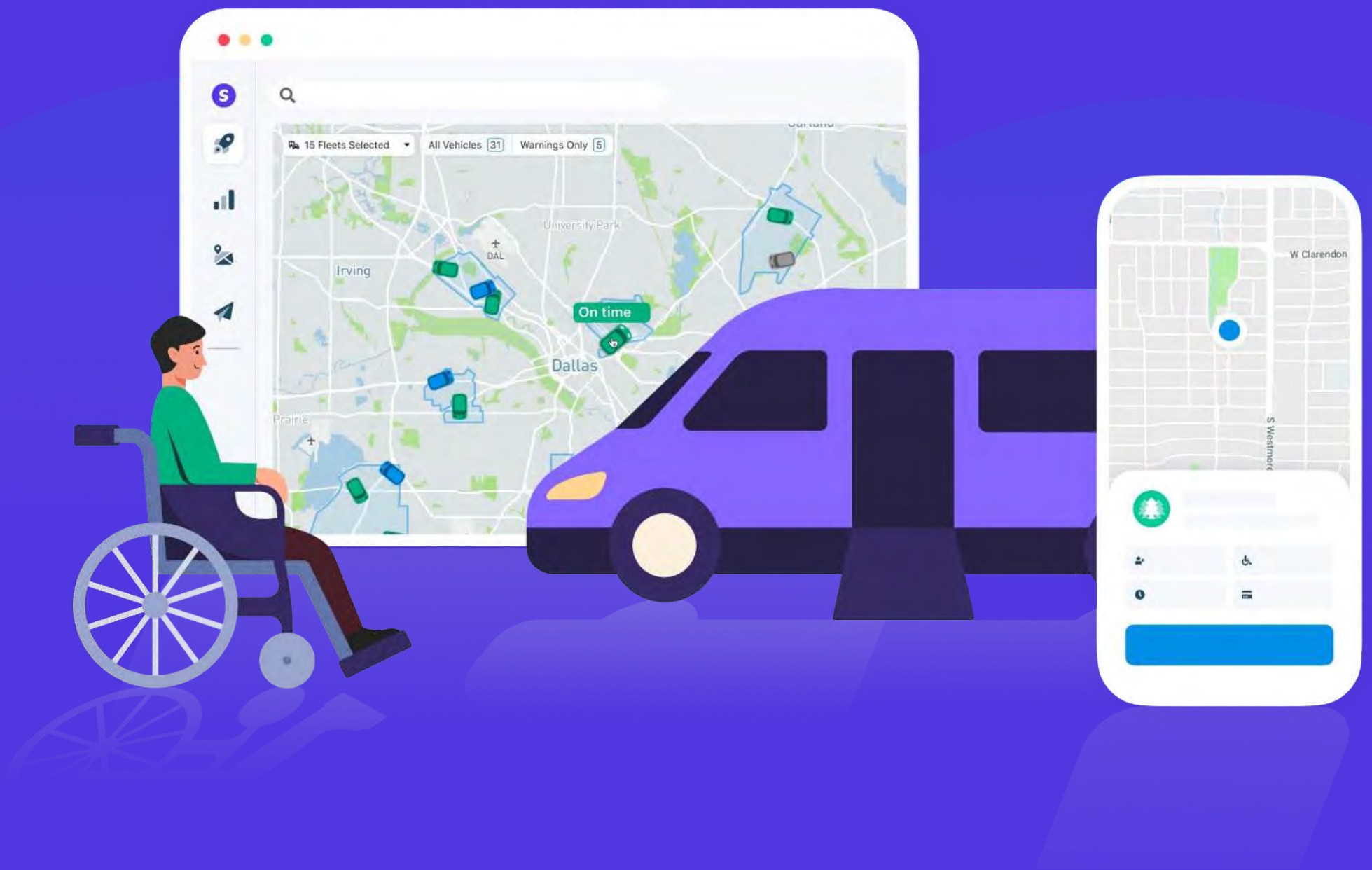
There are several ways you can **access help resources**:



By clicking on the **message icon[9]**: it will redirect you to Spare's Tech Support chat.



By going to your **Spare Account [2]** and selecting **Help**: it will redirect you to Spare's Help Center.



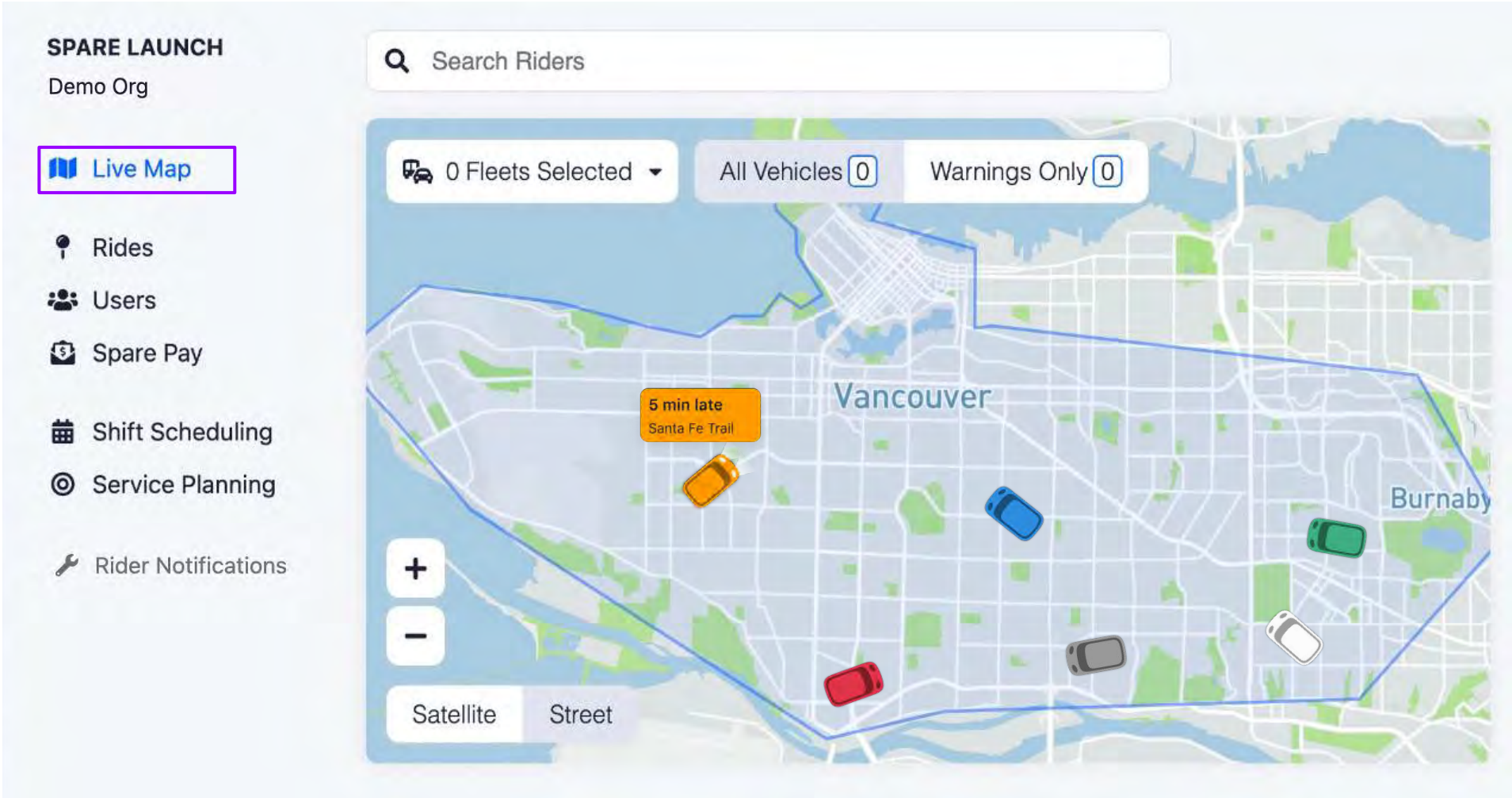
[2] Service Monitoring with Spare Live Map

- Access Spare Live Map;
- Investigate Vehicle/Duty Activity;

2.1. How to Use the Live Map



The Live Map is a great place to view your entire on-demand operations or dive deeper into specific services. The dark blue area represents your service zone boundary, and the vehicles represent the drivers you currently have on duty.



1 Vehicle Color & Information

Vehicle Color	Vehicle Status
Green	The vehicle/duty/driver is currently operating normally and is on time.
Yellow	The vehicle/duty/driver is between 2-10 minutes late to their next pickup/dropoff, or a vehicle has not updated its location (no connection) for 1-2 minutes.
Red	The vehicle/duty/driver is over 10 minutes late to their next pickup or dropoff or has not updated its location (no connection) in over 2 minutes and so is now unmatchable.
Blue	The vehicle is "Idle" and currently has no trips booked to its manifest.
Grey	The vehicle has been paused and is unmatchable.
White	The vehicle is on a driver break.

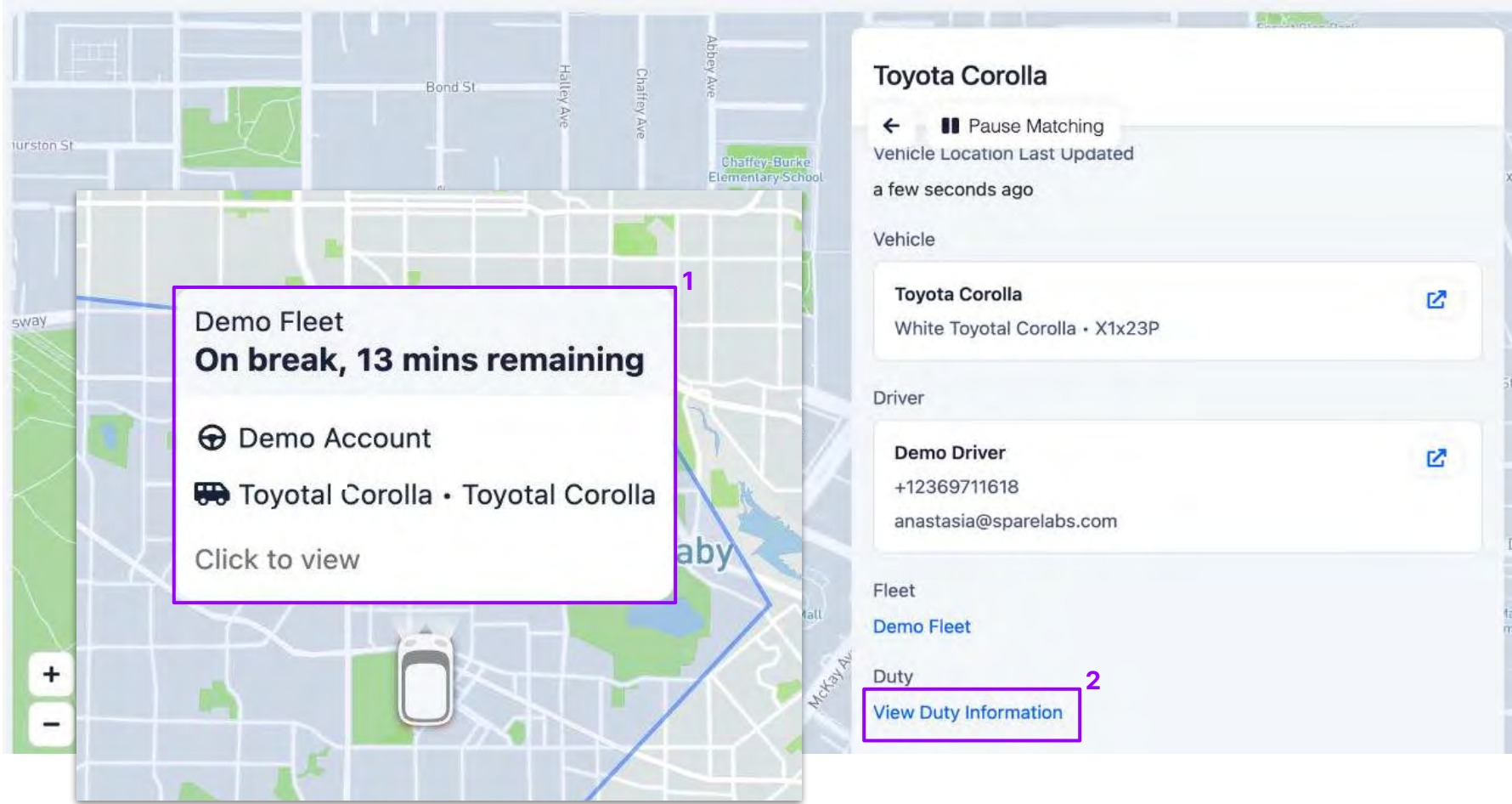


Hovering over or clicking on a vehicle will give you more information on the duty's status and trip manifest.

2.2. How to View Vehicle's Past & Future Activity

1 Vehicle/Duty Details Screen

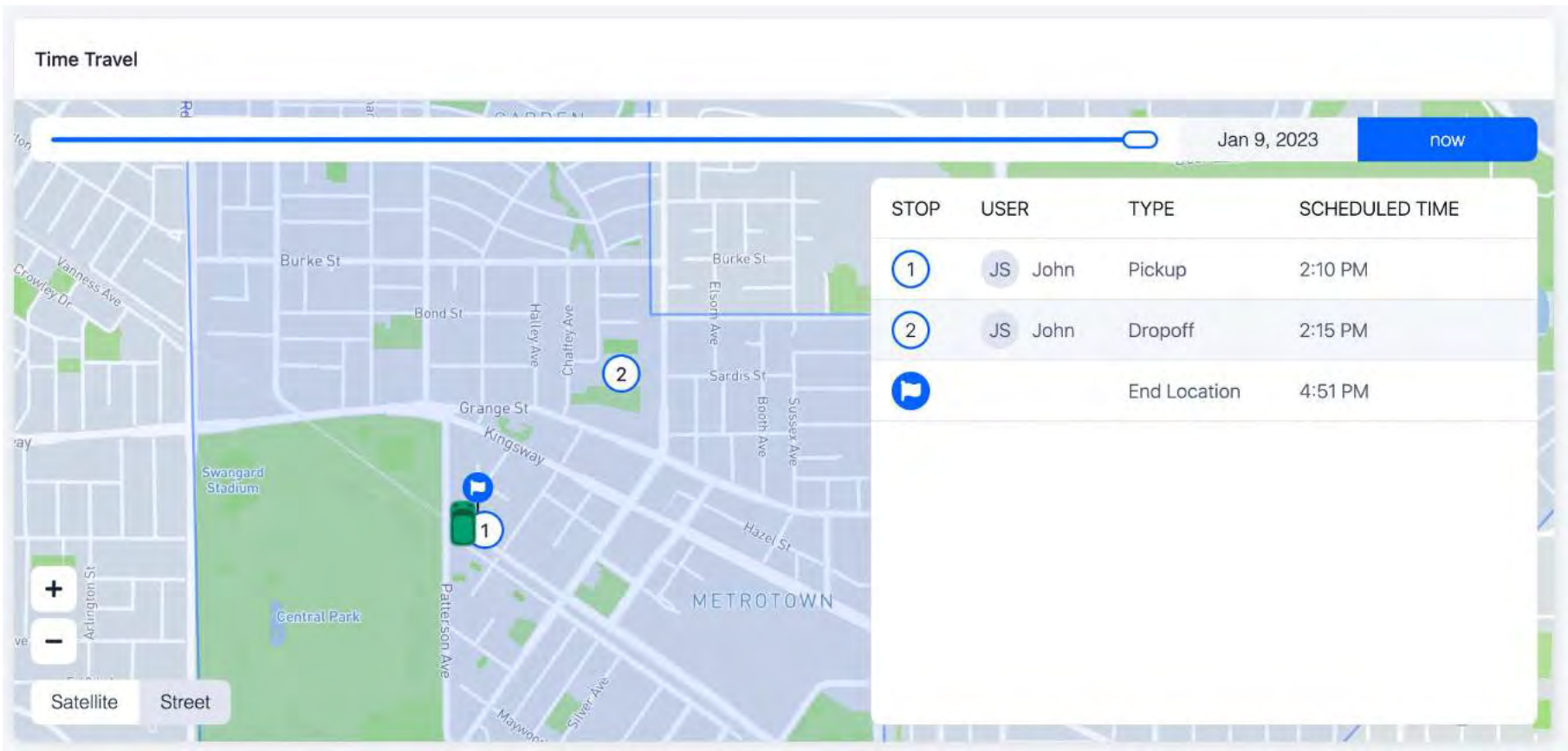
On the **Vehicle Information Card [1]** of the Live Map you will see such information as current status (e.g., “On break”); vehicle name; driver name; duty name. Click on the card to view the details.

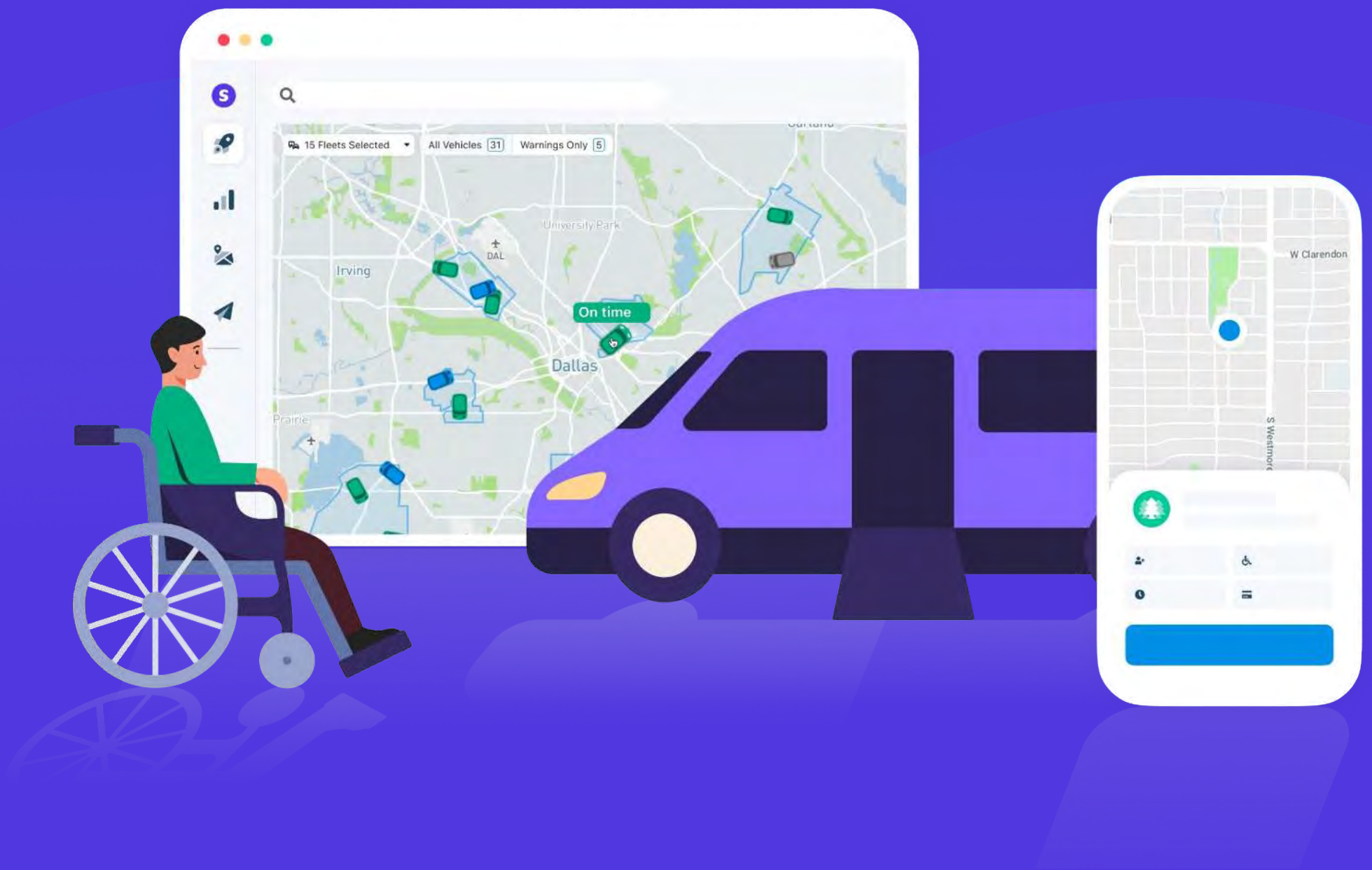


The **Vehicle Details screen** can be extremely useful in diagnosing operational problems and answering questions, such as the current capacity of a vehicle or its current route.

All of the vehicle’s currently **assigned pickups and dropoffs** are shown in a list which is then represented on the map by the chronological stops and the vehicle path. You can also click on **View Duty Information[2]** to see details about that request.

By using the **Time Travel** feature ↓, you can see the status of a vehicle at a specific point in time. This is useful for answering questions from Riders.





[3] Exploring Service Settings

- View Existing Service Settings;
- View Fleets and Rider Groups;

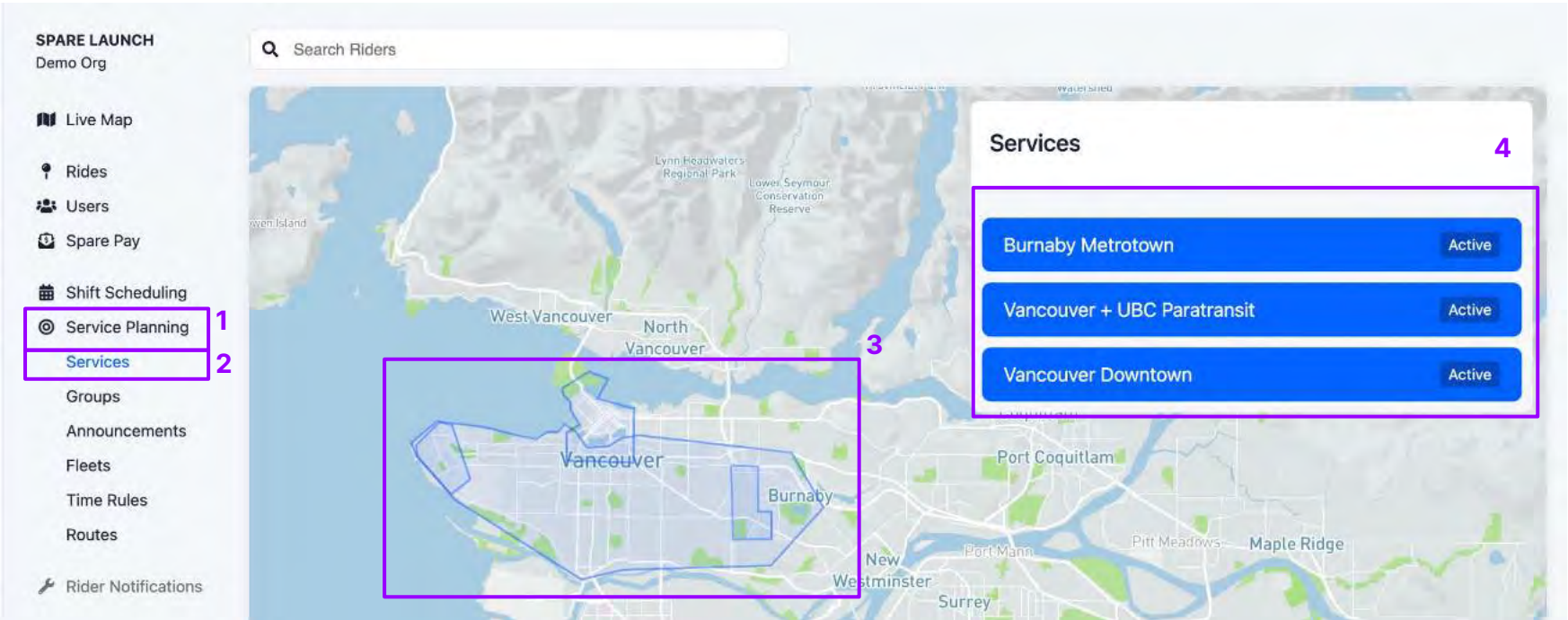
3.1. How to View Existing Service Settings



The majority of service settings are set up by administrators and service planners. Please reach out to your administrator regarding any changes to the settings.

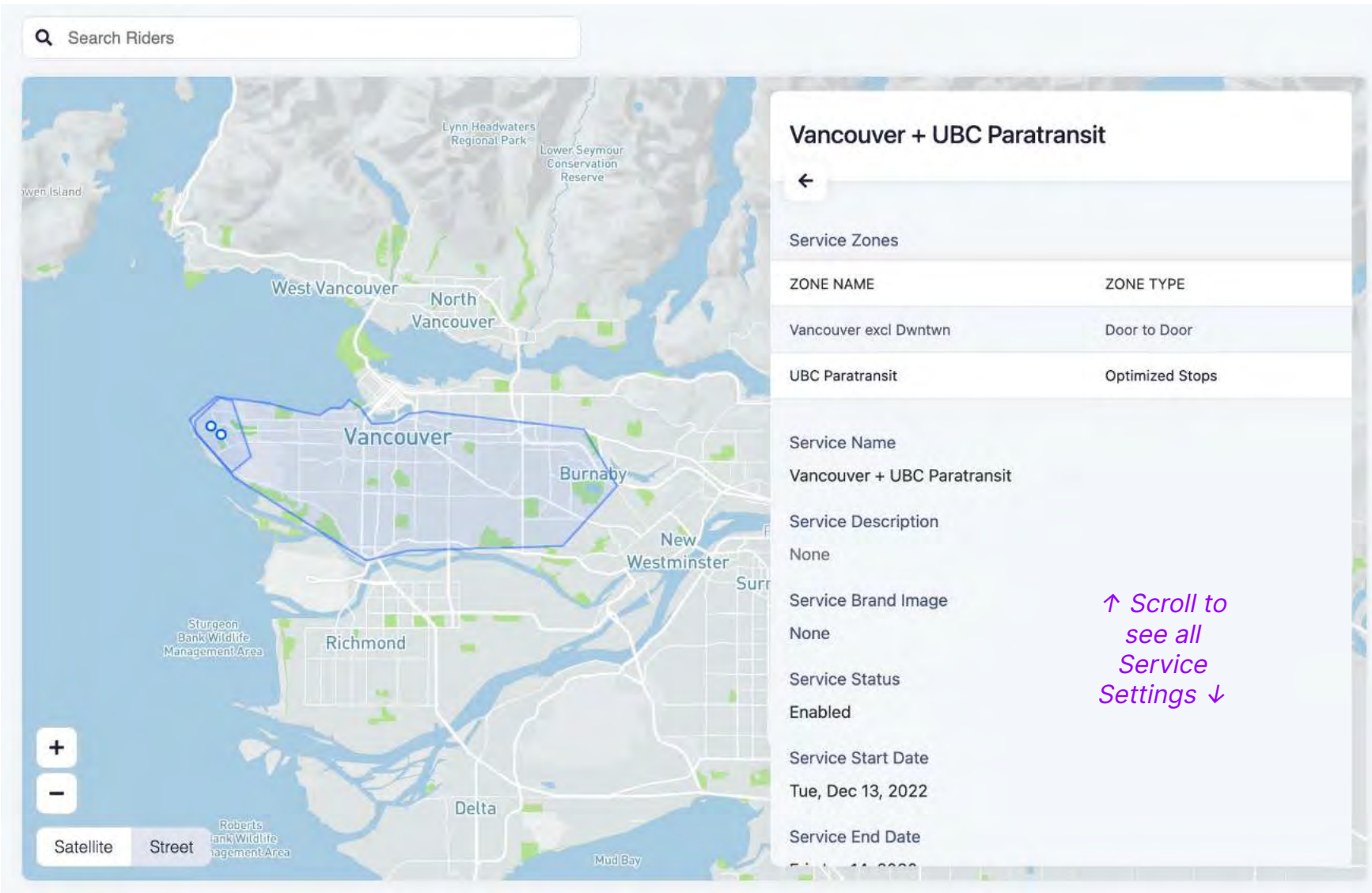
1 Identify Service Area and Status

From the **Service Planning** tab [1], go to **Services** [2]. You will see all **service inclusion zones** displayed on the map [3], as well as each service **name and its status**[4].



2 View Current Service Settings

Click on the service name to get redirected to its information card.



3.1. How to View Existing Service Settings

3 View Rider Groups

From the **Service Planning tab [1]**, go to **Groups [2]**. Click on the group name to see the list of riders and the name of the service associated with the group.

SPARE LAUNCH
Demo Org

Live Map

Rides

Users

Spare Pay

Shift Scheduling

Service Planning

Services

Groups

Announcements

Fleets

Time Rules

Routes

Search Riders

Groups

Filter

NAME	SECRET CODE	CREATED AT
Paratransit - Vancouver	0000	Wed, Dec 14, 2022 4:10 PM

1 results

Previous

Page 1 of 1

Next

i

For more information about riders, see section [8] Managing Riders.

4 View Fleets

From the **Service Planning tab [1]**, go to **Fleets [2]**. All existing fleets will be displayed. Click on the fleet name to open the **Fleet Information page**.

SPARE LAUNCH
Demo Org

Live Map

Rides

Users

Spare Pay

Shift Scheduling

Service Planning

Services

Groups

Announcements

Fleets

Time Rules

Routes

Search Riders

Fleets

Fleets

STATUS	NAME
Active	Demo Fleet

1 results

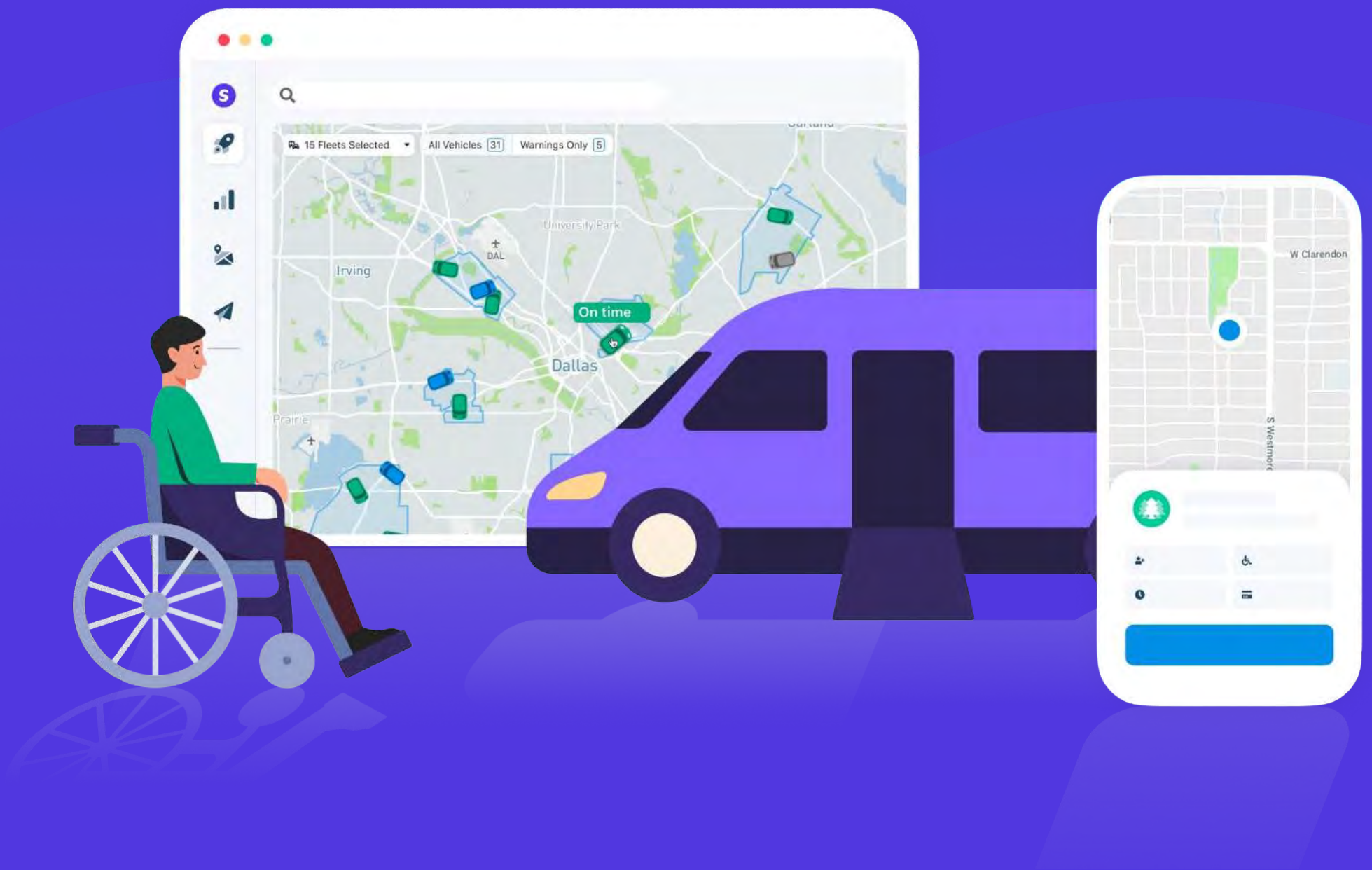
Previous

Page 1 of 1

Next

i

For more information about fleets, see section [6] Managing Driver Fleets.



[4] Managing Drivers

- Create and Edit Driver Records;
- Investigate Drivers' Activity;

4.1. How to Create a New Driver Record

i

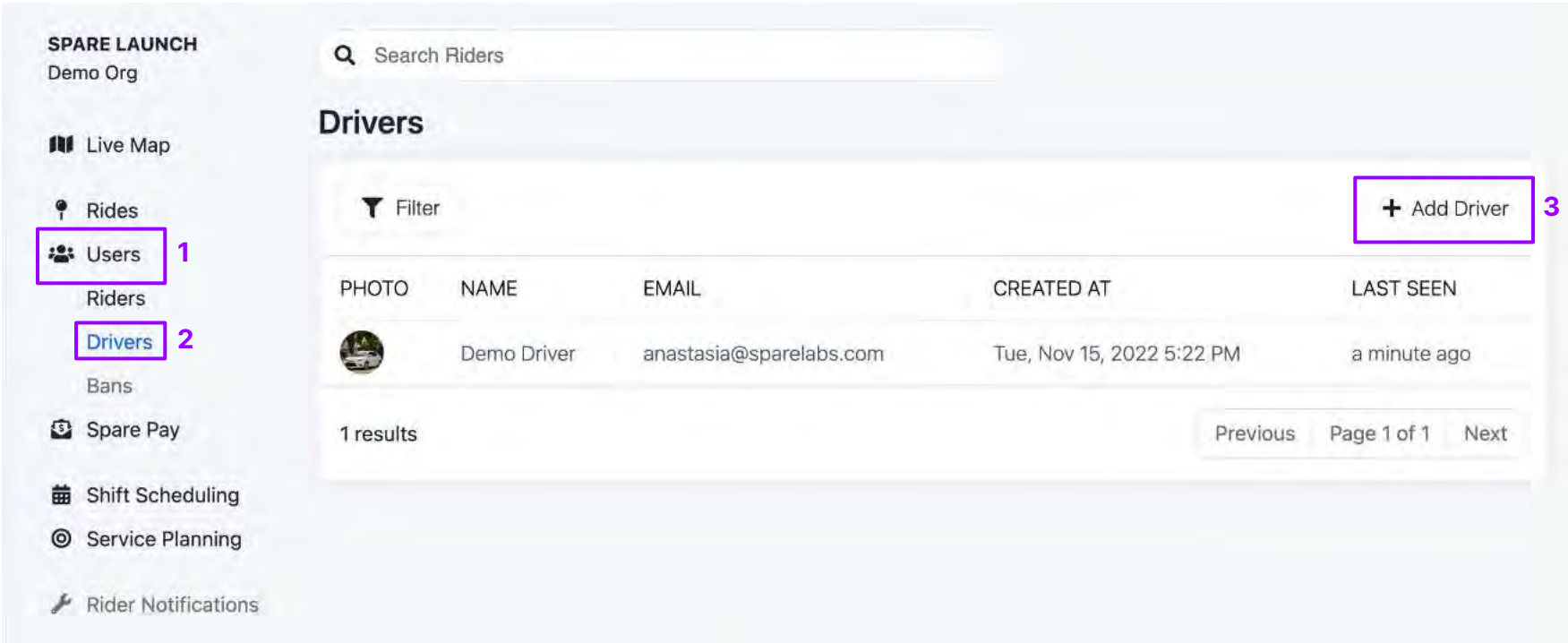
To schedule a shift, you will need the following:

✓ Driver Information; ✓ Vehicle Information; ✓ Fleet Information; ✓ Duty details;

In this chapter, we'll give you step-by-step instructions on how to manage **Driver Information**.

1 Add a New Driver

To access Drivers information, go to the **Users tab [1]** and select **Drivers [2]**.



From there, click **Add Driver [3]** to create a new driver account. You can add their contact information, photo, and fleets they are associated with.

Click **Create New Driver[4]** to save the changes.

Add Driver

New Driver Form

Photo

Upload an image

First Name

Last Name

Phone Number

US

 +1

Email

Unscheduled Driving

Search Fleets

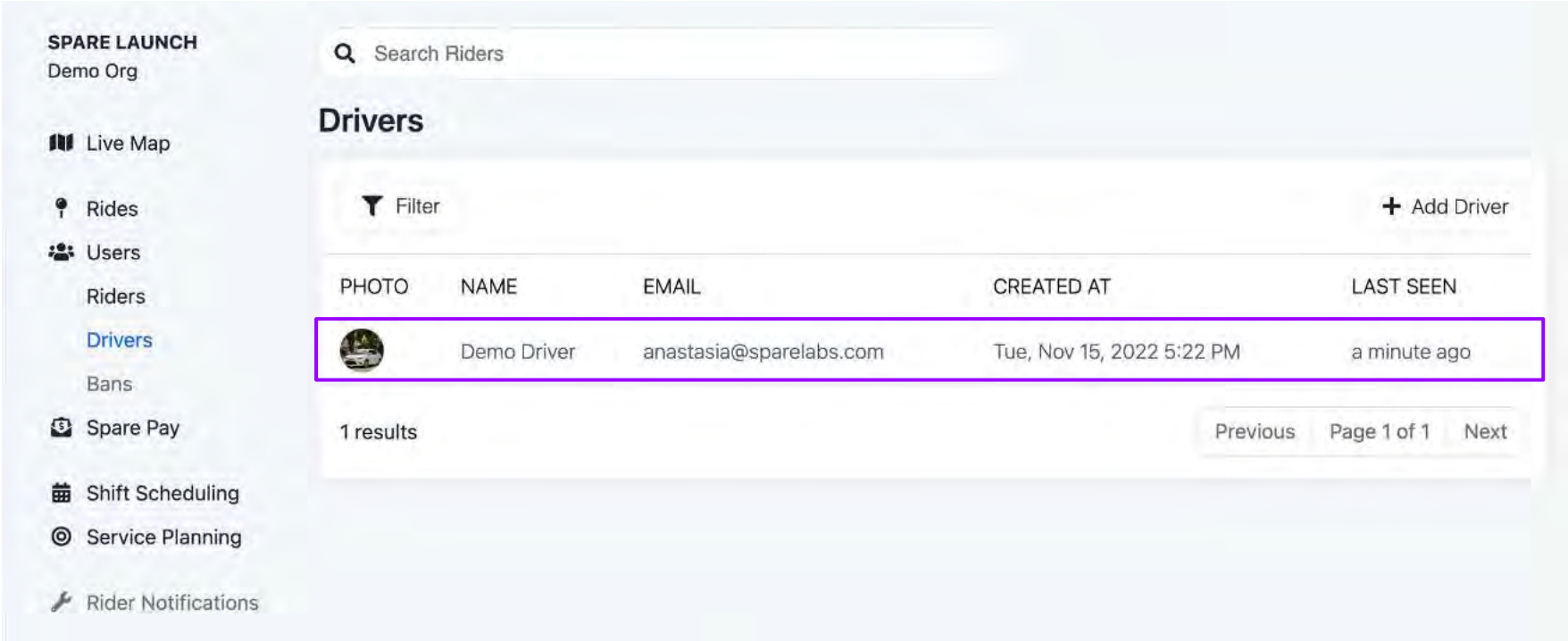
Allows drivers to drive their own vehicle for a given fleet, without a scheduled duty

Create New Driver

4.2. How to Edit an Existing Driver Record

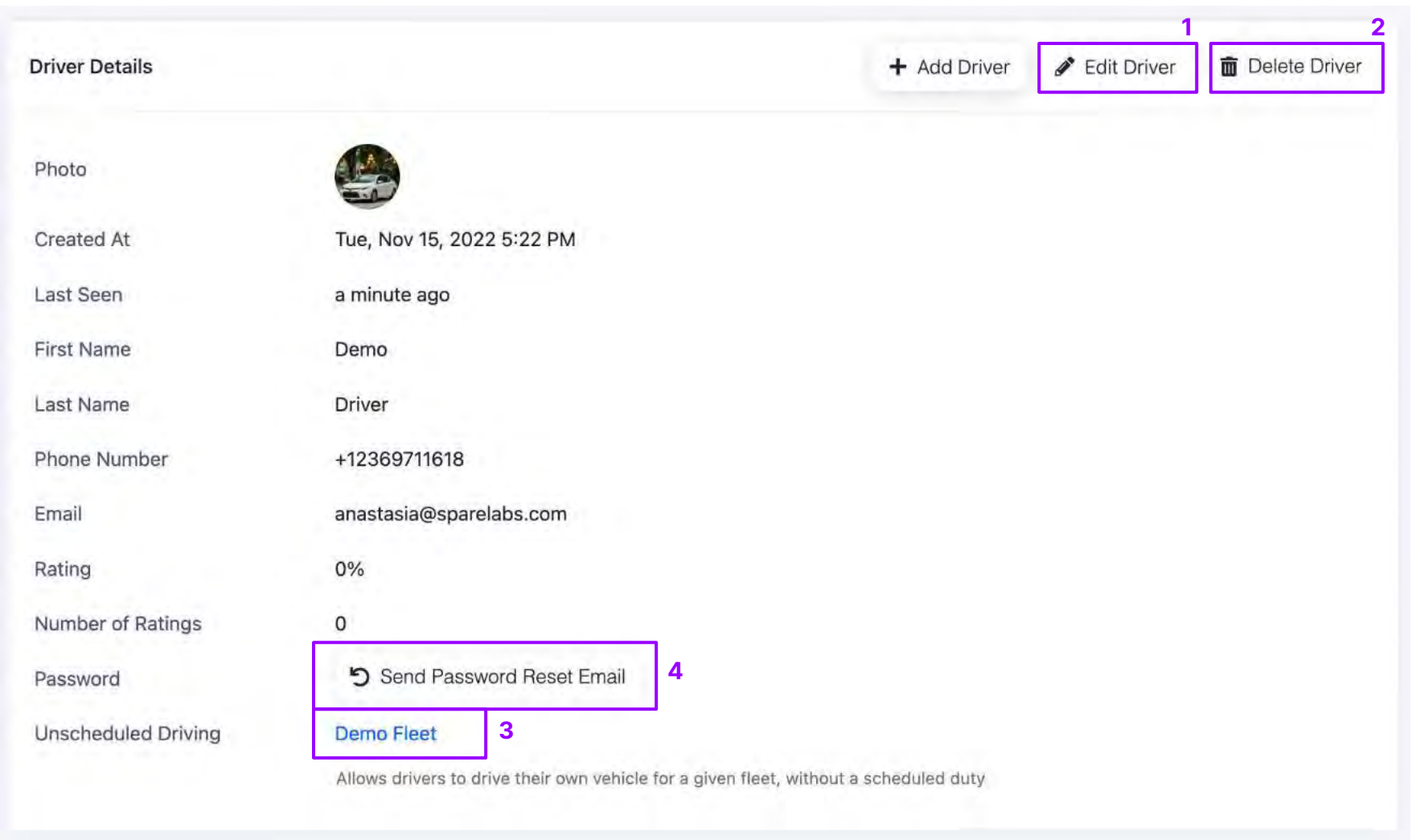
2 View/Edit/Delete an Existing Driver

To view or edit a Driver’s details, **click on their record line**. A Driver information page will appear.



From the Driver Information Page, you will be able to do the following:

- [1] Edit Contact information;
- [2] Delete the Driver Account;
- [3] View the fleet information they are associated with;
- [4] Reset their password;



You can also investigate a driver’s activity from this page. Find out more on the next pages.

4.3. How to Investigate Driver's Activity

1 Explore Duties History

From the Driver Information page, click on a **duty record** to jump into the Duty Information page.

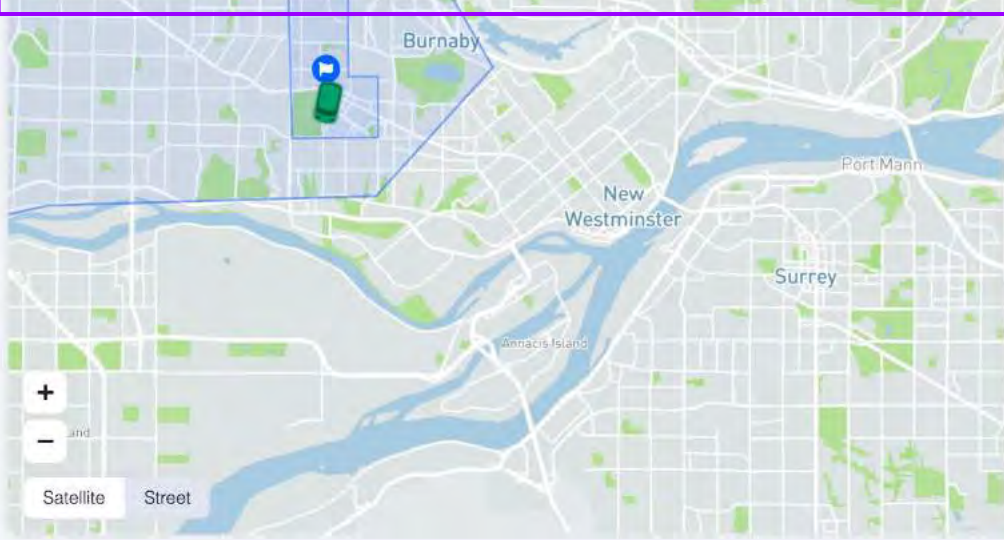
Duties					
STATUS	FLEET	VEHICLE	START TIME	END TIME	OWNERSHIP TYPE
Completed	Demo Fleet	Toyota Corolla	Mon, Jan 9, 2023 1:51 PM	Mon, Jan 9, 2023 4:51 PM	Organization-owned

From there, you will see the duty general information, its Time Travel map, duty itinerary, and the activity log (all changes happened to the duty)

Time Travel

Jan 9, 2023

3:48:21 PM



STOP	USER	TYPE	SCHEDULED TIME
		End Location	4:51 PM

Duty Itinerary

STATUS	TYPE	USER	REQUESTED TIME	SCHEDULED TIME	ADDRESS	COMPLETED TIME

2 View Devices & Vehicle Information

From the Driver Information page, scroll down to see the list of associated devices and vehicles (click on the vehicle record to get transferred to its information page).

Registered Devices

CLIENT ID	EXPO TOKEN	FIREBASE IID	DEVICE OS	DEVICE VERSION	APP TYPE	APP NAME	APP VERSION	LAST OPENED	REGISTERED AT
None	None	cv-mNCP3FONGpnuCcN UDeu	iOS	15.6.1	Driver	Spare Driver	2.42.183	3 hours ago	Nov 29, 2022 12:46 PM

1 results

PreviousPage 1 of 1Next

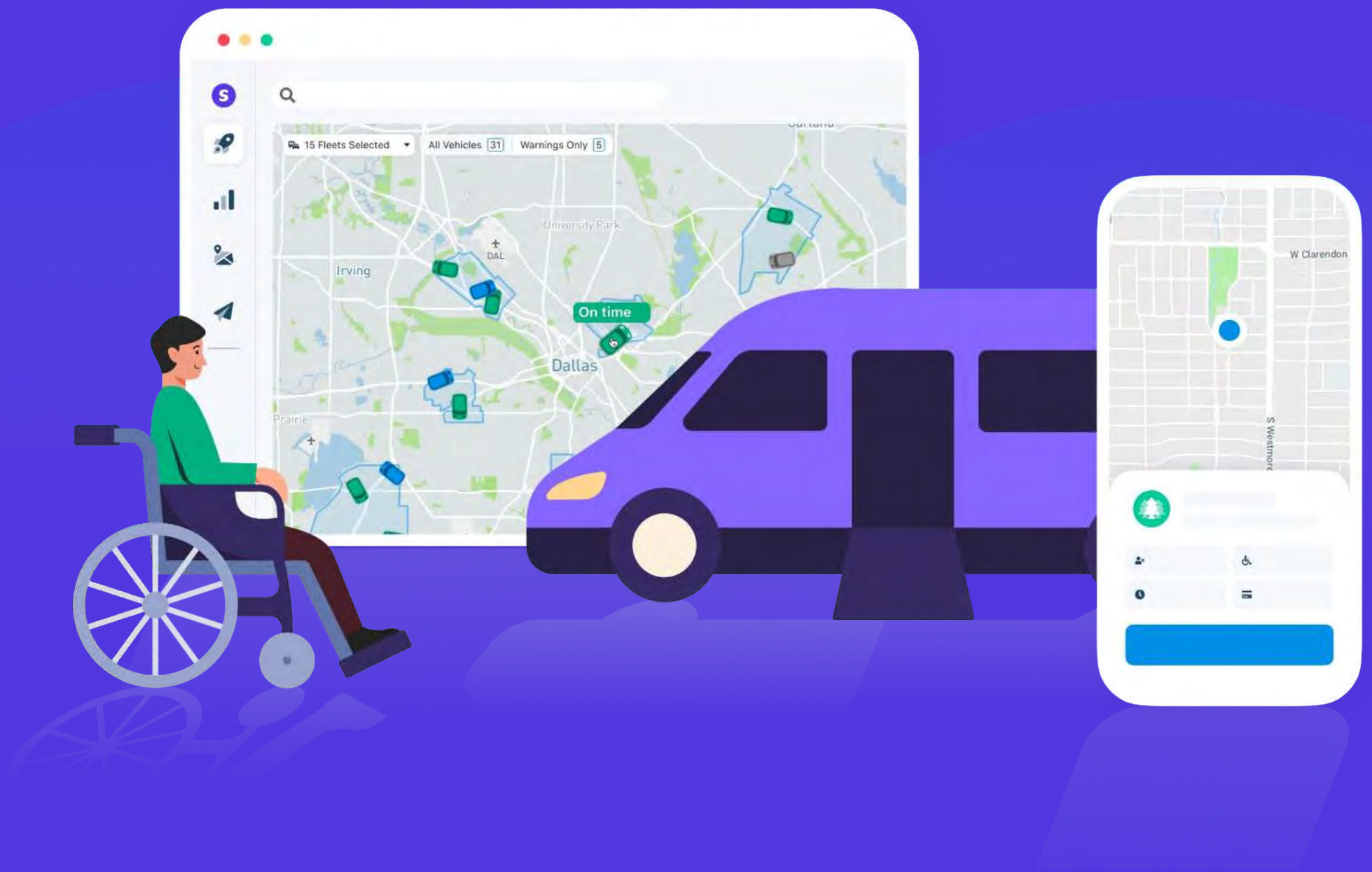
Driver-Owned Vehicles

Filter

Export Vehicles

+ Add Vehicle

IDENTIFIER	CREATED AT	LICENSE PLATE	MAKE	COLOR	MODEL	AUTONOMOUS
Toyota Corolla	Wed, Dec 7, 2022 12:24 PM	X1x23P	Toyotal	White	Corolla	No



[5] Managing Vehicles

- Add a New Vehicle;
- Edit/Delete Existing Vehicles;

5.1. How to Add a New Vehicle

i

To schedule a shift, you will need the following:

✓ Driver Information; ✓ Vehicle Information; ✓ Fleet Information; ✓ Duty details;

In this chapter, we'll give you step-by-step instructions on how to manage **Vehicle Information**.

1 Add a New Vehicle

Go to the **Shift Scheduling tab [1]** and select **Vehicles[2]**. Then, click **Add Vehicle[3]** to create a new record.

SPARE LAUNCH
Demo Org

Live Map

Rides

Users

Spare Pay

Shift Scheduling1

Duties

Vehicles2

Forecasting

Service Planning

Rider Notifications

Search Riders

Vehicles

Filter

Export Vehicles

Import Vehicles

Add Vehicle3

IDENTIFIER	CREATED AT	LICENSE PLATE	MAKE	COLOR	MODEL	AUTONOMOUS
Toyota Corolla	Wed, Dec 7, 2022 12:24 PM	X1x23P	Toyotal	White	Corolla	No
Toyota Yaris	Tue, Nov 29, 2022 12:35 PM	X1x23V	Toyota	Black	Yaris	No

2 results

PreviousPage 1 of 1Next

Fill in the **New Vehicle Form** and click **Create New Vehicle [4]** to save the changes.

New Vehicle Form

Identifier

Passenger Seats

License Plate

Make

Color

Model

Managed by User

Search Drivers

Leave this blank for organization-managed vehicles

Accessibility Features

TYPE	COUNT	ADDITIONAL SEATS REMOVED	REQUIRE FIRST IN, LAST OUT
No accessibility features have been added			

+ Add

Create New Vehicle4

5.2. How to View/Edit Existing Vehicles

1 Edit Vehicle Information

To view or edit vehicle information, click on its record to jump into the Vehicle Information Page.

SPARE LAUNCH
Demo Org

Live Map

Rides

Users

Spare Pay

Shift Scheduling

Duties

Vehicles

Forecasting

Service Planning

Rider Notifications

Search Riders

Vehicles

Filter

Export Vehicles

Import Vehicles

Add Vehicle

IDENTIFIER	CREATED AT	LICENSE PLATE	MAKE	COLOR	MODEL	AUTONOMOUS
Toyota Corolla	Wed, Dec 7, 2022 12:24 PM	X1x23P	Toyotal	White	Corolla	No
Toyota Yaris	Tue, Nov 29, 2022 12:35 PM	X1x23V	Toyota	Black	Yaris	No

2 results

Previous

Page 1 of 1

Next

From there, you will be able to view detailed information, **edit [1]** or **archive [2]** the vehicle. You will also be able to access the **driver's information [3]** from this page.

Toyota Corolla

Vehicle Details

Add Vehicle

Archive Vehicle

Edit Vehicle

Identifier

Toyota Corolla

Passenger Seats

4

License Plate

X1x23P

Make

Toyotal

Color

White

Model

Corolla

Managed by User

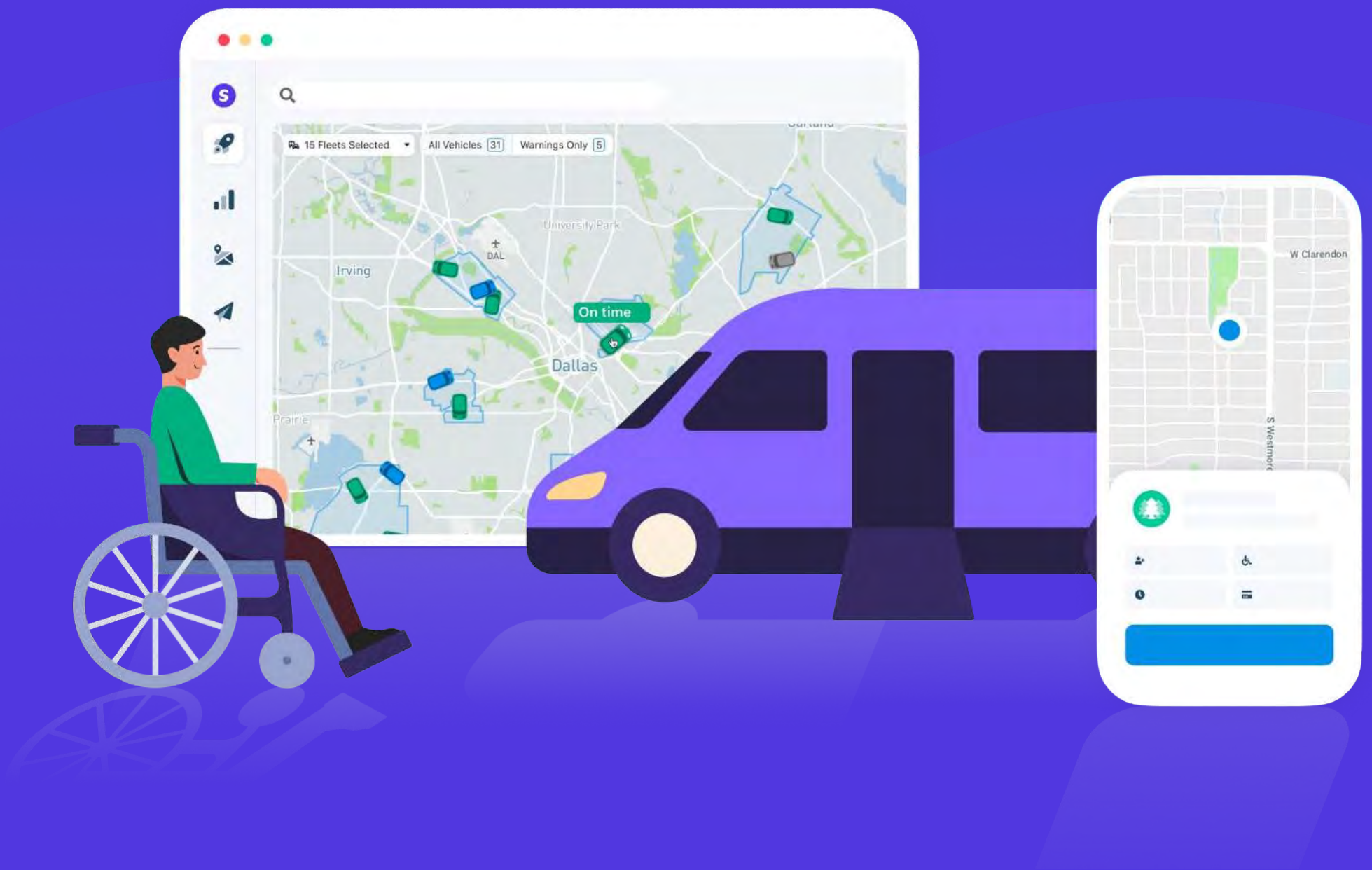
Demo Driver

Autonomous

No

Accessibility Features

TYPE	COUNT	ADDITIONAL SEATS REMOVED	REQUIRE FIRST IN, LAST OUT



[6] Managing Driver Fleets

- View Fleet Information and Linked Services;
- Re-assign Drivers to Fleets;

6.1. How to View Fleet Information



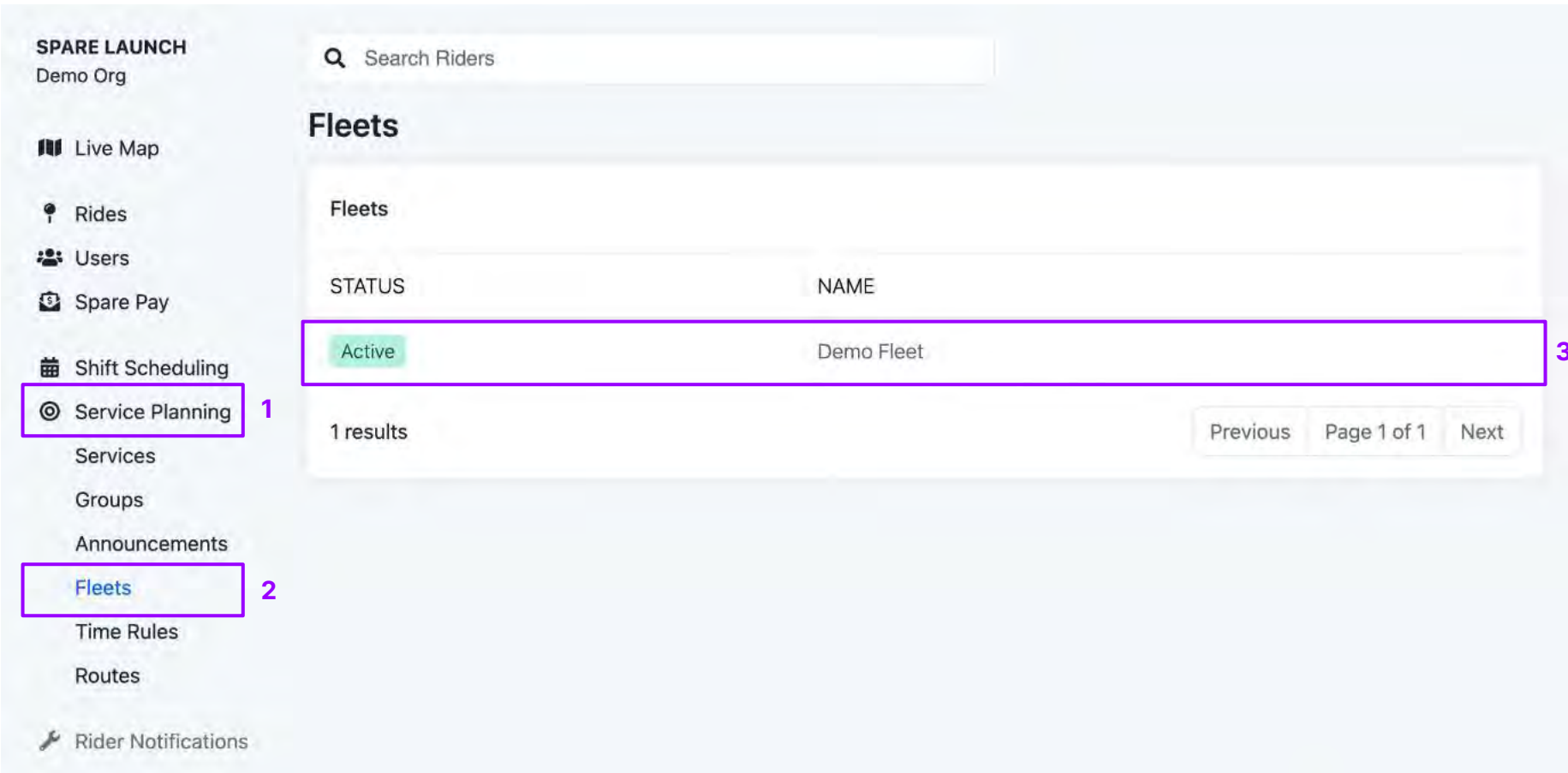
To schedule a shift, you will need the following:

- ✓ Driver Information;
- ✓ Vehicle Information;
- ✓ Fleet Information;
- ✓ Duty details;

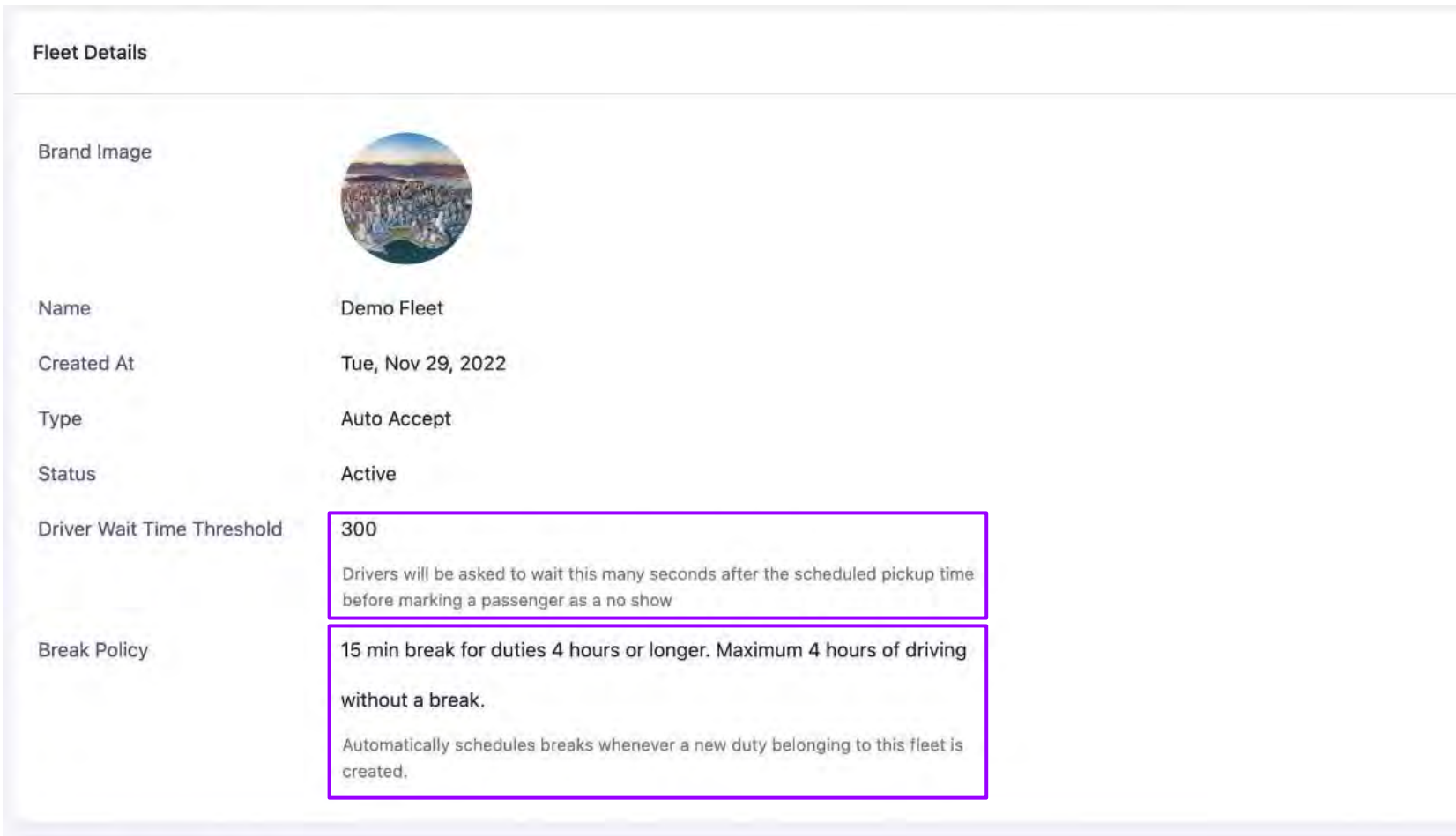
In this chapter, we'll give you step-by-step instructions on how to manage **Fleet Information**.

1 View Existing Fleets Detailed Information

Go to the **Service Planning tab**[1] and select **Fleets**[2]. Click on the **Fleet record**[3] to view its information.



You will then see the fleet details, including its status, **Driver Wait Time** settings and **Break Policy** (if applicable).



6.1. How to View Fleet Information

2 View the Linked Services Information

From the **Fleet Information Page**, scroll down to see the **Services Linked to This Fleet**. Click on the **service line** to see its details.

Services Linked To This Fleet			
SERVICE NAME	SERVICE STATUS	SERVICE START DATE	SERVICE END DATE
Vancouver + UBC Paratransit	Enabled	Tue, Dec 13, 2022	Fri, Jun 14, 2030
Vancouver Downtown	Enabled	Wed, Nov 30, 2022	Tue, May 30, 2023
Burnaby Metrotown	Enabled	Tue, Nov 29, 2022	Mon, May 29, 2023
3 results		Previous	Page 1 of 1 Next

You will then be redirected to the Service Information page.

Investigate the service settings to learn about its settings, such as boarding times, rider types, fare rules, flexibilities, and other information.

Q Search Riders

Vancouver + UBC Paratransit

←

Leave-At Forwards Flexibility (minutes)
10 min
Once a rider's request is confirmed, their pickup time may be moved later by this many minutes.

Leave-At Backwards Flexibility (minutes)
0 min
Once a rider's request is confirmed, their pickup time may be moved earlier by this many minutes.

Arrive-By Backwards Flexibility (minutes)
20 min
Once a rider's request is confirmed, their arrive-by dropoff time may be moved earlier by this many minutes.

Scheduled Search Leave-At Forwards Flexibility (minutes)
120 min
Scheduled requests will be booked up to this many minutes after the requested leave-at time.

Scheduled Search Leave-At Backwards Flexibility (minutes)
60 min
Scheduled requests will be booked up to this many minutes before the requested leave-at time.

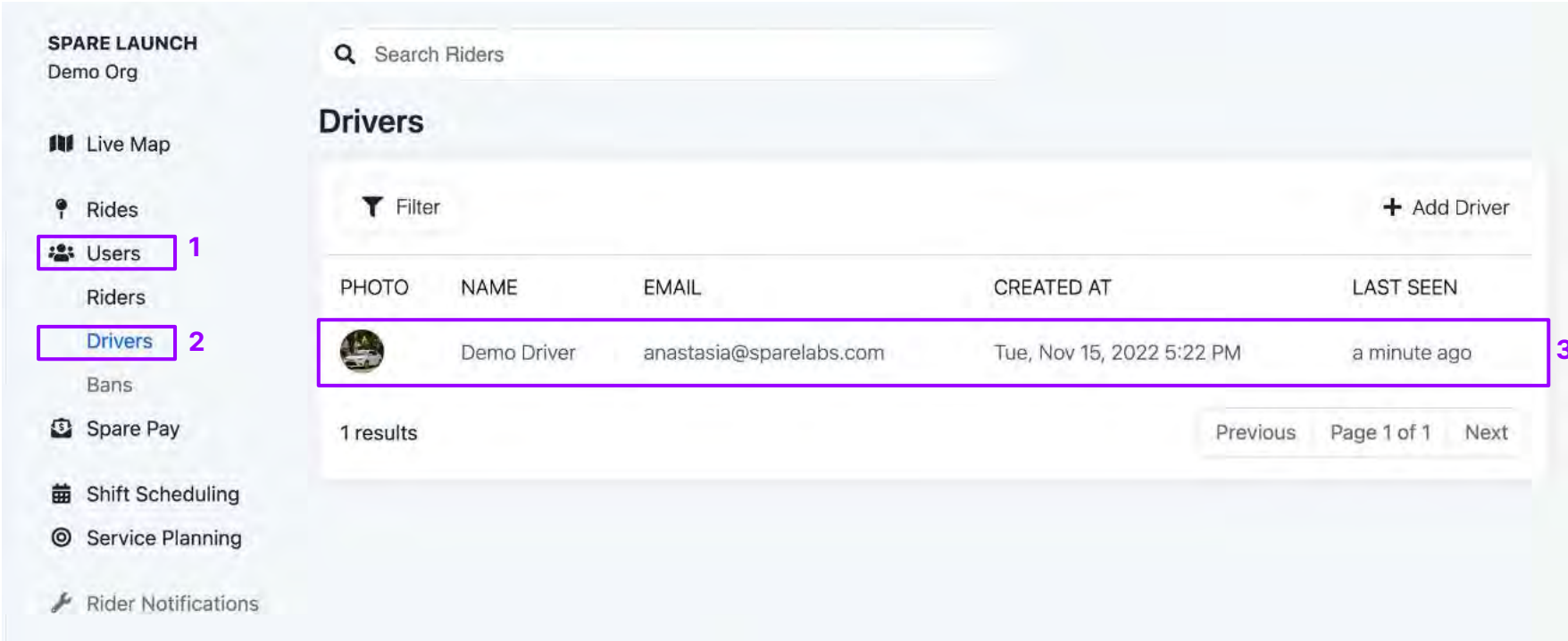


Note that **you can also view Service Information from the Service Planning tab** (Service Planning → Services → Service Name)

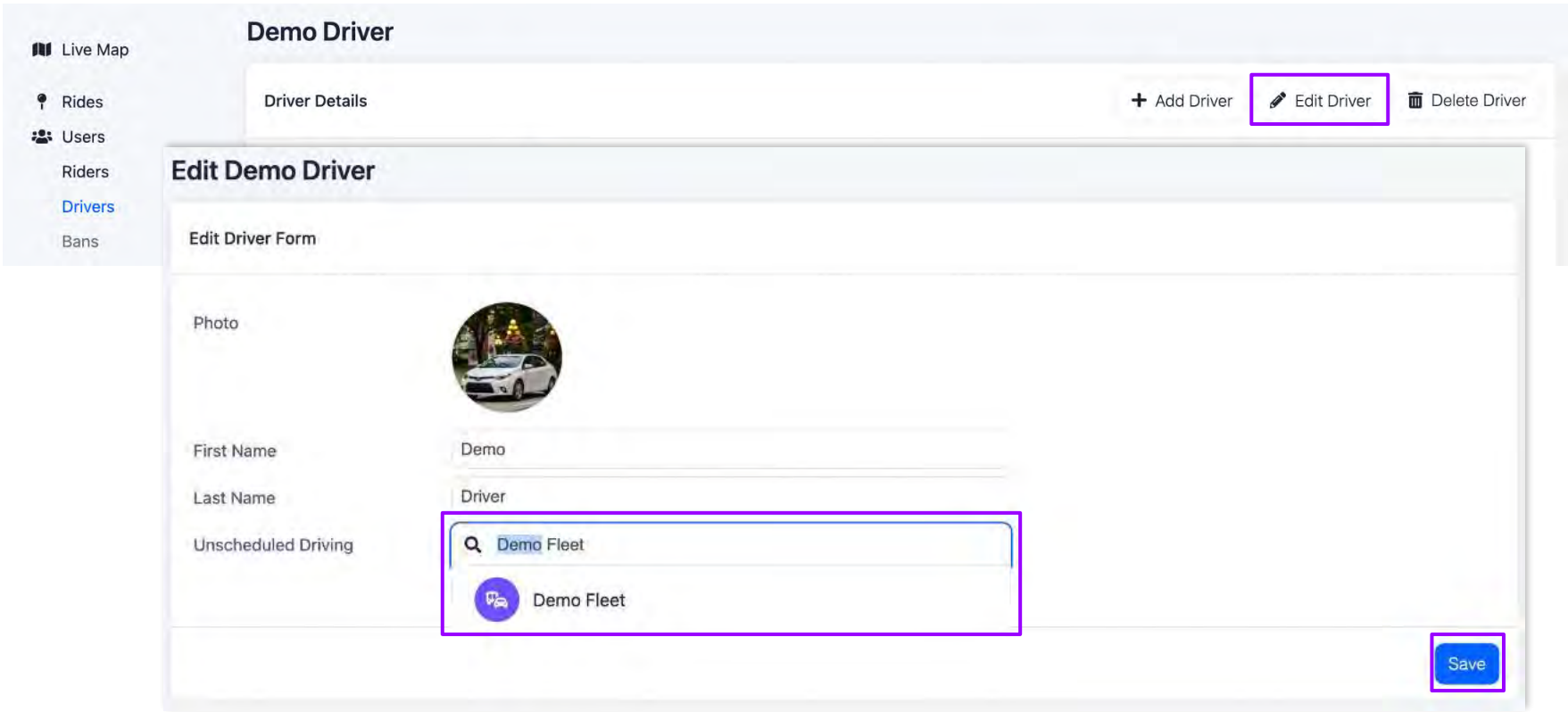
6.2. How to Re-Assign Drivers to Fleets

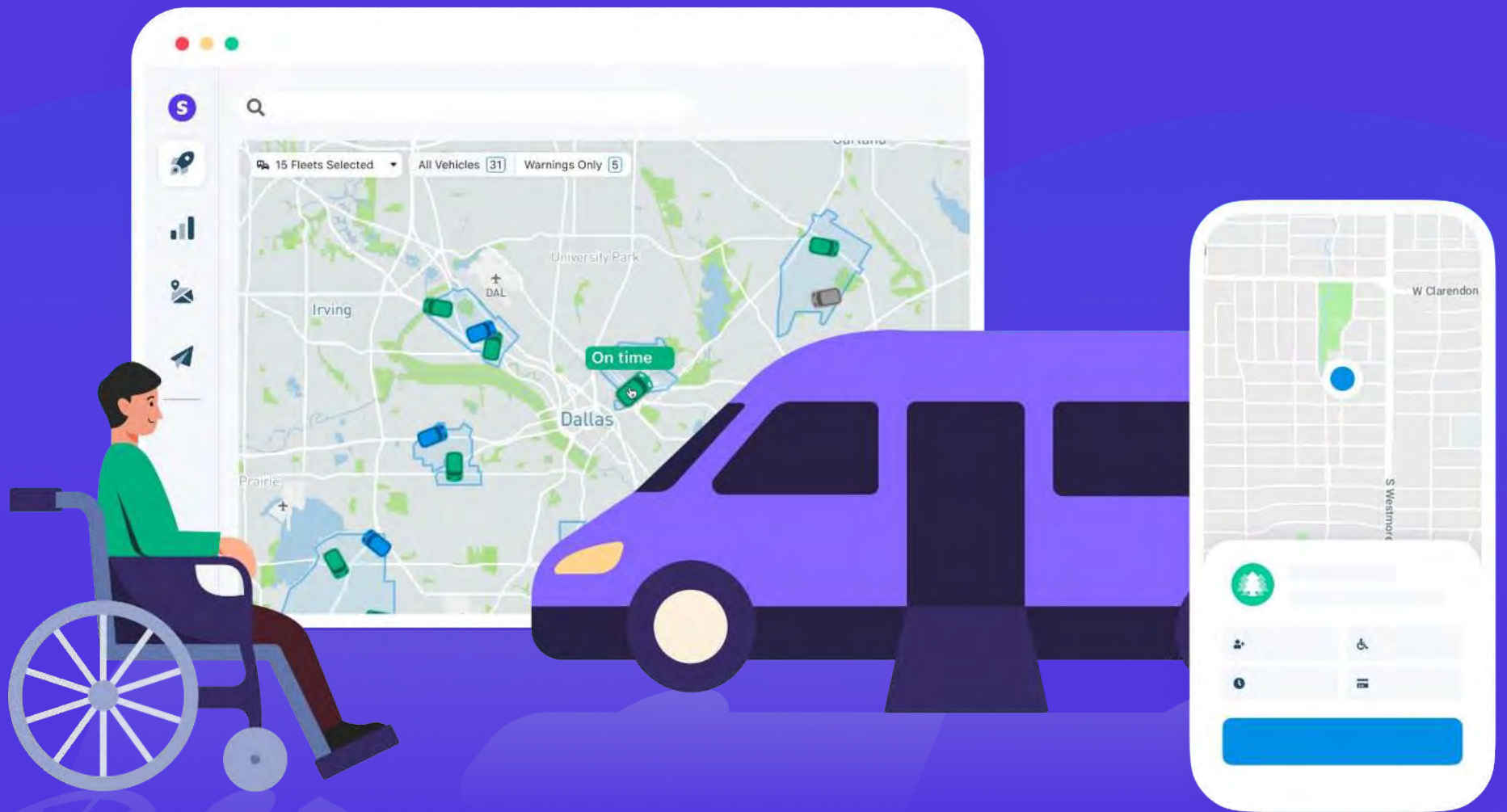
1 Assign Driver to Another Fleet

To assign a driver to another fleet, go to the **Drivers tab (Users[1] → Drivers[2])** and click on the **driver record[3]**. You will then be redirected to the **Driver Information page**.



From there, click **Edit Driver** to go into the **Edit Driver Form**.
Start **typing a new fleet name** and select the fleet from the **drop-down** menu.
Click **Save** to accept the changes.





[7] Managing Shifts/Duties

- Schedule a New Duty
- Edit an Existing Duty

7.1. How to Schedule a New Duty

i

To schedule a duty, you will need the following:

✓

Driver Information;

✓

Vehicle Information;

✓

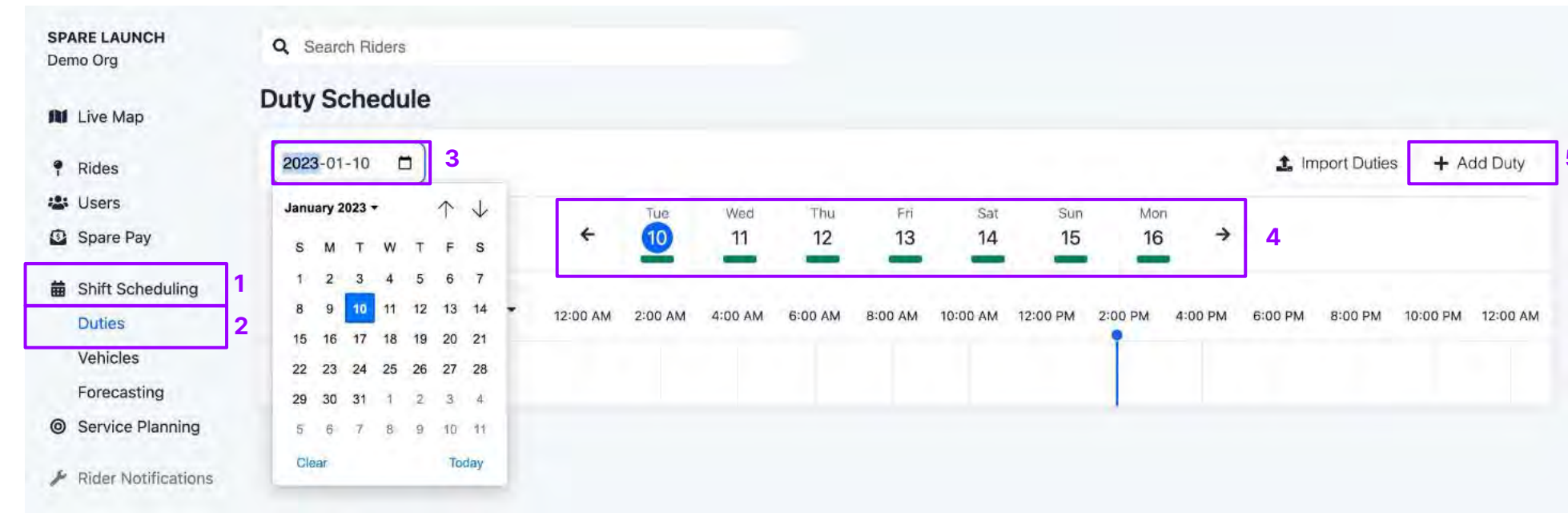
Fleet Information;

✓

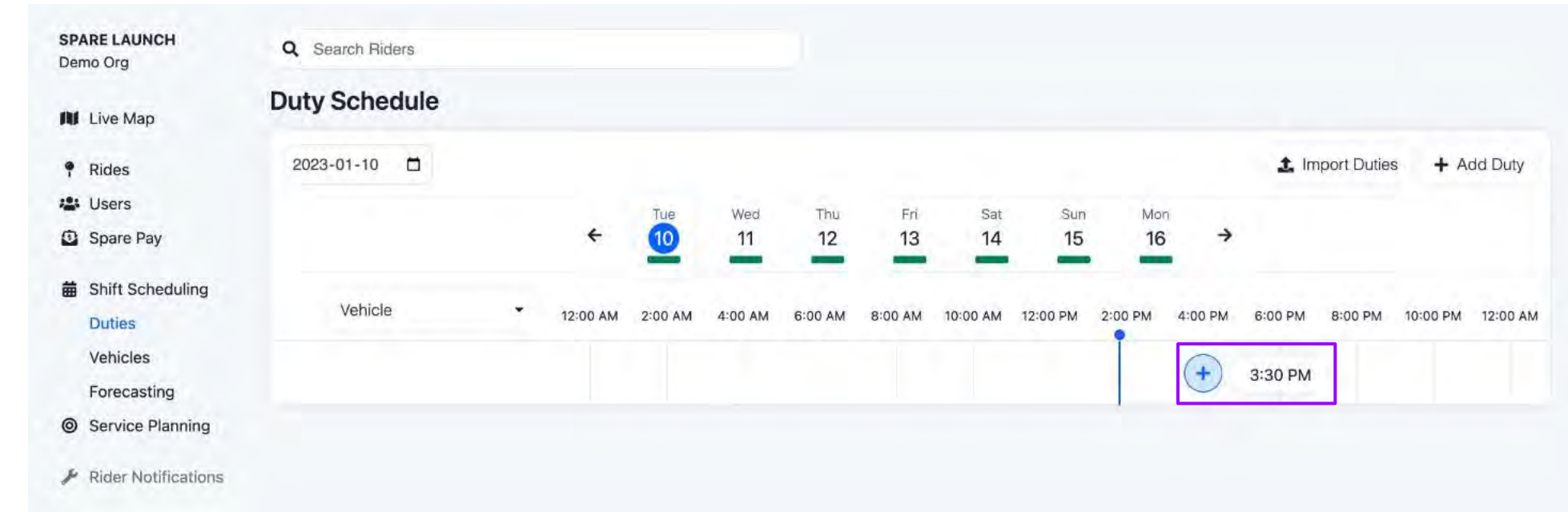
Duty details;

1 Add a New Duty

To create a new shift, go to the **Shift Scheduling tab [1]** and select **Duties [2]**.
From there, select the date in the **drop-down calendar [3]** or by clicking **arrows [4]**, and click **Add Duty [5]**.



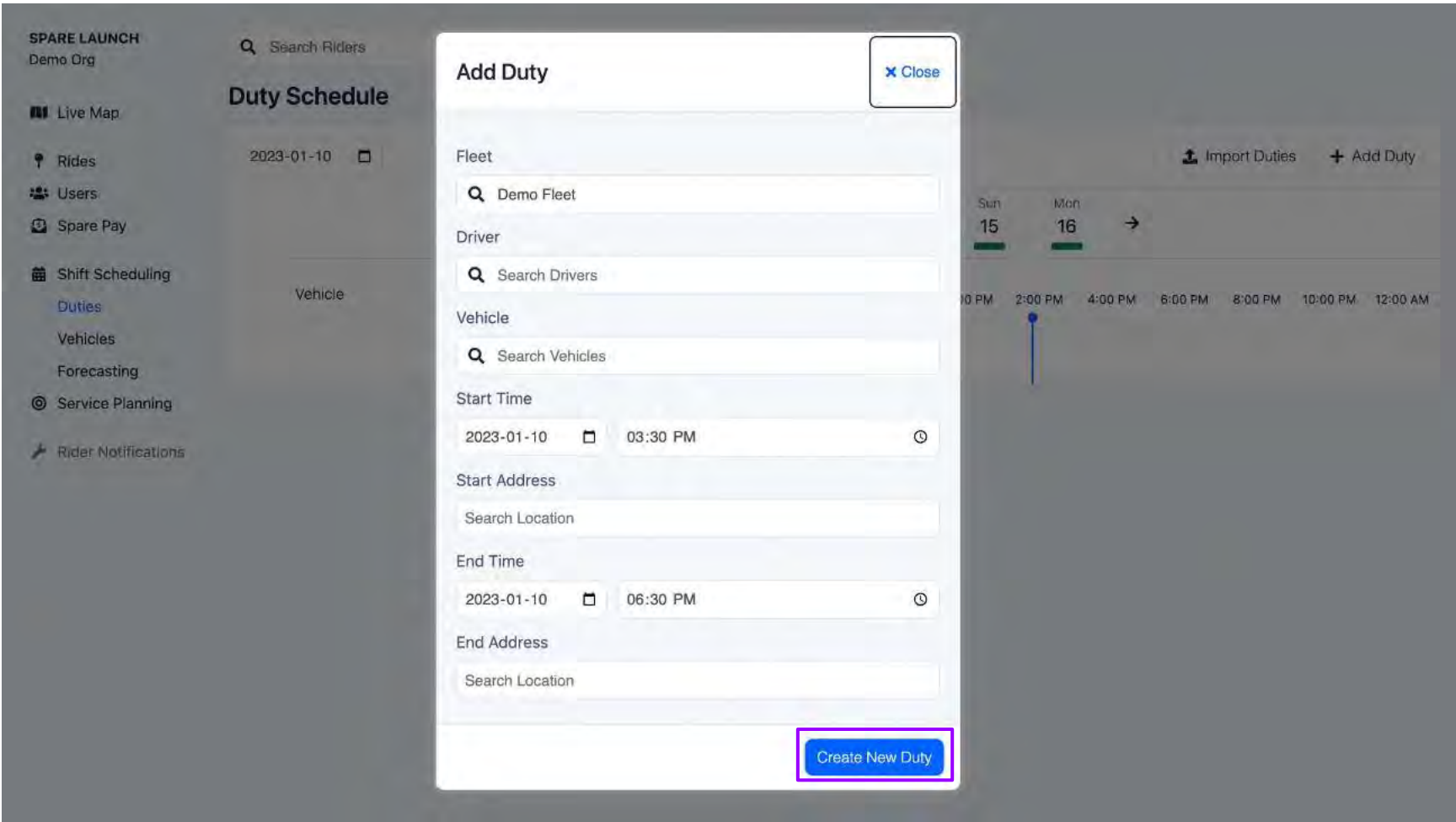
Or simply select the date and time and click on the Duty Schedule field and click on the **+** sign to add a duty.



7.1. How to Schedule a New Duty

2 Fill in the Duty Information

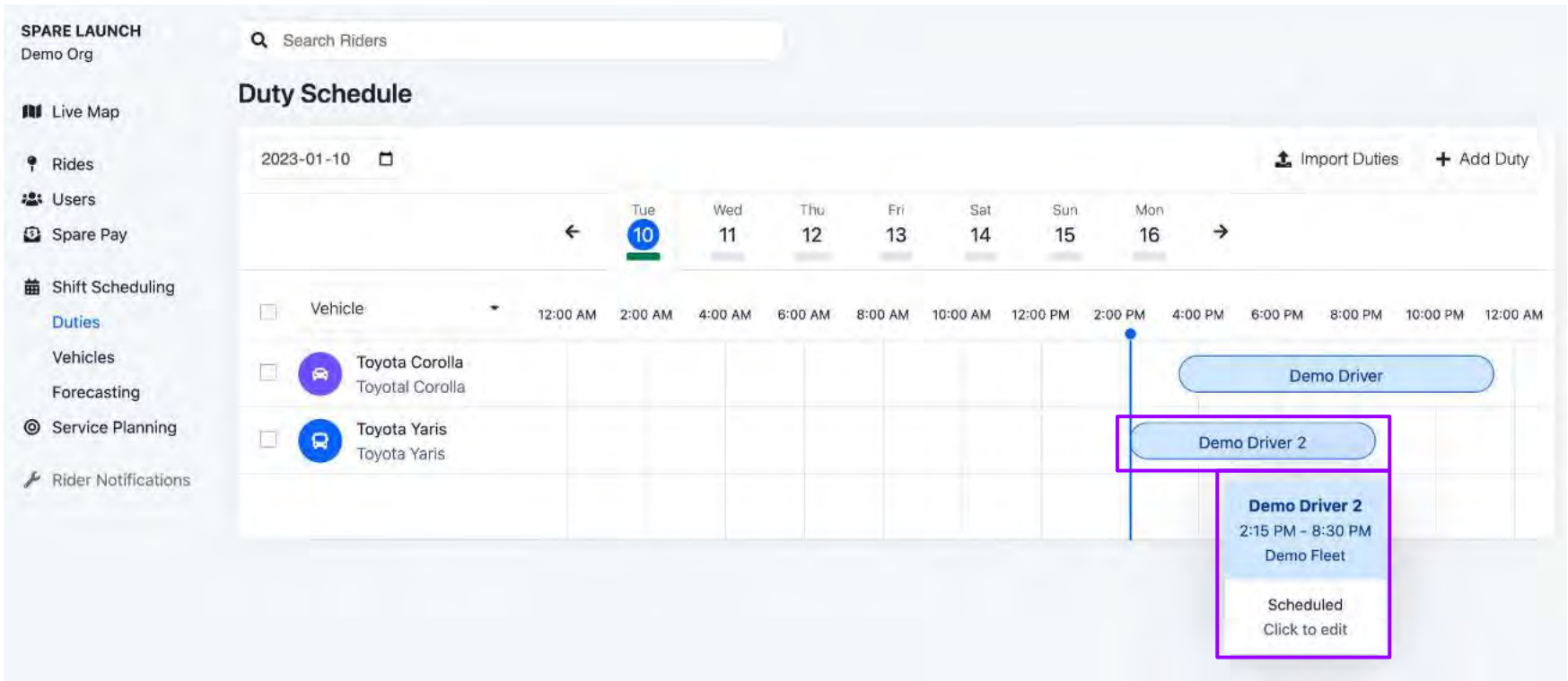
In the **Add Duty** form, complete all required fields and click **Create New Duty** to apply changes.



Once the duty is created, you will see it in the Duty Schedule. Add as many duties as required by repeating the steps above.

3 View the Duty Information

You can view the duty information by hovering over it. A card with a brief description will appear. Click on the duty to see more details.

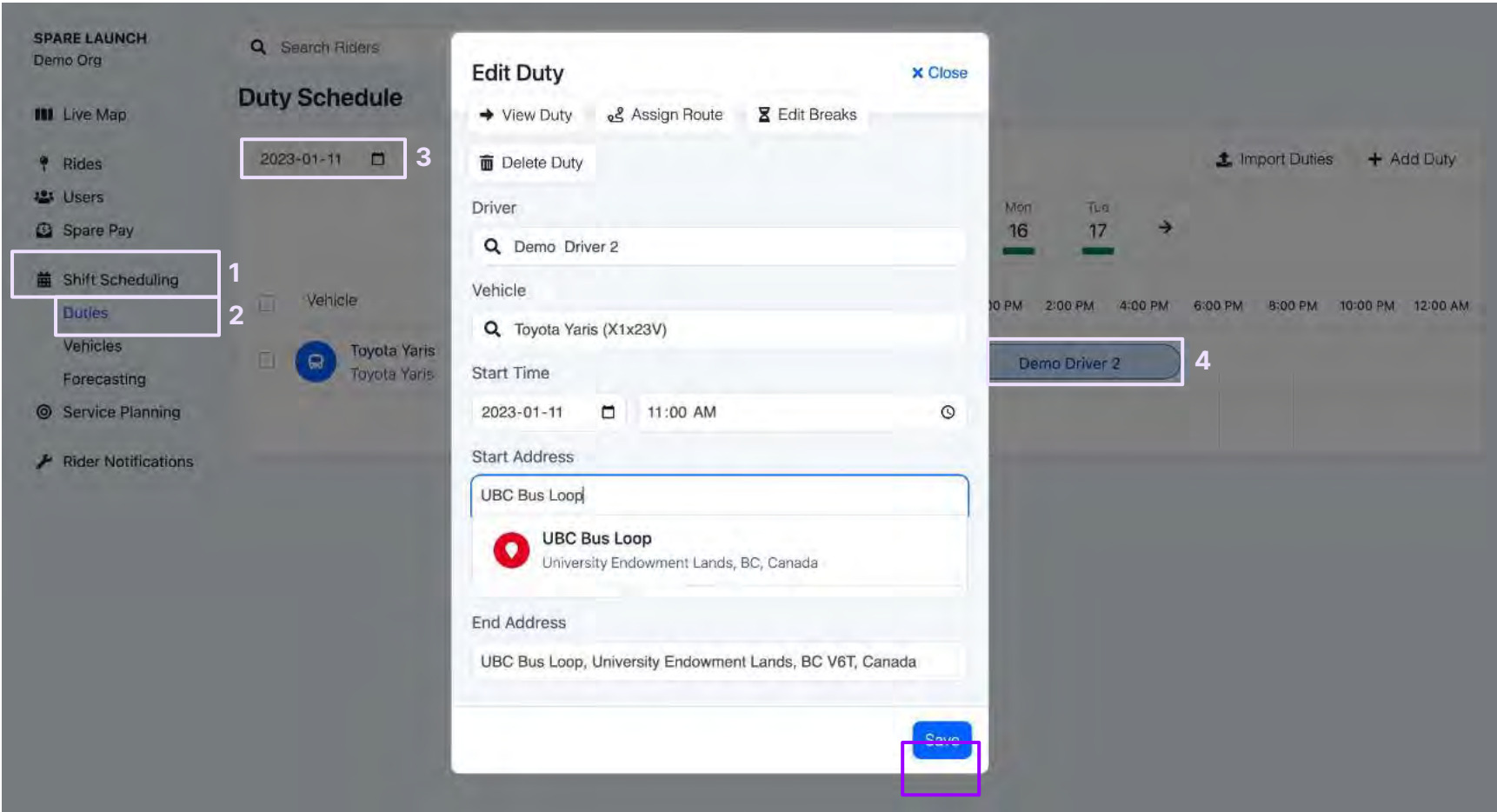


7.2. How to Edit an Existing Duty

1 Make Changes

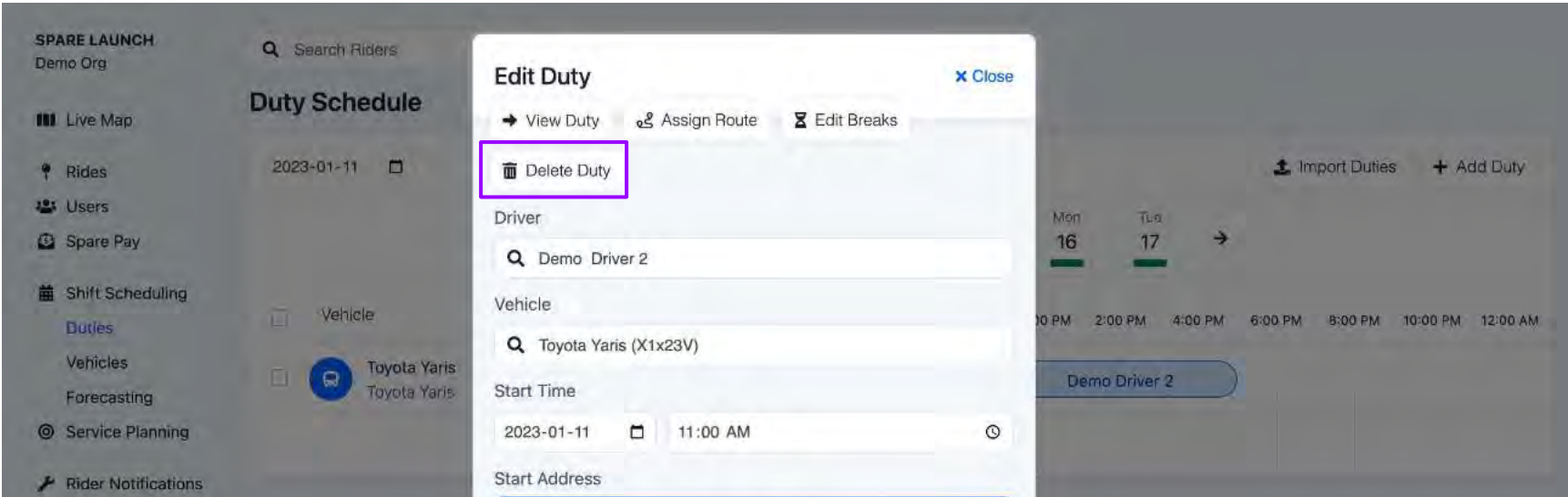
From the **Shift Scheduling** tab [1], jump into **Duties** [2]. **Select the date** [3], **locate the duty record**[4] and click on it.

Update the editable fields and click **Save** to apply the changes.



2 Delete/Cancel a Duty

To cancel or delete a duty, open the **Duty Information** card (see previous step) and click **Cancel/Delete Duty**. **Deleted duties will disappear entirely while** canceled duties will be displayed as grey.



One can **delete** a duty if the duty is **scheduled in the future** AND there are **no requests associated with it**.

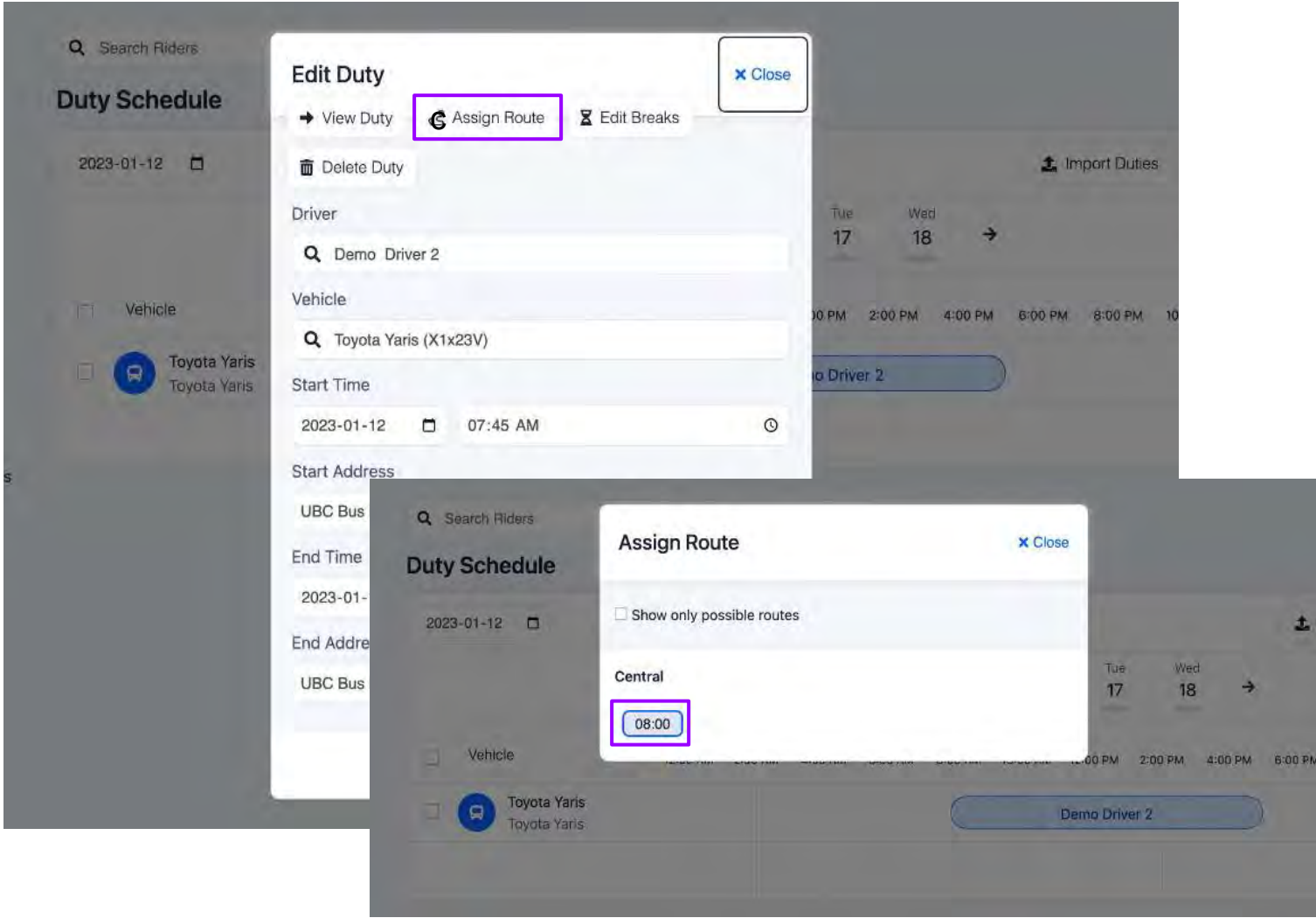
If there are any requests associated with the duty (even if they are further removed and reshuffled by Spare GOLD Engine), or the duty is already in progress, the duty can only be Canceled and NOT Deleted.

7.2. How to Edit an Existing Duty

3 Assign a Route to a Duty (if applicable)

To assign an existing route to a specific duty, open the **Duty Information card** and click **Assign Route**. An Assign Routes menu will appear, enlisting all **pre-built routes** (if enabled for your organization).

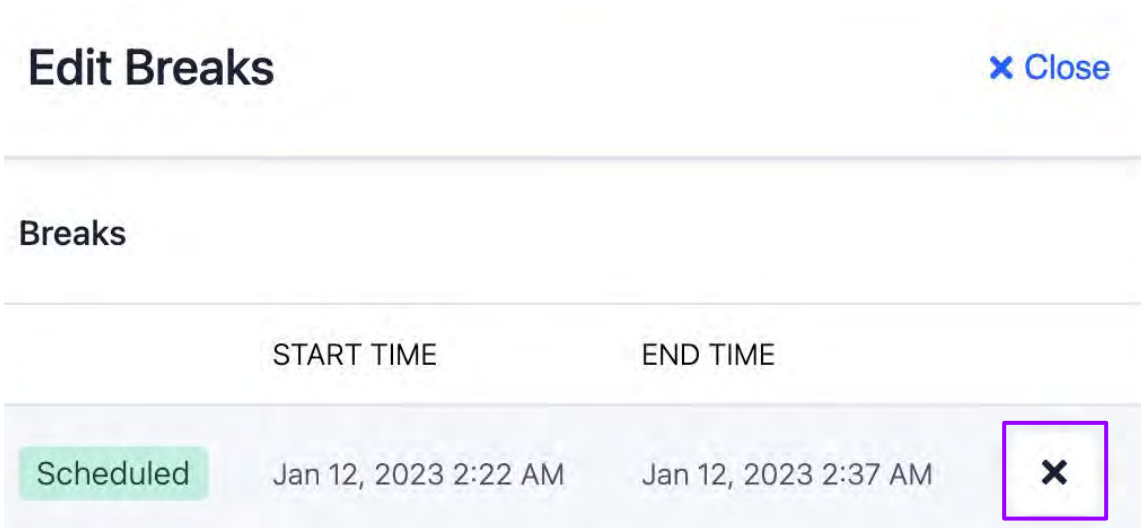
Click on the **route start time** to assign it to the selected duty.

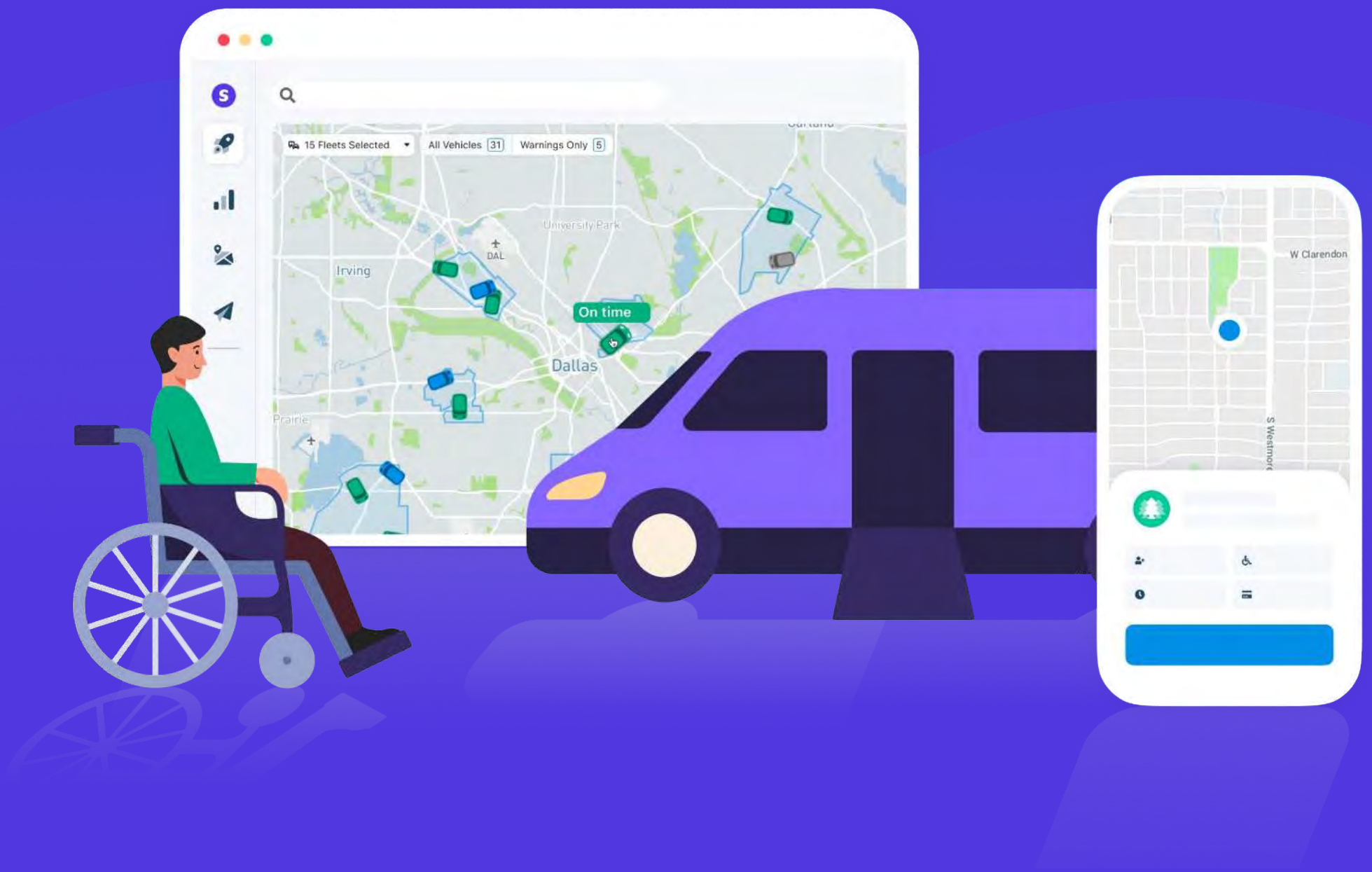


4 Delete Driver Breaks (if applicable)

i If your organization has Automated Driver Breaks function enabled, driver breaks will be scheduled for all duties, according to each Fleet Policy.

To manually delete a scheduled break, open the Duty Information card and click Edit Breaks. Remove the break from the appeared list by clicking **X** next to it.





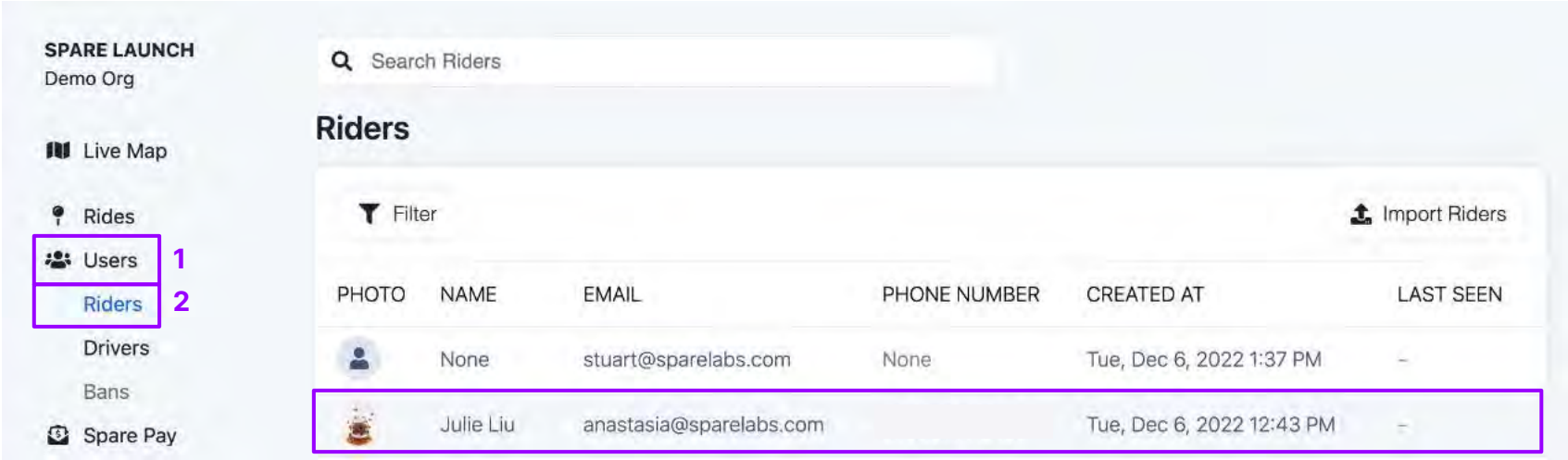
[8] Managing Riders

- View Rider Information
- Edit Rider Information

8.1. How to View Rider Information

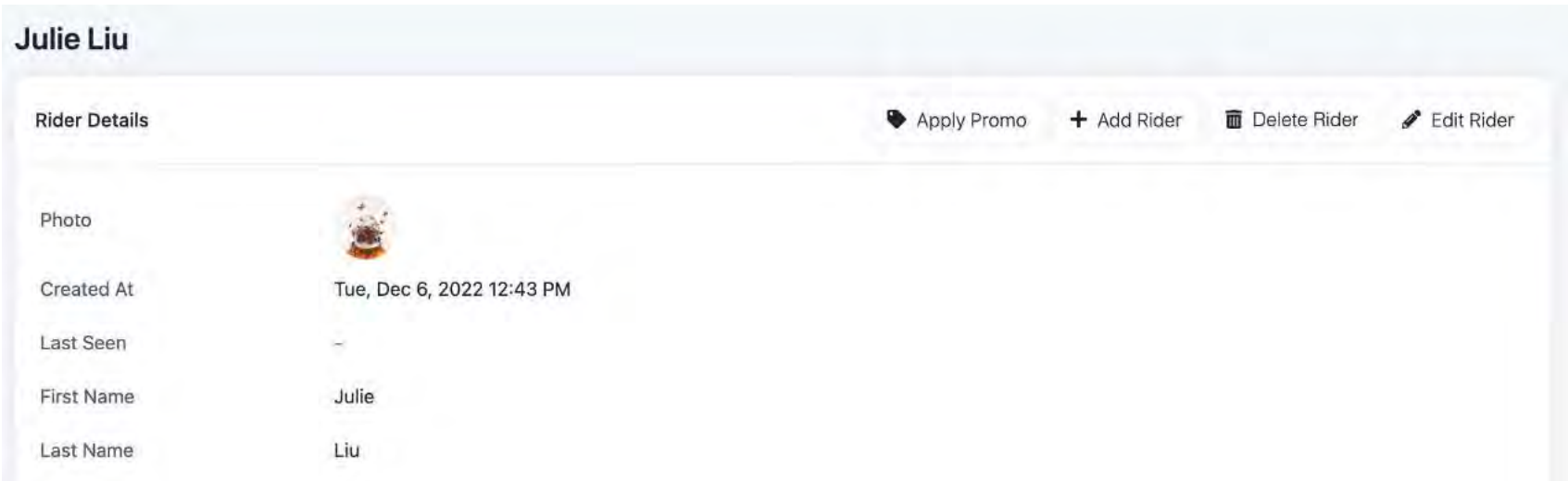
1 View Rider Information

You can see a list of all the Riders registered in the system by clicking **Users[1]** on the left side menu and then **Riders[2]**:



By clicking on a Rider you will be taken to the **Rider Details page** for that specific Rider. For each Rider you can see the follow details:

Contact Information	First name, Last name, Phone, Email (optional for Riders)
Default Request Preferences	You can set a default number (and type) of passengers or required accessibility features for the rider. The new defaults will automatically show up when you in the future create new trip requests for this specific rider.
Default Notes	You can also add default Notes for the Rider that will be shared with the Driver when picking up the Rider.
Favourite Locations	By adding favorite locations a booking agent can simply search for Home in the pickup location field and the saved Home address will show up.
Charges, Promos, Fare Passes, and Payment Methods	If your organization has these features enabled in the Spare Platform.
Requests	This is an overview of all the requests for the rider.



8.2. How to Edit Rider Information



Please reach out to your administrator if you do not have editing permissions.

2

Edit Rider Information

To edit rider information, click on the **Rider record** to open the Rider Information page and select **Edit Rider**. Click **Save** to apply the changes.

SPARE LAUNCH
Demo Org

Live Map

Rides

Users

Riders

Drivers

Bans

Spare Pay

Search Riders

Riders

Filter

Import Riders

PHOTO	NAME	EMAIL	PHONE NUMBER	CREATED AT	LAST SEEN
	None	stuart@sparelabs.com	None	Tue, Dec 6, 2022 1:37 PM	-
	Julie Liu	anastasia@sparelabs.com	+12369711618	Tue, Dec 6, 2022 12:43 PM	-

Julie Liu

Rider Details

Apply Promo

Add Rider

Delete Rider

Edit Rider

Photo

Created At

Tue, Dec 6, 2022 12:43 PM

Last Seen

-

First Name

Julie

Last Name

Liu

Save

3

Delete a Rider Record

To delete rider information, click on the **Rider record** to open the Rider Information page and select **Delete Rider**.

Julie Liu

Rider Details

Apply Promo

Add Rider

Delete Rider

Edit Rider

Photo

Created At

Tue, Dec 6, 2022 12:43 PM

Last Seen

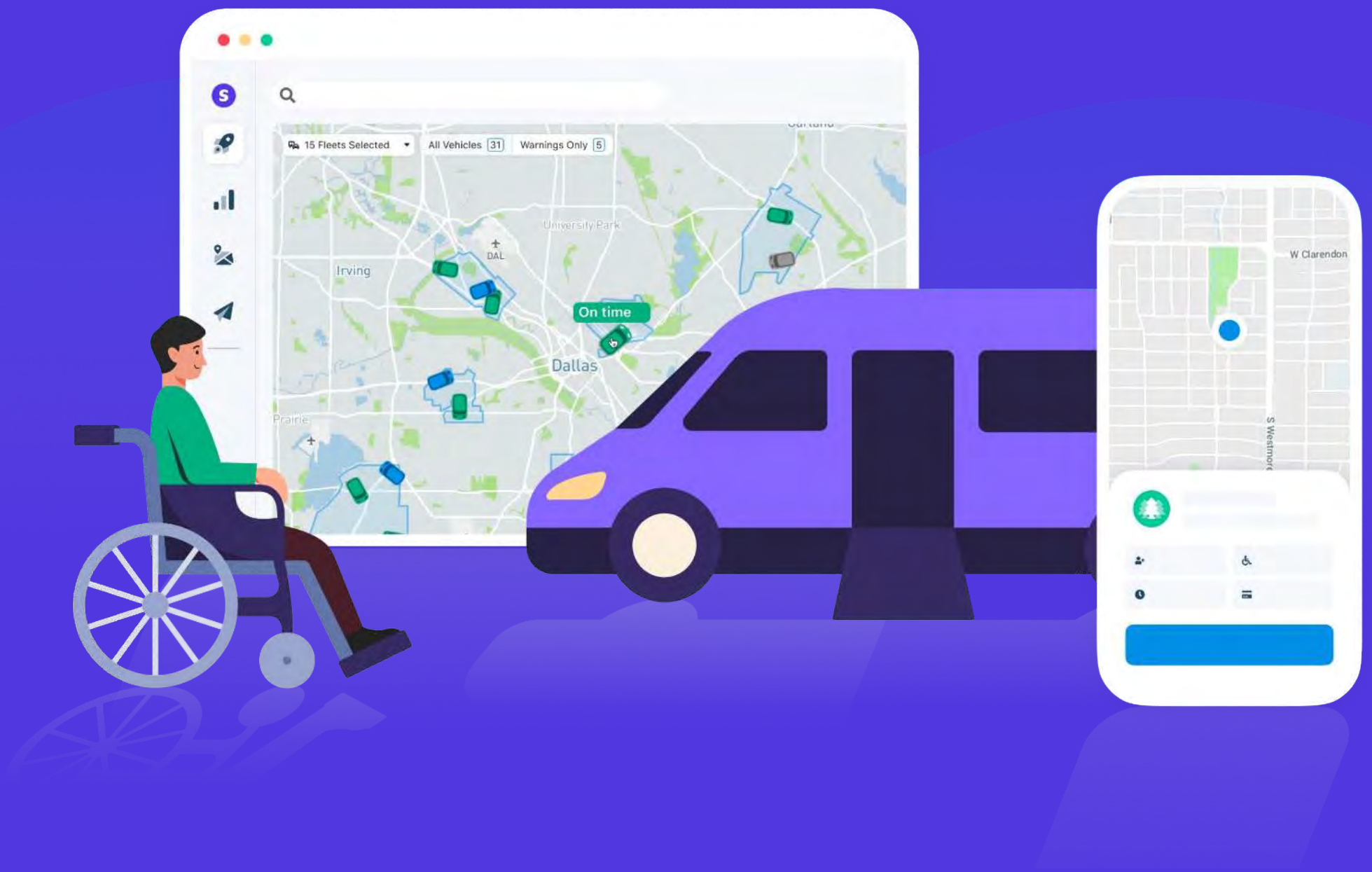
-

First Name

Julie

Last Name

Liu



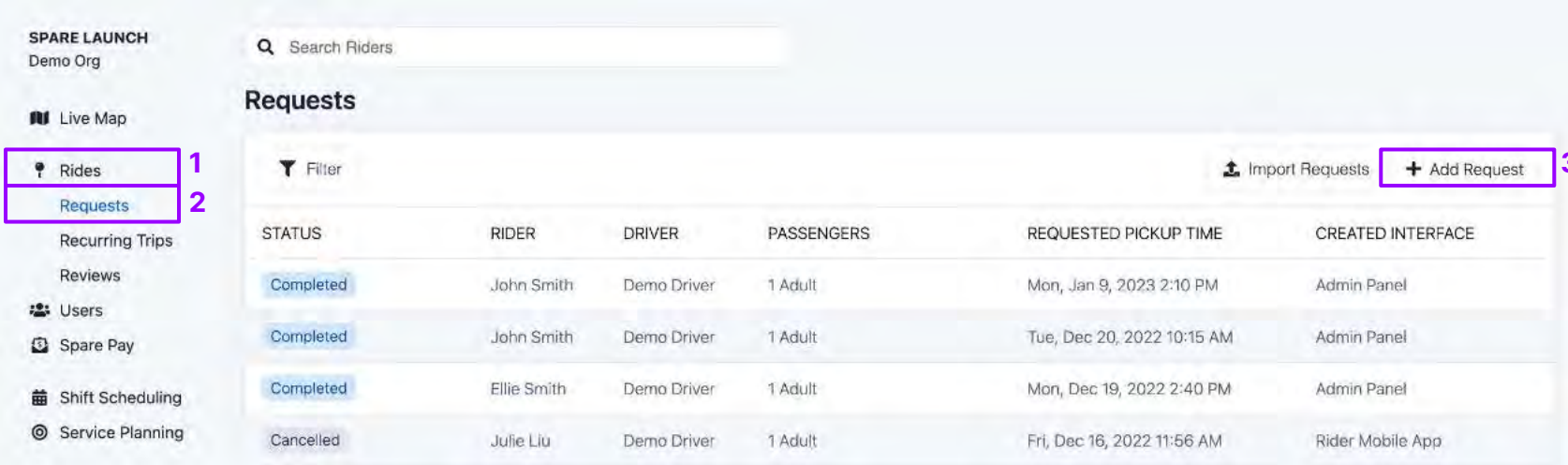
[9] Managing Trip Requests

- Create a Trip Request
- Edit a Trip Request
- Create and Edit a Recurring Trip

9.1. How to Create Requests

1 Add a New Request

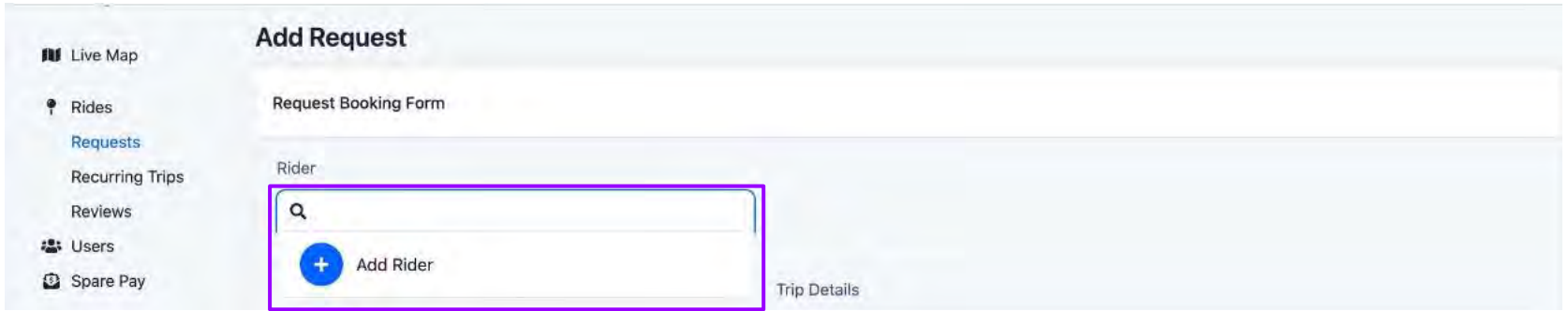
Go to the **Rides tab** [1] and select **Requests**[2]. Click **+Add Requests** [3]



2 Select a Rider

From the **Request Booking Form**, Find the rider by typing a *name or phone number* into the **Search riders field**[1] and select on the desired user in the dropdown menu.

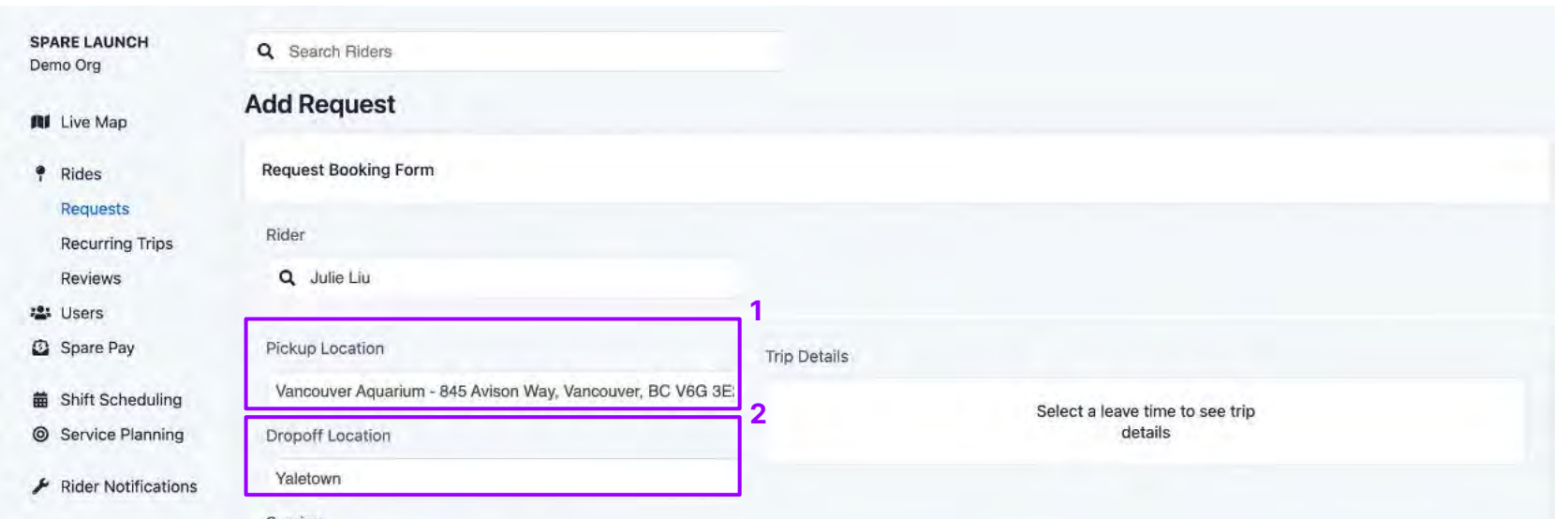
If the rider does not have a user profile, select **Add User** and enter in their details.



3 Select Pick-up & Drop-off Locations

In the **Pickup Location field** [1], type in the address of the riders pickup location and select the virtual stop or address in the dropdown menu.

Do the same for the **Dropoff Location** [2].

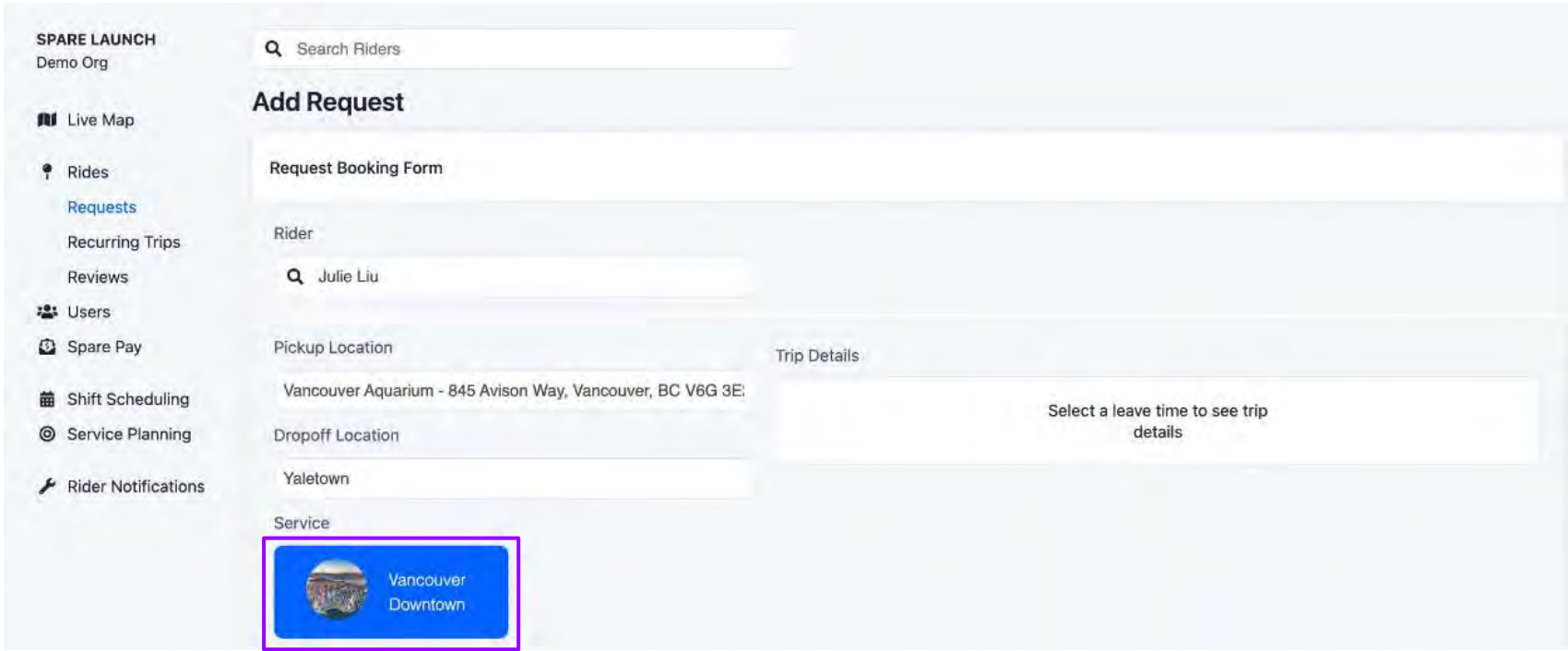


Pro Tip: Allow the browser to fetch your location. This will populate with relevant results faster.

9.1. How to Create Requests

4 Select the Service

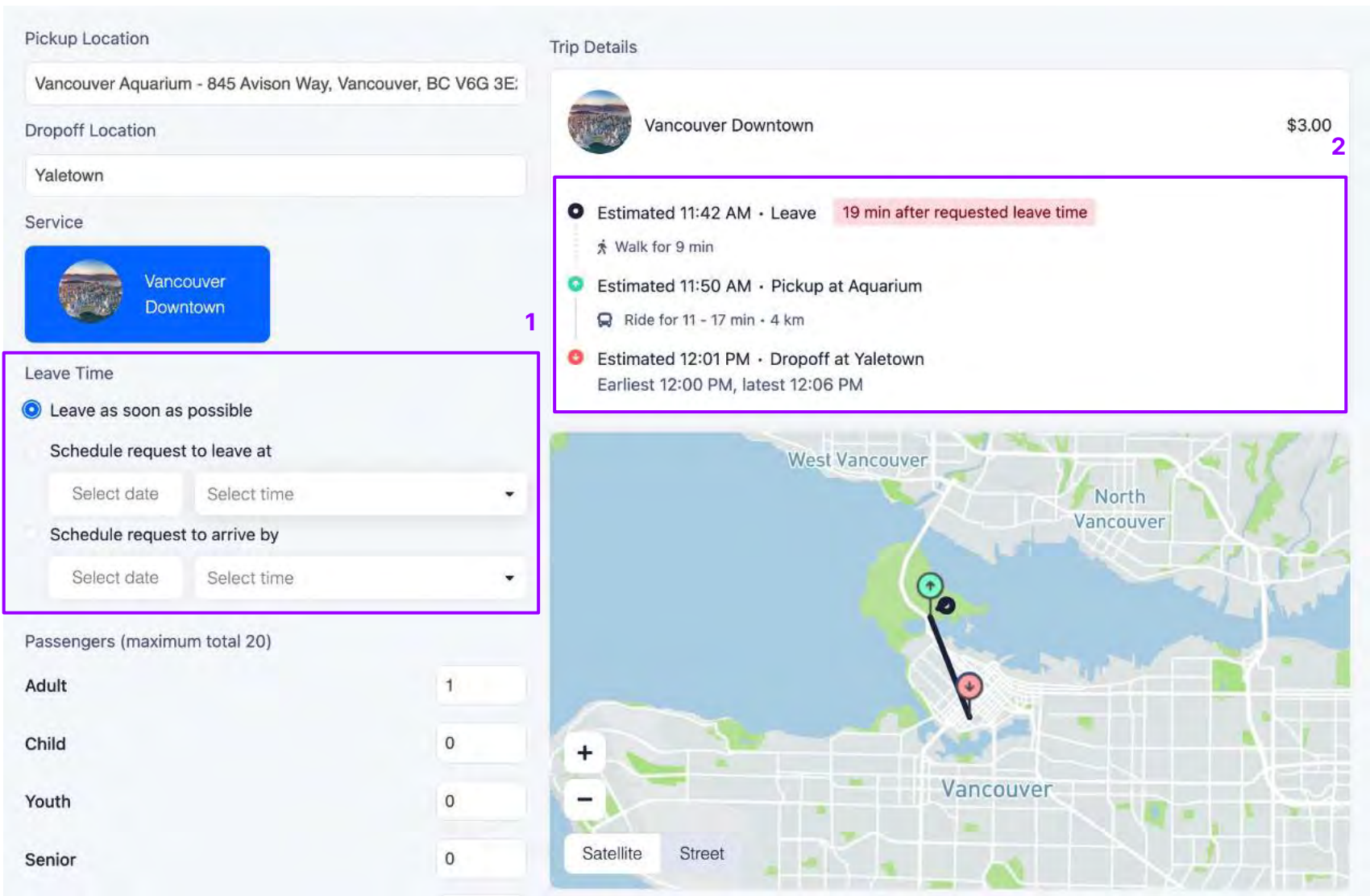
If both pickup and dropoff locations are within an active service zone, the applicable service(s) will show up. Select the service you would like to book the trip on by clicking on its name.



5 Set the Leave Time

The rider can either: **(a)** leave as soon as possible; **(b)** leave at a point in the future (if enabled); **(c)** (if enabled) set an arrive by a time;

Select the most relevant **leave time option[1]** for the rider. If there are available vehicles, **the request pickup and dropoff time estimates will appear [2]**.



9.1. How to Create Requests

6 Add Passenger(s) Information

Enter in the number of passengers along with any accessibility features required for the trip.

Pickup Location

Vancouver Aquarium - 845 Avison Way, Vancouver, BC V6G 3E

Dropoff Location

Yaletown

Service

Vancouver Downtown

Leave Time

Leave as soon as possible

Schedule request to leave at

Select date

Select time

Schedule request to arrive by

Select date

Select time

Passengers (maximum total 20)

Adult

1

Child

0

Youth

0

Senior

0

Trip Details

Vancouver Downtown

\$3.00

Estimated 11:42 AM • Leave

19 min after requested leave time

Walk for 9 min

Estimated 11:50 AM • Pickup at Aquarium

Ride for 11 - 17 min • 4 km

Estimated 12:01 PM • Dropoff at Yaletown

Earliest 12:00 PM, latest 12:06 PM

Map

West Vancouver

North Vancouver

Vancouver

Satellite

Street



Note: This will restrict the request to services and vehicles that can accommodate the passenger's accessibility needs.

7 Lock the Request to Duty (Optional)

If for any reason there is a necessity that the request is to be assigned to a specific driver, you may do so by using the **Lock Request to Duty** feature. **Mark the checkbox[1]** and **select the driver[2]**. **Add a note [3]** for internal records about why you are locking the request to the duty.

Duty

Lock this request to a duty

Manually Select Duty

Select

Demo Driver, Toyota Corolla

Demo Driver 2, Toyota Yaris

Let others at your organization know why you assigned the request to this duty.

9.1. How to Create Requests

8 Select Payment Options

If payments are enabled for the service, select a relevant payment method for the user. Depending on payment options available, this could be **Cash**, **Credit Card**, or a **Mobile Ticketing** option.

If cash is not an option, and payment is required, select **Add Credit Card** with Spare Pay IVR. After selecting this option, an automated system will call the rider and request for them to input a credit card.

Payment Method

Cash

+ Add Payment Method

9 Add Driver Notes

Finally, **add any notes** you'd like to be visible for the driver. Click **Create Request** to book the trip.

Notes

Write your notes here

Ticket Number

0

Ticket Type

Please select value

Trip details created a few seconds ago. Refresh trip details

Create Request



When the request is created, a new pickup and dropoff time might appear. Sometimes it may be different from the original estimate as Spare Engine constantly attempts to increase fleet efficiency and improve the key metrics.

Request

Julie Liu on Thu, Jan 12, 2023

Accepted

+ Add Request

... Actions

Pickup ETA	Fare	Discount	Rider	Vehicle
12:09 PM	\$3.00	-	Julie Liu	White Toyotal Corolla

Estimated 12:09 PM - Pickup at Aquarium

13 min after requested leave time

Earliest 12:05 PM, latest 12:14 PM

Ride for 11 - 17 min - 4 km

Estimated 12:20 PM - Dropoff at Yaletown

Earliest 12:15 PM, latest 12:30 PM

Map of Vancouver showing pickup and dropoff locations

9.2. Request Status and Troubleshooting

Check the Request Status

Check the request status either from the **Requests tab** or from the **Request Information page**.

Status Changes	
STATUS	TIME
Processing	Thu, Jan 12, 2023 11:42 AM
Accepted	Thu, Jan 12, 2023 11:42 AM



What statuses can a trip request have?

Processing: The matching process is updating the request based on the latest information regarding driver availability.

No Drivers Available: The matching process did not find any drivers for the passenger to match with.

Accepted: The request has been accepted into a driver duty.

Driver Arriving: Driver is within a certain distance/time to the passenger pickup location. Note: that this status is only used for on-demand services.

Trip in Progress: Trip is in progress.

Cancelled: The request has been cancelled. To find more information about the specific cancellation reason, navigate to the detailed information regarding the specific request.

Trip Completed: The trip/request was completed by a driver.

Cannot Create a Request?

If you go through the enlisted steps and cannot get a trip estimate, there are a few possible reasons why.

If no service appears after you enter the pickup and dropoff addresses, the following are potential reasons why:

- 1. One or both of the addresses falls outside of the service zones of your organization’s services
- 2. The service you are trying to book for has been disabled

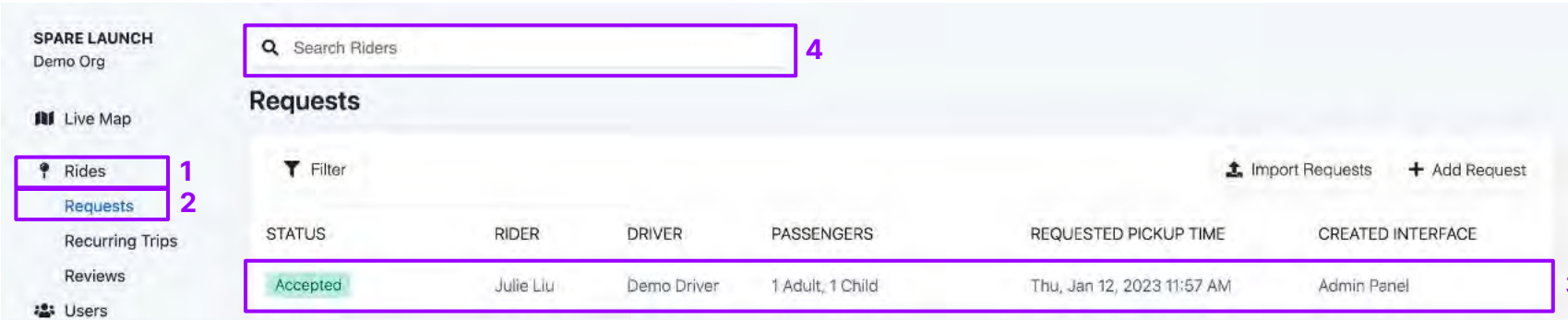
If after having entered the pickup and dropoff addresses, clicking on the respective service, and entering a desired leave time, **no trips can be found**, the following are potential reasons why:

- 1. The estimated pickup and/or dropoff time falls outside of the service’s operating hours
- 2. There are no duties scheduled for this service during the estimated pickup and/or dropoff time
- 3. An active vehicle has gone offline due to not updating its location and so has become unmatchable. Check the Live Map to confirm by clicking on the vehicles within the zone to check the status (red color indicates the vehicles is potentially unmatchable)
- 4. The number of passengers and/or accessibility features cannot be accommodated (either at this time due to other trips or generally by the service)

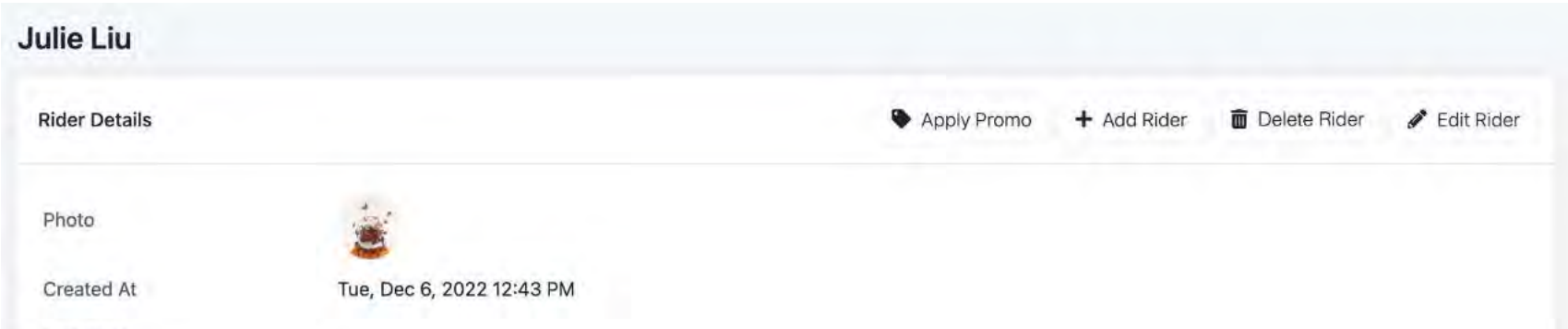
9.3. How to Edit Requests

1 Select the Request

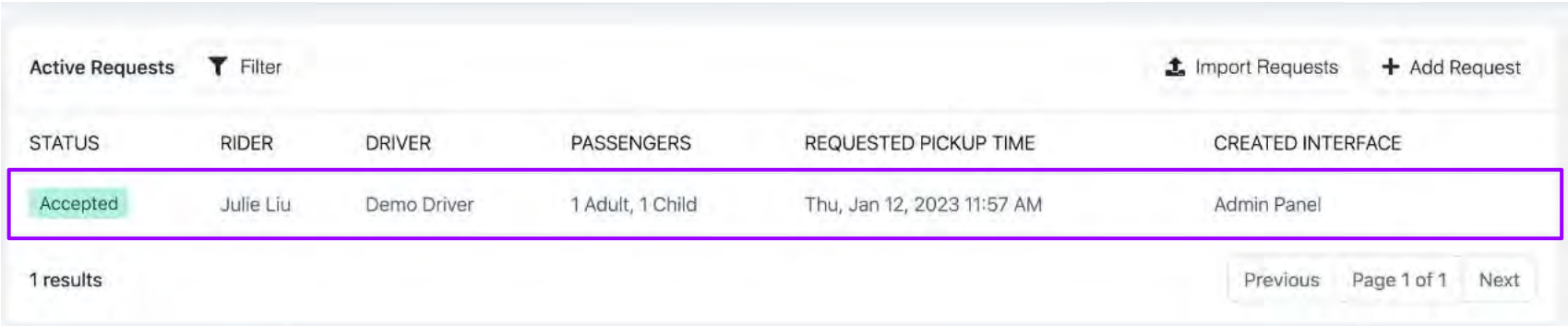
If you need to change an existing request, first, locate it in the Requests list. To do so, go to the **Rides tab**[1] and select **Requests**[2]. Click on the **request record**[3] you'd like to change.



You can also search the request by rider. Type the rider's name in the **search bar**[4] and select the rider card. Once in the **rider profile**, scroll down to their **requests history**. **Select the request** you'd like to change.

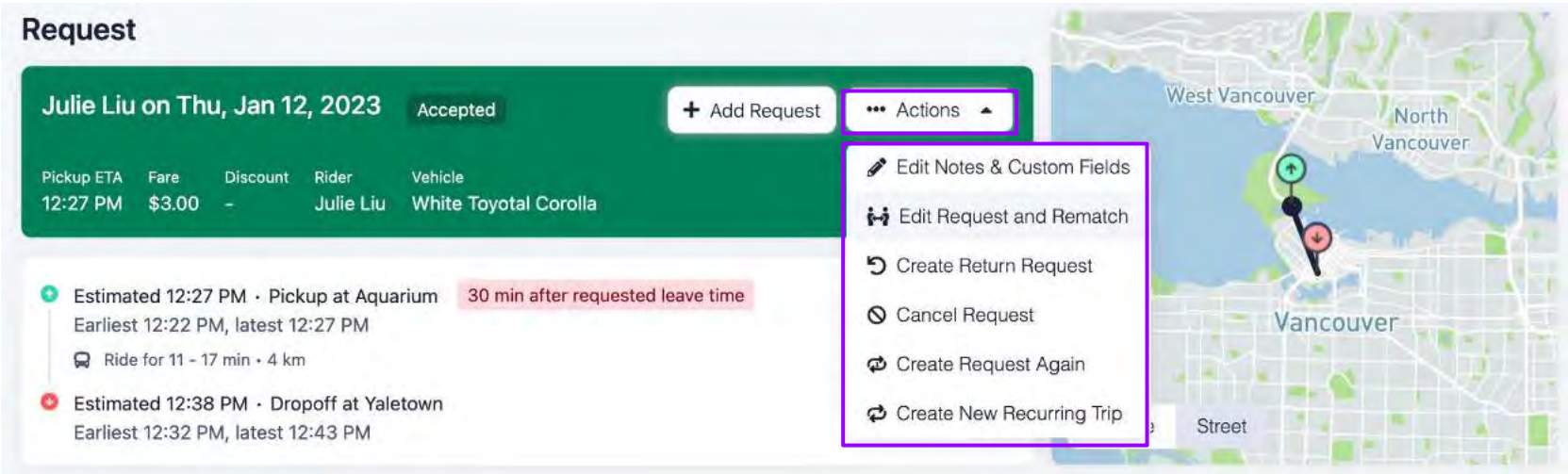


Scroll Down ↓



2 Edit, Cancel, or Copy the Request

Once on the Request Information page, click **Actions** and **select one of the options** from the drop-down menu. **Save** the changes to apply them.



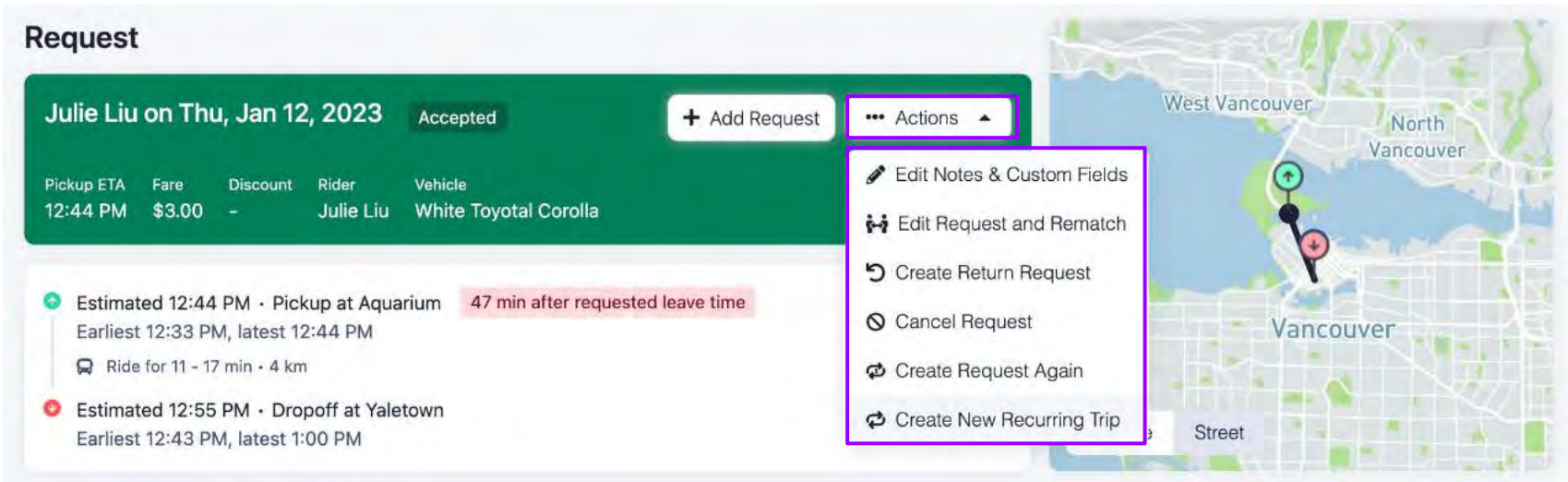
9.4. How to Create Recurring Trip Requests

1 Locate the “BluePrint” Request

Find a trip to act as the "blueprint". You can either select an existing trip Request or create a new one.



The system will copy the specific rider, pickup and dropoff locations, notes, service, and any accessibility features.



2 Check Existing Details

Review all existing details that are populated to the New Recurring Trip Form.



3 Set Recurring Parameters

In the form, set the days of the week and the time period. Add exceptions, if necessary. Click **Create New Recurring Trip** to apply changes.

Repeat on

M Tu W Th F Sa Su Select All

Begin on

2023-01-12

Repeat until

☒ Forever

Request Time

Leave at

11:57 AM

Departure time may occur between 11:57 AM and 12:57 PM.

Return Request Time

☒ No return request

Exceptions

DATE	OUTBOUND REQUEST	RETURN REQUEST
No exceptions have been added		

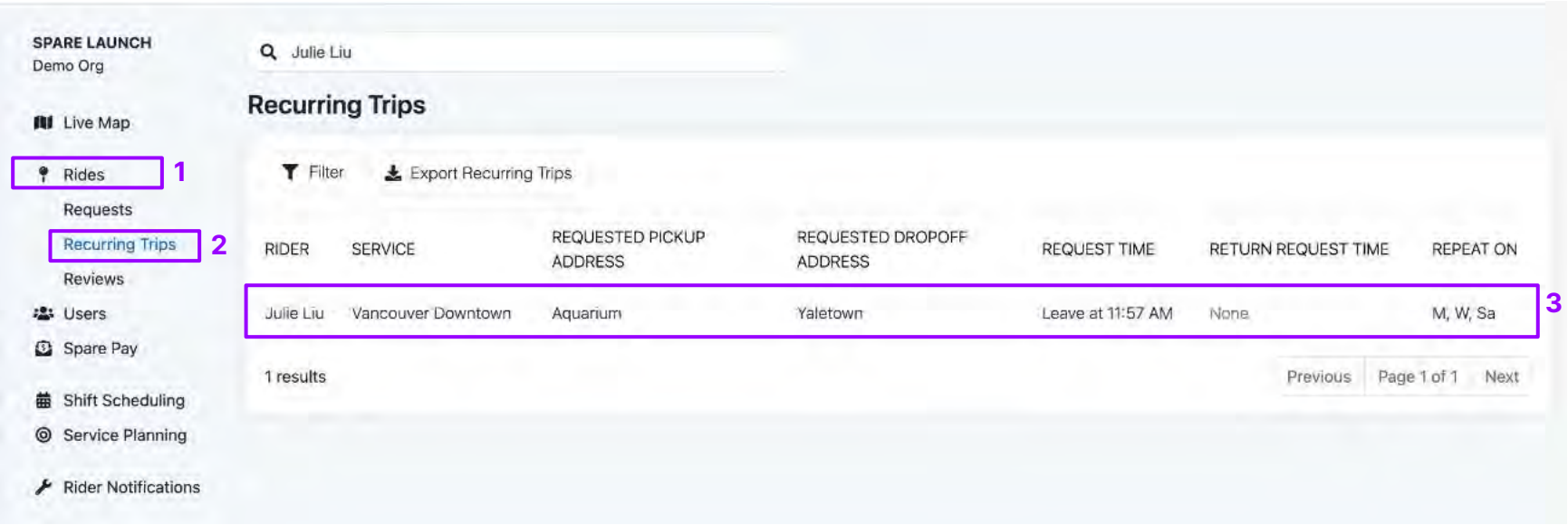
+ Add

Create New Recurring Trip

9.5. How to Edit Recurring Trip Requests

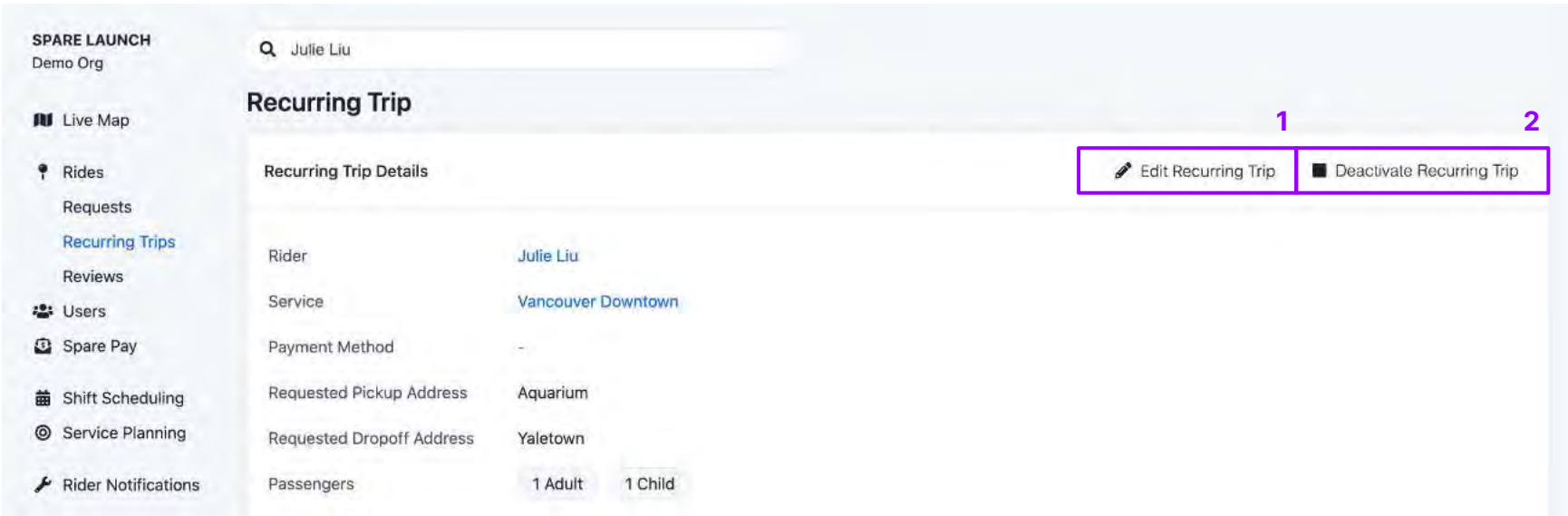
1 Open the Recurring Trip Information Page

If you need to change an existing recurring trip request, first, locate it in the Recurring Trips list. To do so, go to the **Rides tab**[1] and select **Recurring Trips**[2]. Click on the **request record**[3] you'd like to change.

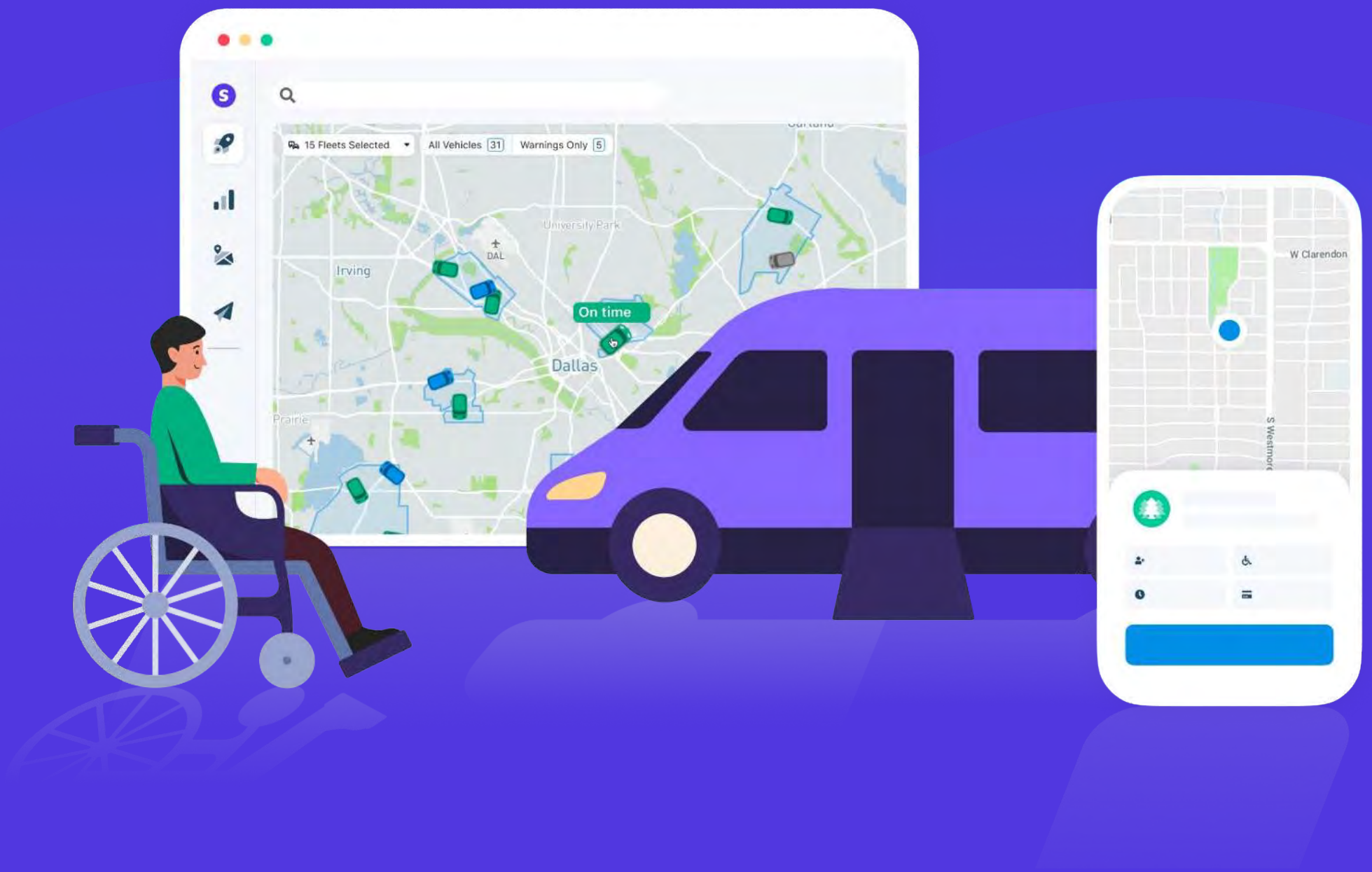


2 Edit or Deactivate the Trip

From the Recurring Trip Information Page, **Edit**[1] or **Deactivate**[2] the trip. Follow the platform instructions to apply the changes.



Changes will apply to any requests created by the recurring trip from the moment of applying the new parameters. Any requests that have already been created will remain unchanged.



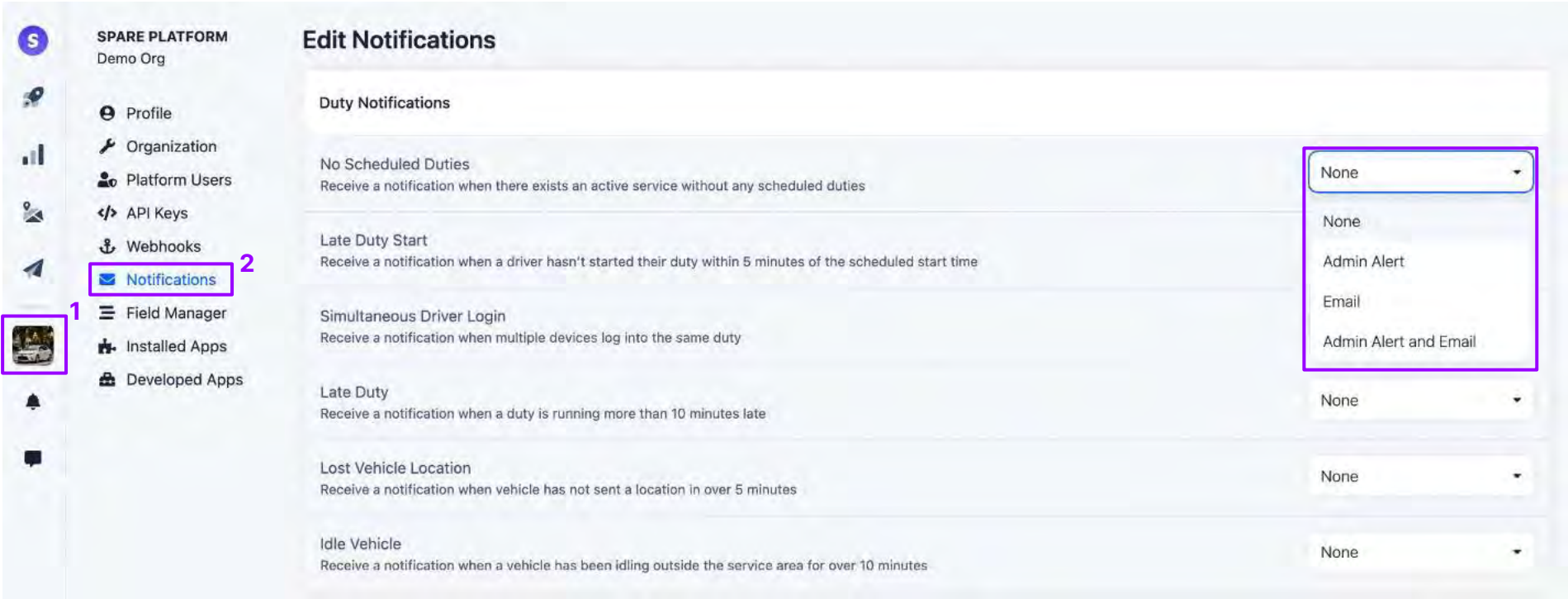
[10] Administrator Notifications

→ Set up Platform(Admin)
Notifications

10.1. How to Set Up Platform Notifications

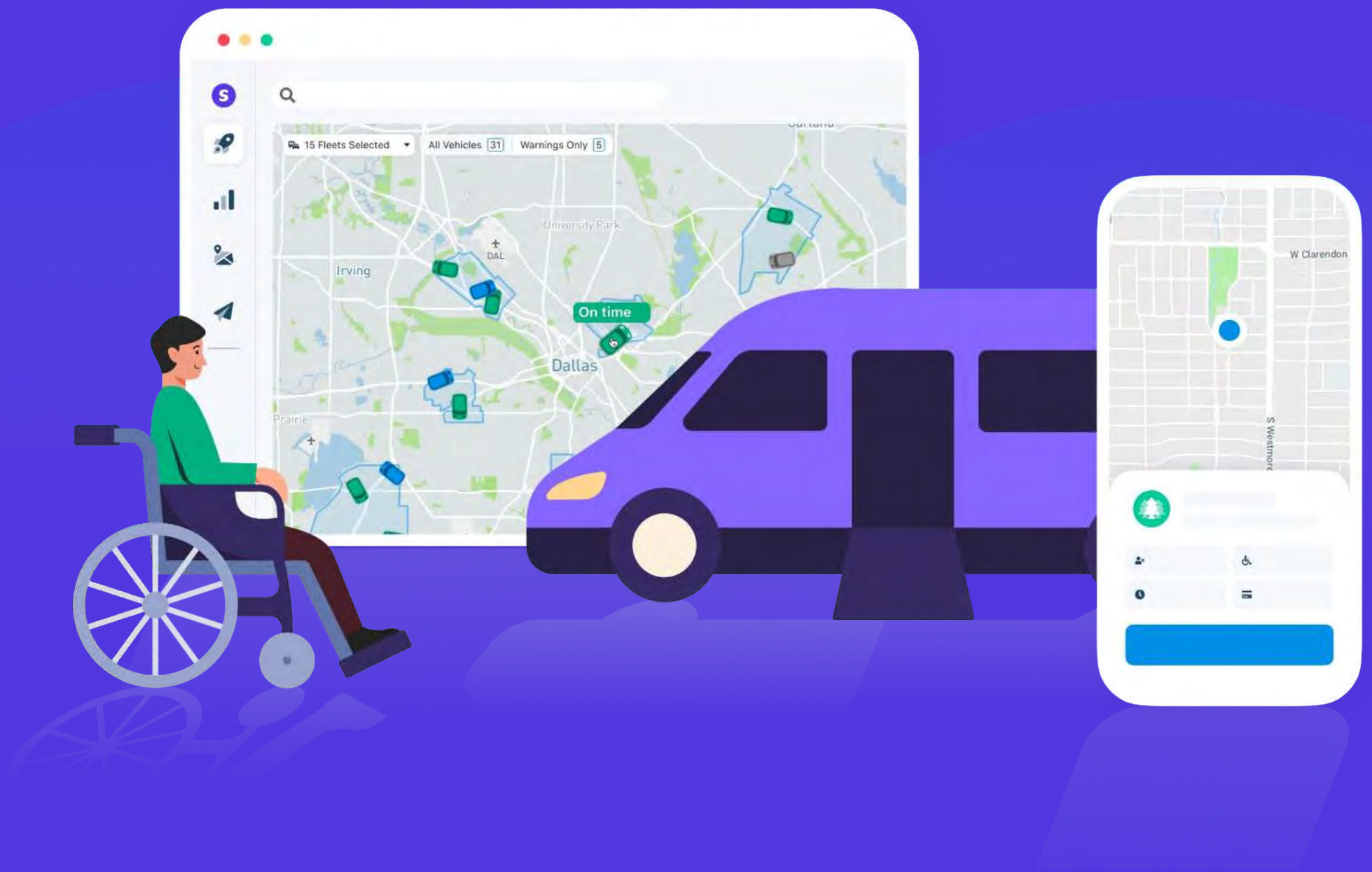
i Administrator notifications provide information to platform users about events within the platform. Unlike the notifications in the Launch menu, which notify riders, the notifications in the Administrator menu notify your specific user profile either through in platform alerts, via email, or both.

To access the administrator notifications, select your **Account icon[1]** on the left-hand side of the screen, navigate to the **Settings** section, and then select **Notifications[2]**.



There are currently 4 groups of notifications (see the table below. You can set up your preferred notification mode for each of them.

Notification Group	Notification Modes
Duty Notifications: No Scheduled Duties, Late Duty Start, Simultaneous Driver Login, Late Duty, Lost Vehicle Location, Idle Vehicle	☐ Admin Alert (in-platform) ☐ Email ☐ Admin Alert & Email ☐ None
Request Notifications: System at Capacity, No Drivers Available, No Show Cancellation, Recurring Trip Failure, Stranded Requests	☐ Admin Alert (in-platform) ☐ Email ☐ Admin Alert & Email ☐ None
Review Notifications: Negative Review Posted, Positive Review Posted with Comment	☐ Admin Alert (in-platform) ☐ Email ☐ Admin Alert & Email ☐ None
Engage Notifications (if applicable): Case Assignment	☐ Admin Alert (in-platform) ☐ Email ☐ Admin Alert & Email ☐ None



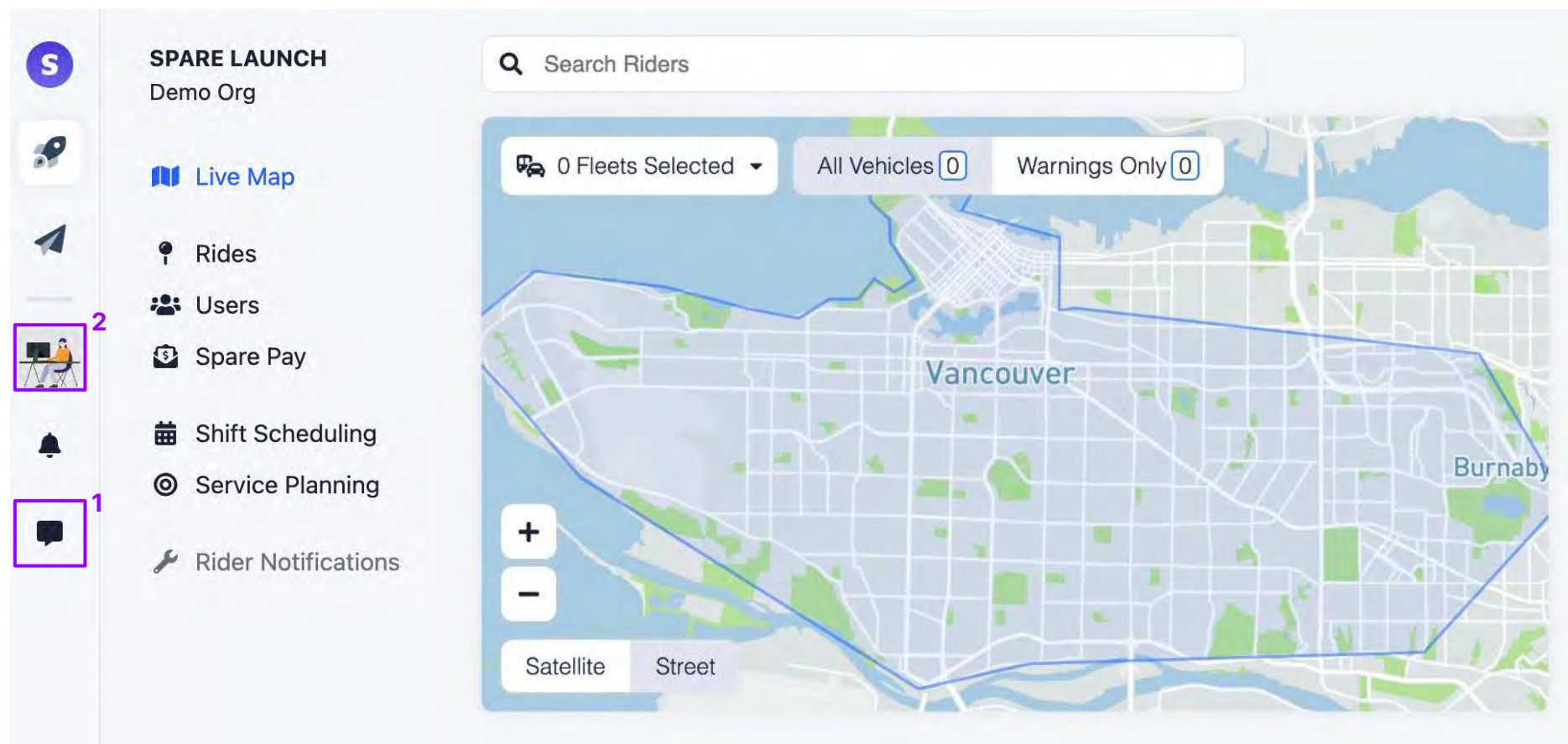
[11] Help & Troubleshooting

- Spare Help Centre
- Spare Tech Support

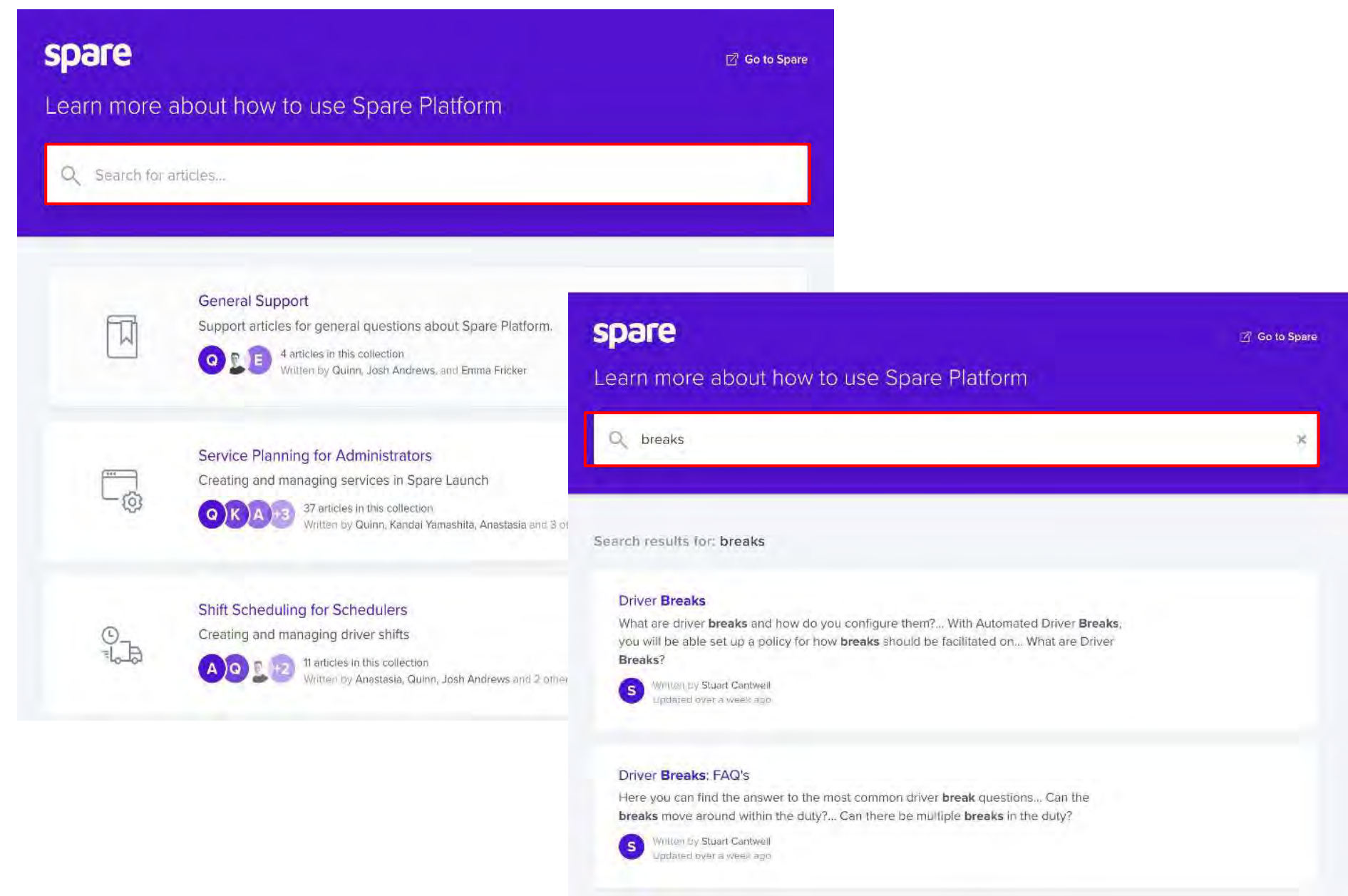
11.1. How to Reach out for Support

There are several ways you can **access help resources**:

-  By clicking on the **message icon[9]**: it will redirect you to **Spare's Tech Support** chat.
-  By going to your **Spare Account [2]** and selecting **Help**: it will redirect you to [Spare's Help Center](#).



If you are browsing Spare's Help Centre, feel free to type in the keywords in the search tab and click Enter to get all related results.



...area, ... Main St, Austin TX) is outside
...fill an eligible paratransit customer, CityPara will be unable to pick you up or
...your home address. In order to utilize CityPara, all pick up and drop off
...within the ADA service area.
What ADA paratransit service area?
...ansit service is offered within 3/4 mile of fixed-route bus service offered by
...same operating time frame of the fixed-route bus in that area. The
...red-route service area regularly, holding public input meetings prior to
...approving a change. Because the Paratransit service area mirrors fixed-
...CityPara customers will be contacted if a proposed change will affect
How approved service area change may or will affect my rides?
...ation on service changes at www.citymetro.org or through the GO-
...participate in public discussion about changes which may affect you
...CityPara makes a decision on a service change.

SPARE ENGAGE
CityMetro

Search Riders

Cases

All Cases

Paratransit Eligibility

Eligibility Appeal

Case Templates

Filter

All Cases

Assigned To You

Action Needed

Received	RIDER	CASE TEMPLATE	RECEIVED
Complete	Vicky Mondello	Paratransit Eligibility	May 4, 2022 1:03 PM
Interview Scheduled	Rick McCormick	Paratransit Eligibility	May 2, 2022 10:23 AM
Complete	Lois Lin	Eligibility Appeal	May 9, 2022 9:37 AM
Received	Chris Hornbury	Paratransit Eligibility	May 7, 2022 11:03 PM
Received	Ben Washington	Paratransit Eligibility	May 6, 2022 6:39 AM
Interview Scheduled	Yvonne Kim	Paratransit Eligibility	May 8, 2022 7:23 AM
Interview Scheduled	Jane McCarthy	Paratransit Eligibility	May 3, 2022 10:03 AM
Interview Scheduled	Hope Scott	Eligibility Appeal	May 4, 2022 11:03 PM
Complete	Jim Williamson	Paratransit Eligibility	May 5, 2022 8:21 AM
	Ginny Schultz	Travel Training	May 5, 2022 10:03 PM

3409 results

Add Form Field

Type

Aa Text

Number

Toggle

Single Choice

Multi-select

Date

Date & Time

Address

Drawing

Close

API Name for this field when accessing this object
Once created, this cannot be changed.

Engage Walkthrough

A guide to managing paratransit eligibility with Spare Engage.

Eligibility Application
by CityMetro

CityMetro

Do you use a mobility aid when you travel?

Yes

Type of mobility device used?

☐ Walker ☒ Wheelchair ☐ Cane

☐ Scooter ☐ Service Animal

spare

Preparing & Accepting Applications

Create and share digital application forms that your riders can access, submit, and update from any device. Or, you can also download and print your forms to allow submissions by PDF or on paper.

Creating forms

Applications can have multiple forms, such as an Eligibility Application for riders to fill out, a Medical History form for doctors to fill out, and any others your agency requires as part of the submission process. You can also create forms for internal approval processes that only Spare Engage users can see. On each form, you can control whether specific fields are hidden, visible, or editable by outside users like riders.

The screenshot displays the 'SPARE ENGAGE CapMetro' interface. On the left is a sidebar with navigation icons and labels: 'Cases' (with sub-items 'All Cases', 'Paratransit Eligibility', and 'Eligibility Appeal'), and 'Case Templates'. The main content area is titled 'Eligibility Application Form Template' and includes a 'Search Riders' bar. Below the title are three action buttons: 'Print Blank Form', 'Share New Case Link', and 'Edit Form Template Details'. A 'Form Template Details' section contains the following information:

Name	Eligibility Application
Description	Riders should begin their application for paratransit eligibility with this form.
Key	eligApp
Included Rider Profile Fields	First Name, Last Name, Phone Number, Email Address, Date of Birth, Agency ID, Preferred Language These fields from the Rider profile will be included at the beginning of the form. Rider Profile fields can be controlled from the Field Manager.

Below this is the 'Form Fields' section, which has tabs for 'Active' and 'Archived'. It lists five active form fields, each with an equals sign icon, a question, a status label, and 'Archive' and 'Edit' buttons:

Field	Status	Actions
☒ Do you use a mobility aid when you travel?	Editable and visible to riders	Archive Edit
☐ Type of mobility device used?	Editable and visible to riders	Archive Edit
☐ How do you plan to use this service?	Editable and visible to riders	Archive Edit
☒ Do you have a program qualifying disability?	Editable and visible to riders	Archive Edit
☒ Please select your city of residence.	Editable and visible to riders	Archive Edit

Digital applications

To allow riders to apply online for specialized transit, you can include a link to Spare Engage on your agency website. Once a rider clicks the link, Engage securely collects riders' names, phone numbers, and completed forms. When a rider submits their responses, a new case is automatically created in Engage.

Or, you can download a blank version of any form as a PDF that you can print or post online for riders to fill out.

Eligibility Application
by CapMetro

Do you use a mobility aid when you travel?

Yes

Type of mobility device used?

☐ Walker ☒ Wheelchair ☐ Cane ☐ Scooter ☐ Service Animal

How do you plan to use the service?

☒ Shopping ☒ Medical ☒ Social ☐ Work

☒ Connect to fixed route bus ☐ Other

Do you have a program qualifying disability?

Yes

ID Document
May be a state-issued ID, driver's license, lease, or current utility bill. ID may also serve as proof of age.

Choose Files
or drag and drop file here
File must be either jpg, jpeg, or pdf, under 5 MB.

front.jpg 1.2 MB

back.jpg 1.3 MB

Submit

Back

SPARE ENGAGE
Specialized Transit

Search Riders

Edit Eligibility Application Form

Form Responses

Do you use a mobility aid when you travel?

Yes

Type of mobility device used?

☒ Walker ☒ Wheelchair ☐ Scooter ☐ Cane ☐ Service Animal

☐ Not Applicable

How do you plan to use this service?

☒ Shopping ☒ Medical ☒ Social ☐ Work

☒ Connect to fixed route bus ☐ Other

Do you have a program qualifying disability?

Yes

ID Document

Choose Files
or drag and drop file here
File must be either jpg, jpeg, or pdf, under 5 MB.

id-front.jpg 1.5 MB

id-back.jpg 1.2 MB

May be a state-issued ID, driver's license, lease, or current utility bill. ID may also serve as proof of age.

Supporting Eligibility Document

Choose Files

Paper applications

For applications received by mail, agency staff can easily and quickly enter the information and create a digital case within Engage.

Evaluating Applications

Agency staff can track case progress and collaborate across teams to make a timely determination on an application.

Viewing cases

New cases and existing cases can be viewed in the All Cases section of Engage. You can filter the list by status, assigned users, time until limit, and more.

SPARE ENGAGE
Squirrel Transit

Search Riders

All Cases

Filter

+ Add Case

	RIDER	CASE TEMPLATE	RECEIVED	TIME UNTIL LIMIT	ASSIGNED TO
Received	Vicky Mondello	Paratransit Eligibility	May 4, 2022 1:03 PM	7 days, stopped	CM Casey Mendoza
Complete	Rick McCormick	Paratransit Eligibility	May 2, 2022 10:23 AM	1 day over, counting	GL Guy Lafontaine
Interview Scheduled	Lois Lin	Eligibility Appeal	May 9, 2022 9:37 AM	-	-
Complete	Chris Hornbury	Paratransit Eligibility	May 7, 2022 11:03 PM	20 days, counting	CM Casey Mendoza
Received	Ben Washington	Paratransit Eligibility	May 6, 2022 6:39 AM	11 days, stopped	CM Casey Mendoza
Received	Yvonne Kim	Paratransit Eligibility	May 8, 2022 7:23 AM	19 days, counting	GL Guy Lafontaine
Interview Scheduled	Jane McCarthy	Paratransit Eligibility	May 3, 2022 10:03 AM	3 days, stopped	-
Interview Scheduled	Hope Scott	Eligibility Appeal	May 4, 2022 11:03 PM	-	-
Interview Scheduled	Jim Williamson	Paratransit Eligibility	May 5, 2022 8:21 AM	17 days, stopped	CD Cheyenne D
Complete	Ginny Schultz	Travel Training	May 5, 2022 10:03 PM	-	-

3409 results

Previous Page 1 of 1 Next

Collaborating on cases

Once a case has been created, multiple people may work on the case as it goes through your internal processes. As work gets done, Engage users can change the case's status to reflect its current stage of the process, assign it to the applicable coworker, and leave notes on the case for others.

The screenshot shows the 'George Prayumna Case' interface. At the top, there is a search bar labeled 'Search Riders'. Below the title, there are three tabs: 'Case Details' (selected), 'To Do', and 'Assign To'. An 'Edit Case' button is also present. The 'Case Details' tab contains a table with the following information:

Rider	George Prayumna
Case Template	Paratransit Eligibility
Received	Nov 3, 2022 12:16 PM
Timer	Stopped. 4 days counted, 17 days until limit.
Notes	Nov 4: Talked to George on the phone - he needs an appt soon because he will be traveling starting Nov 25 Nov 6: Attempted to contact doctor for more info about seizures Nov 7: Heard back from doctor, added seizure info to Med Followup form Nov 8: Interview scheduled for Nov 14, 3pm

Following up on cases

Should more information be needed from an applicant to process their application, you can send a link to a specific form for them to complete or update.

The 'Share Form Link' modal is displayed. It has a title bar with 'Share Form Link' and a 'Close' button. The main content area contains the following text:

This link allows George Prayumna to log in online and submit responses to this form.

Link

<https://forms.sparelabs.com/forms/d65-470/eligibility/case/8o7iub>

At the bottom, there are two buttons: 'Copy Link' and 'Open External Form'.

Tracking cases

Time limits can be set for case determination. ADA regulations mandate a 21-day turnaround from application to decision, but you can set the limit to any length you like.

If work starts and stops, you can log the dates on a case. Engage will automatically track how many days a case has been in progress for. All changes to a case are tracked in the Activity Log.

Timer

☒ Enabled

Allows adding Start and Stop dates to each case, and automatically keeps track of how many calendar days have passed.

Time Limit

21

days

Timer

Stopped. 4 days counted, 17 days until limit.

Timer Events

EVENT	DATE	
Start	2022-11-22	
Stop	2022-11-25	
Start	2022-11-27	Add

Add events to record when the timer started or stopped counting.

Rider Communication

Keep riders informed on their application status from submission to decision to renewal.

Creating letter templates

Agencies can create multiple letter templates that use variables like the current date and the rider's name and address. You can include images and a range of formatting options, and see a realistic preview of how the letter will look to your riders.

SPARE ENGAGE
Squirrel Transit

Search Riders

Create Letter Template

Letter Template Details

Name

Out of ADA Insert (English)

Content

Write here, adding formatting using [Markdown syntax](#) and variables using [Spare variable syntax](#). For more control over the letter's appearance, you can add [HTML with inline styles](#).

B I H1 H2 H3 **Bulleted List** **Numbered List** **Link** **Image** Add Variable

<p style="font-size: 12px; margin-bottom: 0px;">Capital Metropolitan Transportation Authority</p>

<p style="font-size: 12px ; margin-top: 0px;">2910 East Fifth Street, Austin, Texas 78702 | TEL 512.389.7400 | FAX 512.389.6596 | www.capmetro.org</p>

{{date.current}}

{{(rider.firstname)}} {{(rider.lastname)}}
{{(rider.address)}}

Re: The ¼ Mile ADA Service Area

Dear {{(rider.firstname)}} {{(rider.lastname)}},

This notice is to advise you that your ****home address {{{(rider.address)}}} is outside of the MetroAccess ¼ mile ADA paratransit service area.****

Preview

When a letter is generated for a specific case, variables will be replaced with values belonging to the rider of case.

Previous Page 1 of 2 Next

CapMetro
Capital Metropolitan Transportation Authority
2919 East Fifth Street, Austin, Texas 78702 | TEL 512.389.7400 | FAX 512.389.6596 | www.capmetro.org

{{date.current}}

{{(rider.firstname)}} {{(rider.lastname)}}
{{(rider.address)}}

Re: The ¼ Mile ADA Service Area

Dear {{(rider.firstname)}} {{(rider.lastname)}},

This notice is to advise you that your **home address {{{(rider.address)}}} is outside of the MetroAccess ¼ mile ADA paratransit service area.**

What does this mean?

While you are still an eligible paratransit customer, MetroAccess will be unable to pick you up or drop you off at your home address. In order to utilize MetroAccess, all pick up and drop off locations must be within the ADA service area.

What is the ¼ mile ADA paratransit service area?

MetroAccess ADA paratransit service is offered within ¼ mile of fixed-route bus service offered by Capital Metro during the same operating time frame of the fixed-route bus in that area. The paratransit service area is not based on feeder, flex, limited, or express bus or rail service.

Sending letters

When it's time to formally notify a rider of your decision, you can generate a letter for them. Their name and other details will be automatically filled in, and you can preview the letter before downloading it as a PDF that you can print out or send digitally. Engage keeps a record of who generated the letter and when, and stores a copy of the file.



Capital Metropolitan Transportation Authority

2910 East Fifth Street, Austin, Texas 78702 | TEL 512.389.7400 | FAX 512.389.6596 | www.capmetro.org

March 19, 2023

Jane Doe
1234 Main St, Austin TX
Re: The ¾ Mile ADA Service Area

Dear Jane Doe,

Thank you for participating in your recent MetroAccess Eligibility Review and welcome to MetroAccess! The information from your application, professional verification, eligibility review, and functional transit assessment (where applicable) was used to determine your individualized eligibility for MetroAccess services. **You have qualified for unconditional use of MetroAccess.**

Your MetroAccess customer information:

- MetroAccess ID Number: 123456
- Eligibility Expiration Date: 08/04/2025
- Mobility aids on file: Walker
- Personal Care Attendant (PCA) on file: None

Your designated level of service is:

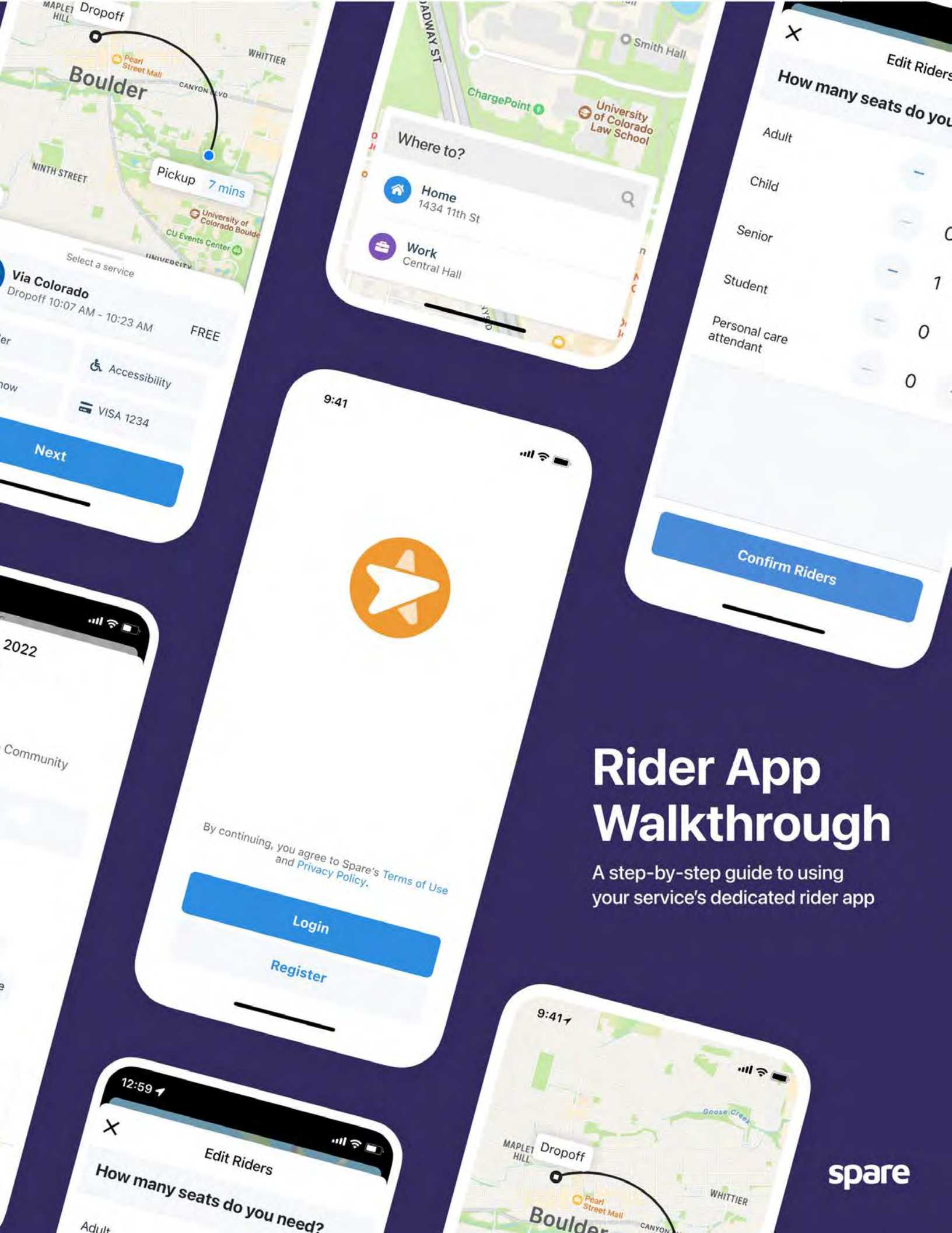


Door To Door Service

At your pickup location, the vehicle operator will assist you from the first doorway to the vehicle and help you board the vehicle.

At your drop off location, the vehicle operator will help you exit the vehicle and assist you to the first door of your drop off location.

Based on all the information gathered, it has been determined that you currently are not able to independently use the regular Capital Metro city bus under reasonable circumstances. Your



Rider App Walkthrough

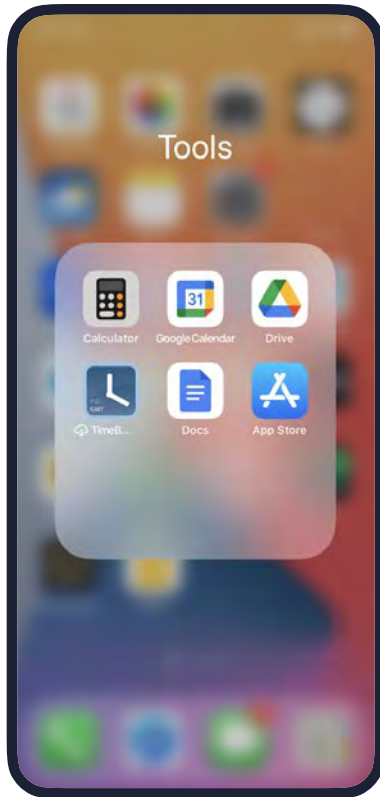
A step-by-step guide to using your service's dedicated rider app

spare

Table of Contents

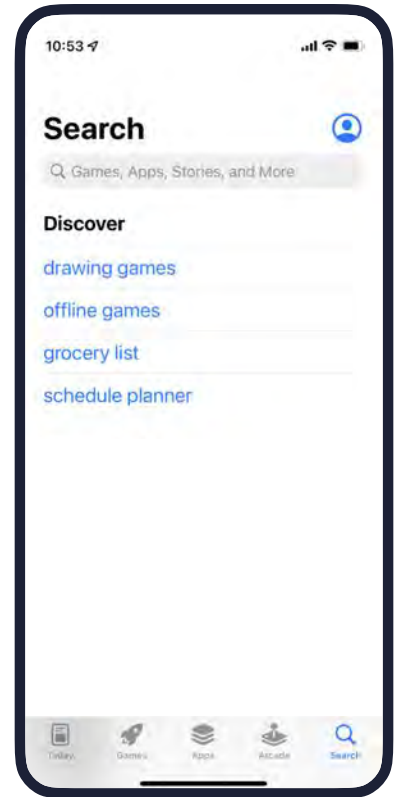
Downloading the App	1
Pickup and Drop off Locations	3
Seating and Accessibility Accommodations	4
Leave Time and Scheduled Trips	5
Driver Arriving and Drop Off	6

How to download the Spare Rider App from the App Store (iOS Users)



Locate the App Store

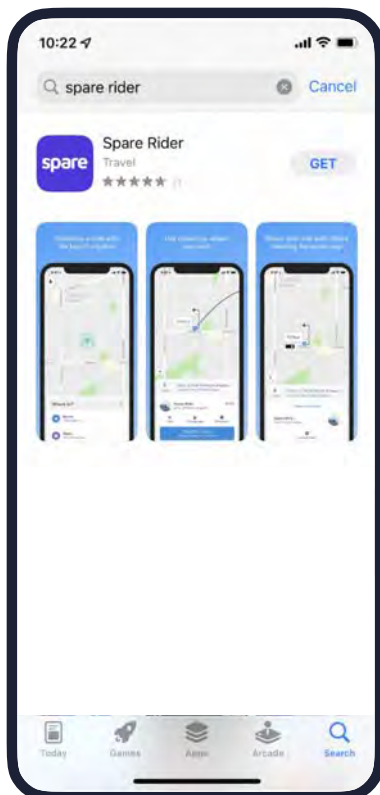
Locate and tap the App Store Icon on your iOS Device



Search for the app

Tap on the search bar at the top of the screen.

Then type in a search for the 'Spare Rider app'



Select the app

Tap on the Spare icon which will appear in your search results. This will then take you to a page to begin downloading the app.

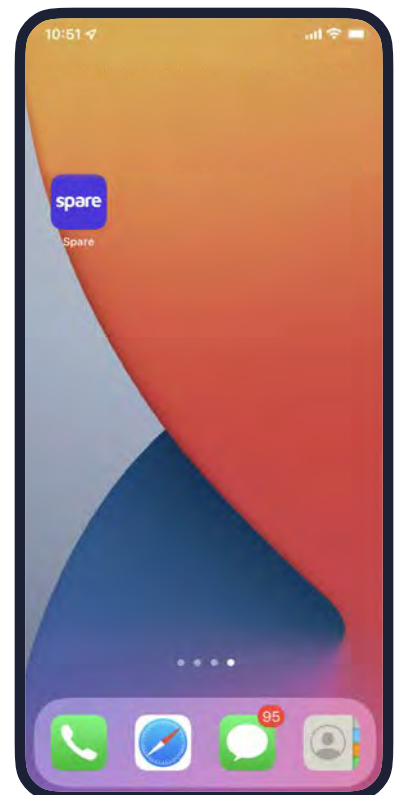


Download the app

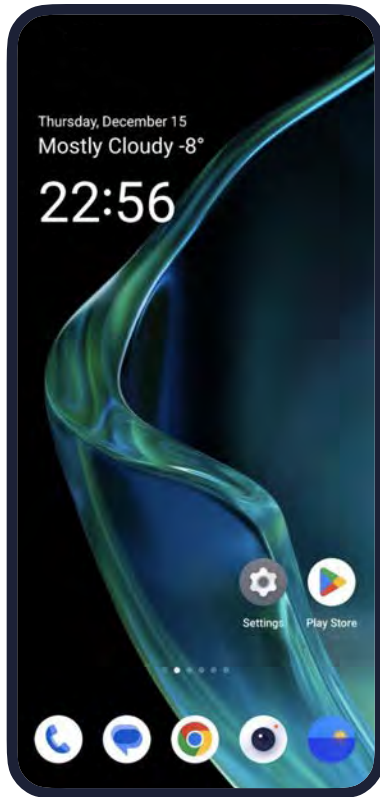
Download the app to your device by clicking the "Get" button.

You may need to type in your Apple ID login and password to start downloading.

Once the app is installed, you will be able to use the app by tapping on the apps icon which is now installed on your devices main screen.

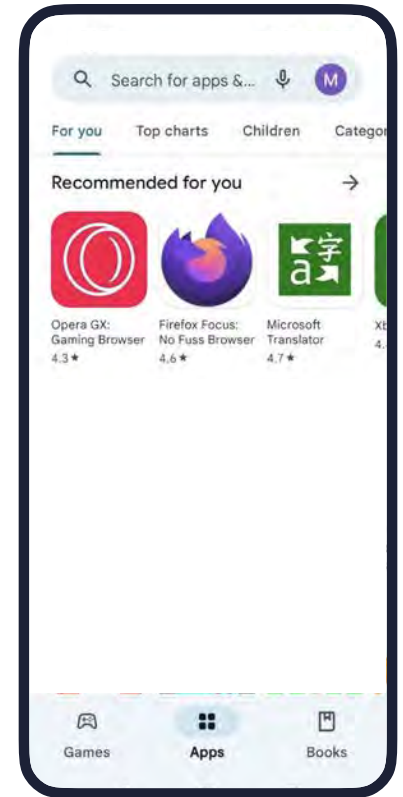


How to download the Spare Rider App from Google Play Store (Android Users)



Locate the Play Store

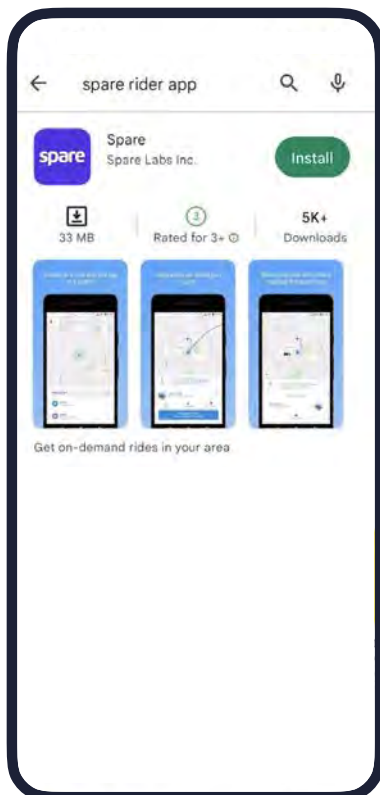
Locate and tap the Play Store Icon on your Android Device



Search for the app

Tap on the search bar at the top of the screen.

Then type in a search for the 'Spare Rider app'



Select the app

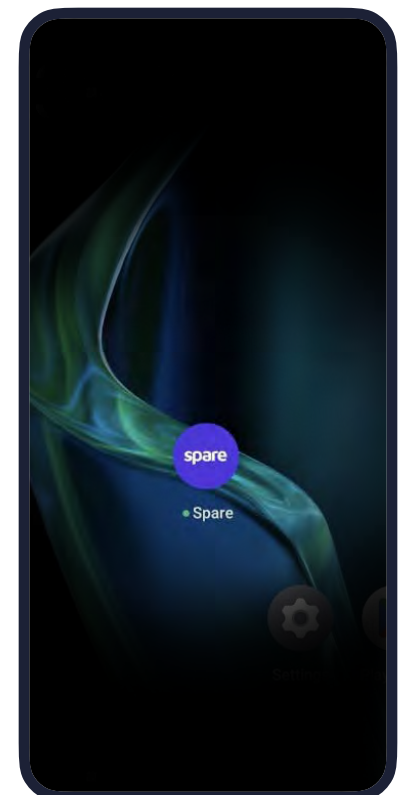
Tap on the Spare icon which will appear in your search results. This will then take you to a page to begin downloading the app.

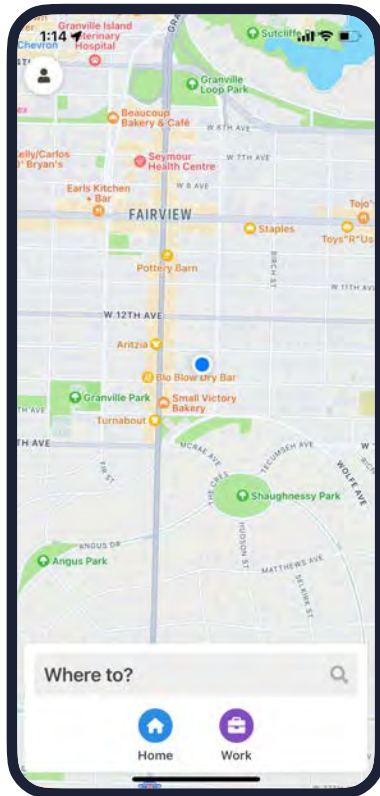


Download the app

Download the app to your device by clicking the Green **Install** button.

Once the app is installed, you will be able to use the app by tapping on the apps icon which is now installed on your devices main screen.





Homescreen

Riders start booking a trip by tapping "Where to?"

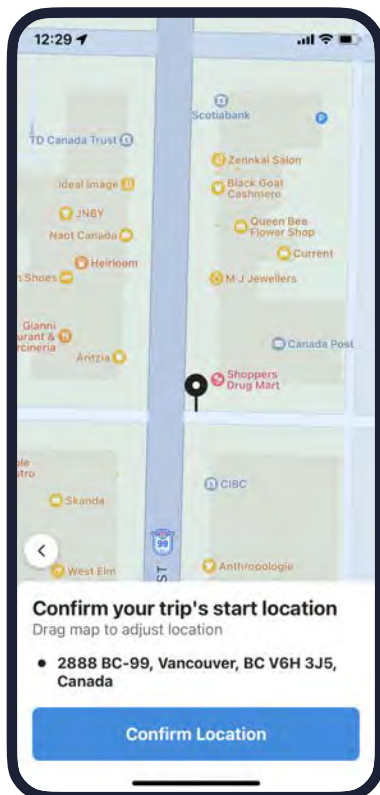
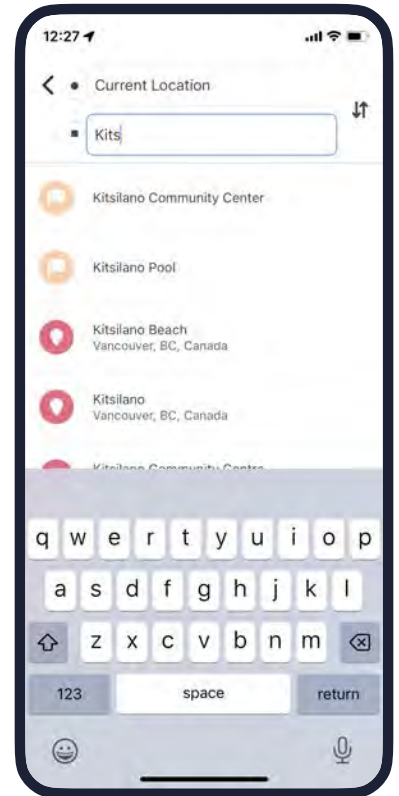
Riders can also set favorite locations that let them start a booking from the homescreen with one tap.



Set locations

Enter the desired pickup & dropoff locations.

Select a stop (orange flag) or point of interest (red pin) from the list.



Confirm pickup location

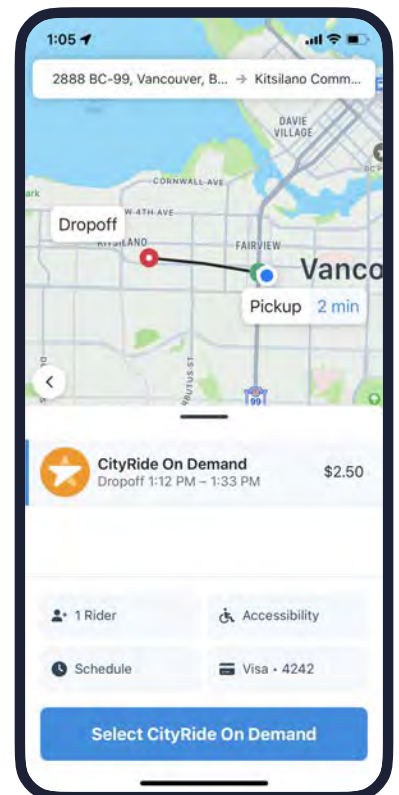
Confirm the trip's start location by moving the pin to the desired pickup spot on the map.

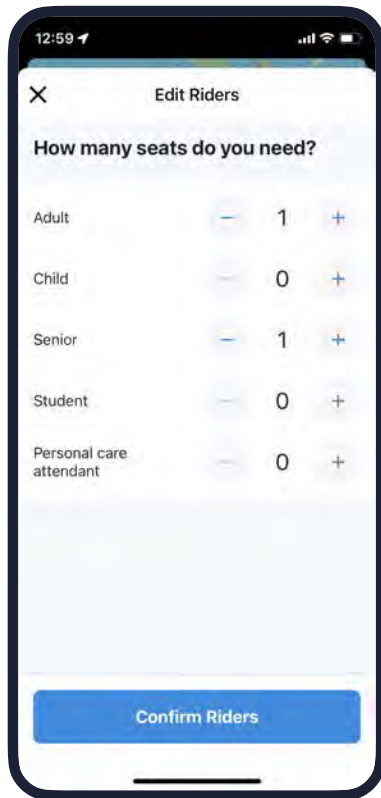


See ride options

Riders can see the fare and estimated dropoff time of any available on-demand services.

If multimodal is enabled, fixed-route transit options will also be listed here.





Add riders

Reserve extra seats for everyone who's traveling.

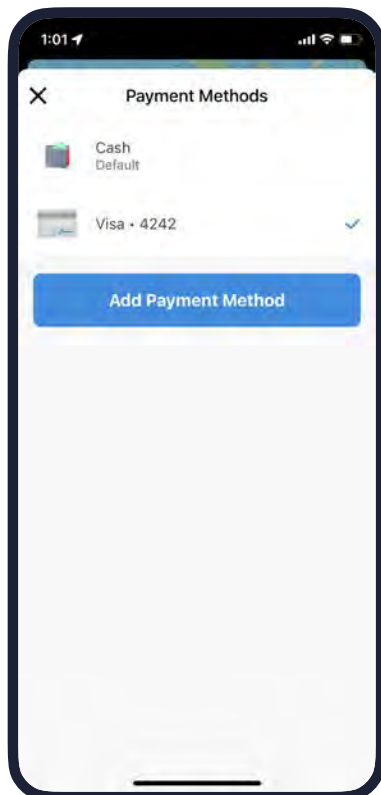
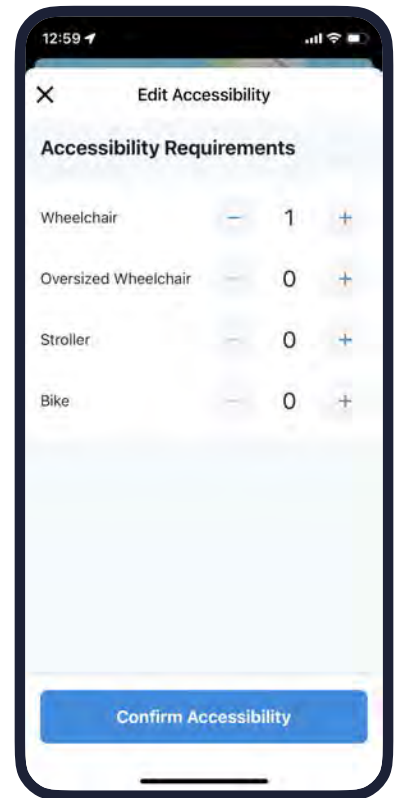
You can choose which rider types you want to support on your services. Fares can be set independently for each rider type.



Add accessibility features

Add any accessibility requirements.

Riders will only be matched to vehicles that can support their needs.



Choose payment

Choose a payment method such as credit card, debit card, transit pass, or cash.

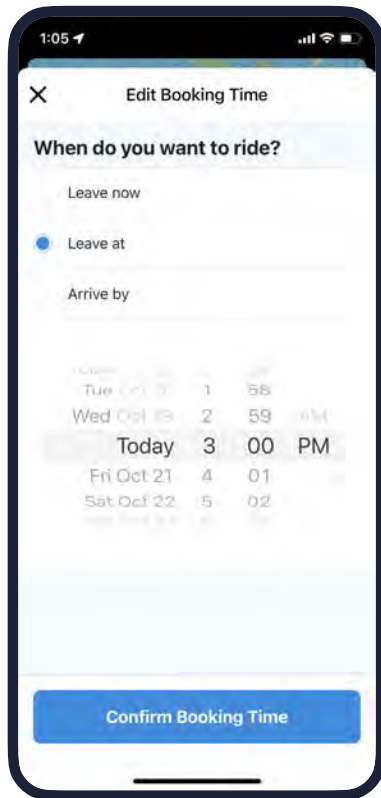
Credit and debit payments are processed instantly and securely.



Fare Passes can be configured as stored value or time-based passes and sold in-app.



Promos can be linked to transit agency promotions, special events, student or senior discounts, employer-subsidized commuter rides, and more.



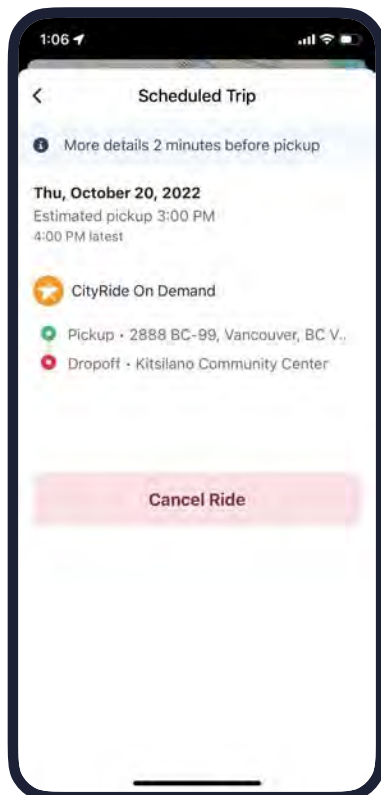
Schedule for later

If scheduling a trip for the future, riders can specify the time they'd like to leave at or arrive by.



View scheduled trips

Upcoming scheduled trips can be viewed from the menu.



Preview your trip

Details about the trip are added as the pickup time approaches.

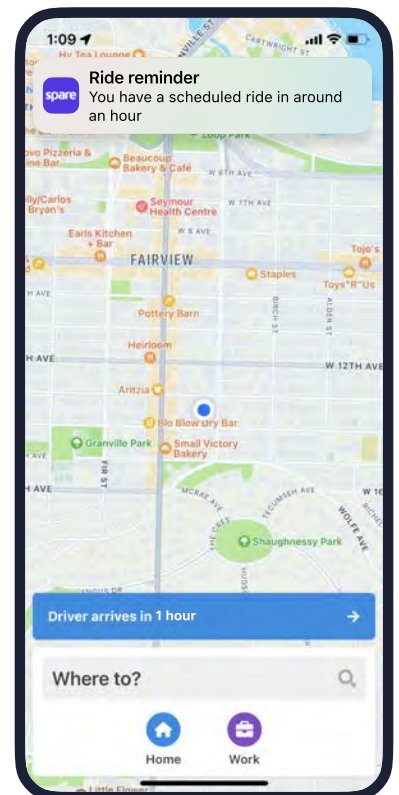
Riders can also cancel from here if they don't need the trip anymore.

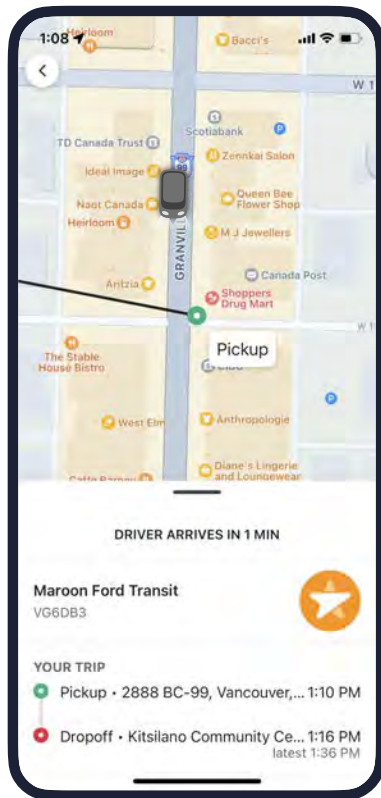


Get reminded

Before pickup time, riders receive reminder notifications.

A banner on the homescreen provides a shortcut to view the trip.

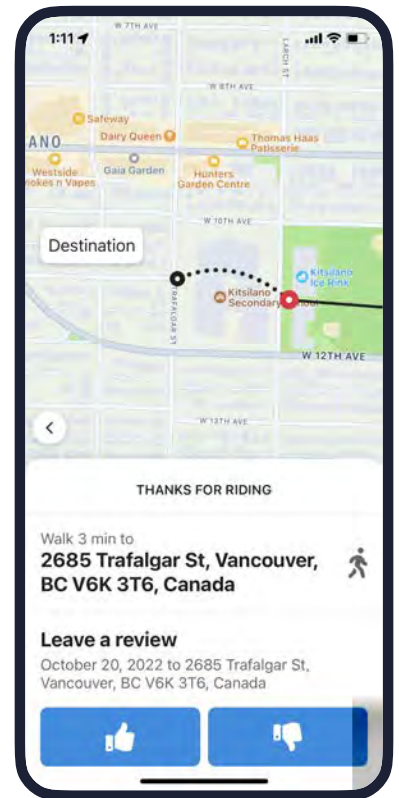




At pickup time

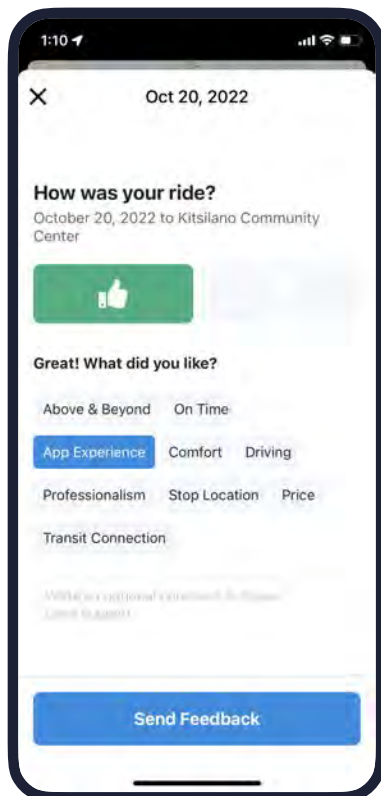
When it's pickup time, riders can see where the vehicle is, where & when they'll be picked up and dropped off, and which vehicle to look for.

In stop-based services, riders will see walking directions to their stop.



After dropoff

After the ride, riders can see walking directions to their destination.



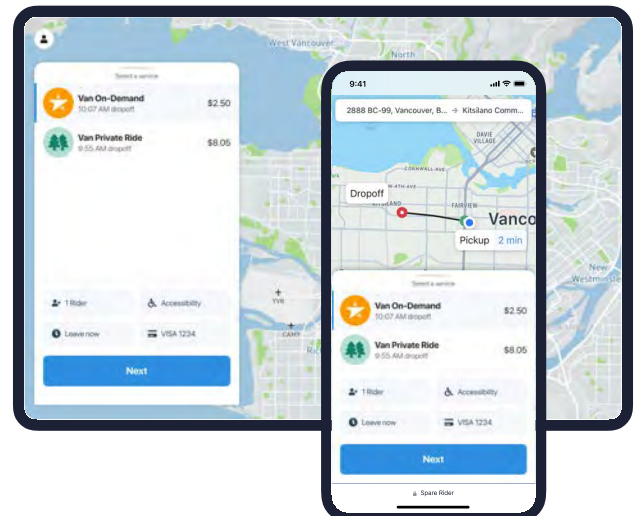
Review

Riders can leave a review to let you know what their ride was like.



Book on the web, too!

In addition to mobile apps for Android and iOS, Spare Rider is also available as a website on desktop and mobile.



Securing payments with Twilio programmable voice

TWILIO IS PCI DSS LEVEL 1 CERTIFIED

PCI STANDARDS OVERVIEW

- Build and Maintain Secure Network and Systems
- Maintain a Vulnerability Management Program
- Implement Strong Access Control Measures
- Regularly Monitor and Test Networks
- Maintain an Information Security Policy
- Protect Cardholder Data

Credit card fraud is the most common form of identity theft, with over 14.2 million accounts exposed and fraud losses totaling \$905 million in 2017, according to a report by the Federal Trade Commission (FTC)¹. At Twilio, we understand with stakes this high, mitigating the risk of a potential security breach is paramount.

Twilio's Payment Card Industry Data Security Standard Level 1 (PCI DSS) compliance and certification extensively expands the scope of how customers can accelerate their business by using our trusted cloud communications platform and APIs. Twilio customers can capitalize on our certification to provide solutions that will enable them to securely capture credit card data over the phone using [Twilio Programmable Voice](#). Whether you are already PCI compliant or building an application that requires PCI compliance, rely on Twilio to accept payment securely. Organizations, big and small, have access to the Twilio platform to accept payments over the phone with security built in and PCI DSS v3.2.1 certified.

The Payment Card Data Security Standard governs technical and operational requirements for managing cardholder data on a consistent basis globally. All entities processing, transmitting, or storing cardholder or sensitive authentication data must comply with this security standard or be subject to substantial financial penalties.

¹ Source: Federal Trade Commission's 2017 Consumer Sentinel Network Report



Accepting payments with Twilio Programmable Voice

Twilio's integration with payment providers eliminates the need for a business to become PCI DSS compliant to accept customer payments. Twilio will manage the capturing and processing of credit card information on your behalf using the payment provider of your choice.

Self-Service Interactive Voice Response (IVR) is an intuitive and customizable automated pay-by-phone solution for collecting credit card information without an agent present. This minimizes our customers PCI compliance scope using our <Pay> API, that only requires one line of code, speeding your time to market and ultimately reducing your development costs.

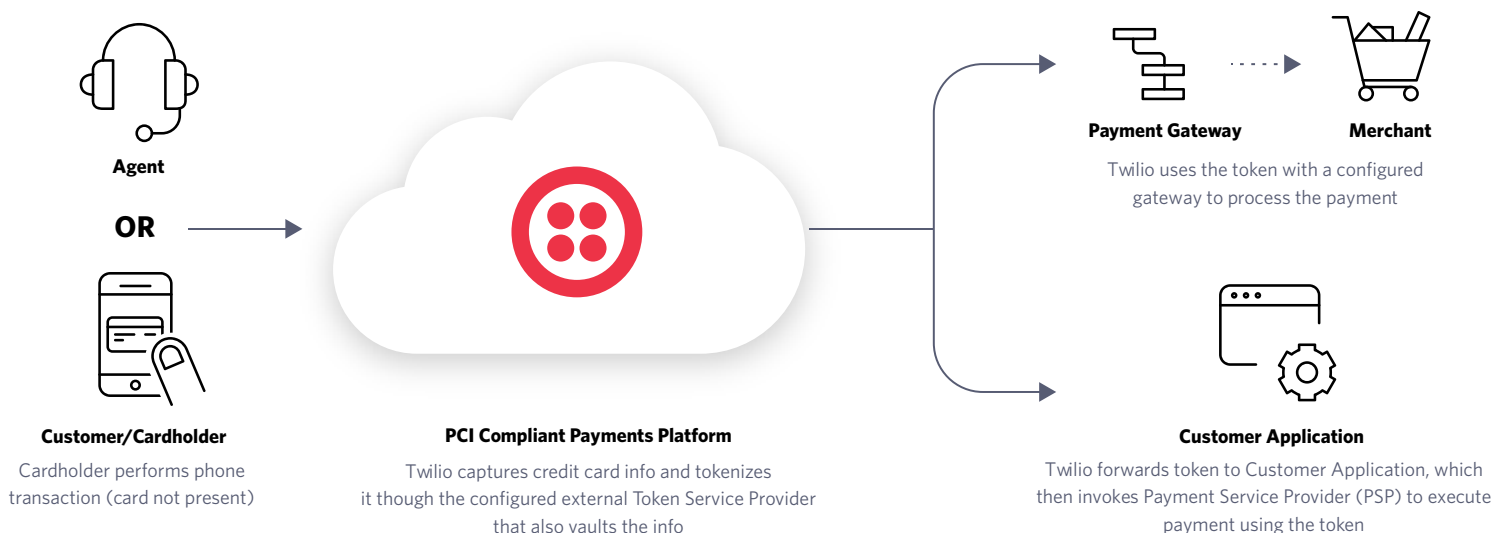
Replacing payment card numbers with surrogate values (tokens) can be used in future payments without the need for the charging entity to access credit card information. Tokenization protects card data by substituting a card's Primary Account Number (PAN) with a unique, randomly-generated sequence of numbers. The generated number is the same length and format as the original PAN. Therefore, it is no different from a standard payment card number in the virtual eyes of back-end transaction processing systems, applications,

and databases. This security technology is already being used by leading consumer financial brands like Visa and Mastercard.

Below, the diagram demonstrates how Twilio can be integrated on the front-end of the payment flow as a PCI compliant platform managing the collection and tokenization of credit card information or to optionally make a payment on behalf of customer applications. Payment gateways, used to authorize the transactions between you and your customer, can be selected from the Twilio Marketplace and support your existing billing relationships. In the case of executing the payment, Twilio would integrate with payment gateways classifying as card-not-present transactions, where neither the cardholder nor the credit card is physically present at the time of the transaction, which includes payments made over the phone.

The token is generated by the payment provider selected by the customer. Twilio is simply a proxy passing that information to the customer's application and will not store the information. Once a token is securely transmitted to the customer's application it is deleted. Payment providers can be selected from [<Pay> Connector navigation link](#) in the Programmable Voice console page.

Agent or Self-Service IVR





How Twilio Programmable Voice Complies with PCI DSS 3.2.1

Providing high levels of security is how we build trust in the tools our customers use to power their applications using our platform. Below is an overview of how Twilio is complying with PCI DSS standards.

- **Building and Maintaining Secure Network and Systems:** Developers must follow the Twilio Security Development Lifecycle (TSDL) while developing products, ensuring they are secure by design. Twilio's Cloud Security Standard (TCSS) comprises best-in-class security practices that include a defense-in-depth approach in our production environment, where all customer data and customer-facing applications are logically isolated in an AWS Virtual Private Cloud (VPC). Firewalls are used to maintain network segregation between different security zones in both the Corporate and Production environments. Twilio leverages AWS Access Control Lists (ACLs) to manage traffic and firewall rules are reviewed quarterly.
- **Protecting Cardholder Data:** Twilio supports TLS 1.2 to encrypt network traffic between the customer application and Twilio to safeguard sensitive cardholder data during transmission over open, public networks. Twilio defaults to the highest cipher supported by the customer's client; customers must enable TLS on their side. Twilio will never store cardholder data in our environment. Once the token is transmitted to the customer application the information is deleted via an automated process.
- **Maintaining a Vulnerability Management Program:** In adherence to the Twilio Vulnerability Management Standard, scans are conducted periodically and target different segments of our infrastructure.

Employee laptops have behavior-based anti-virus and anti-malware detection.
- **Regularly Monitoring and Testing Networks:** Twilio logs high risk actions and changes in our production network. We leverage automation to identify any deviation from our technical standards and raise issues within minutes of the configuration change occurring. Periodic risk assessments are performed at least annually to review the effectiveness of existing security controls and safeguards, as well as to identify new risk. Internal penetration testing is performed every six months to verify segmentation methods are operational, effective and the Cardholder Data Environment (CDE) is isolated.

Twilio employs a network-based intrusion detection system (IDS), GuardDuty, that analyzes AWS CloudTrail, VPC Flow Logs, and AWS DNS logs. It uses threat intelligence feeds, including lists of malicious IPs and domains, and machine learning to identify unexpected and potentially unauthorized and malicious activity within the Twilio AWS environment.



- **Implementing Strong Access Control Measures:** Access to information is restricted with a least privilege model. Twilio employees must take Twilio Security and Privacy training once a year, which covers our information security policies, best practices, and privacy principles to support company-wide awareness on the importance of security.
- **Maintaining an Information Security Policy:** Twilio maintains a suite of information security policies and standards as part of our continued commitment to maintain the confidentiality, integrity, and availability of Twilio systems, customer confidence, and corporate governance. These policies and standards apply to all Twilio employees, interns, and contractors accessing internal systems and/or customer data.

We also provide developers with a library of resources to facilitate integrating Twilio into their applications with security available at <https://www.twilio.com/docs/usage/security>. Additionally developers can reach out to our support team 24/7.



Twilio's Trust Mission

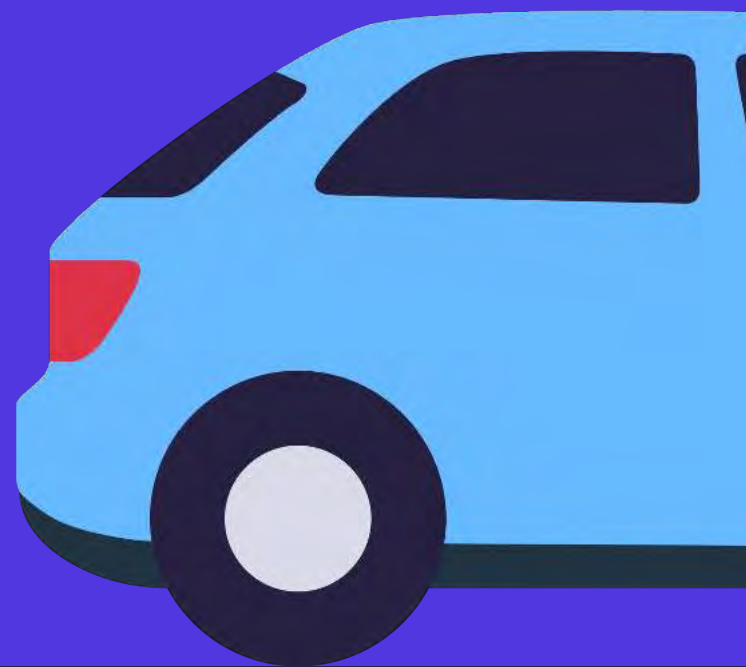
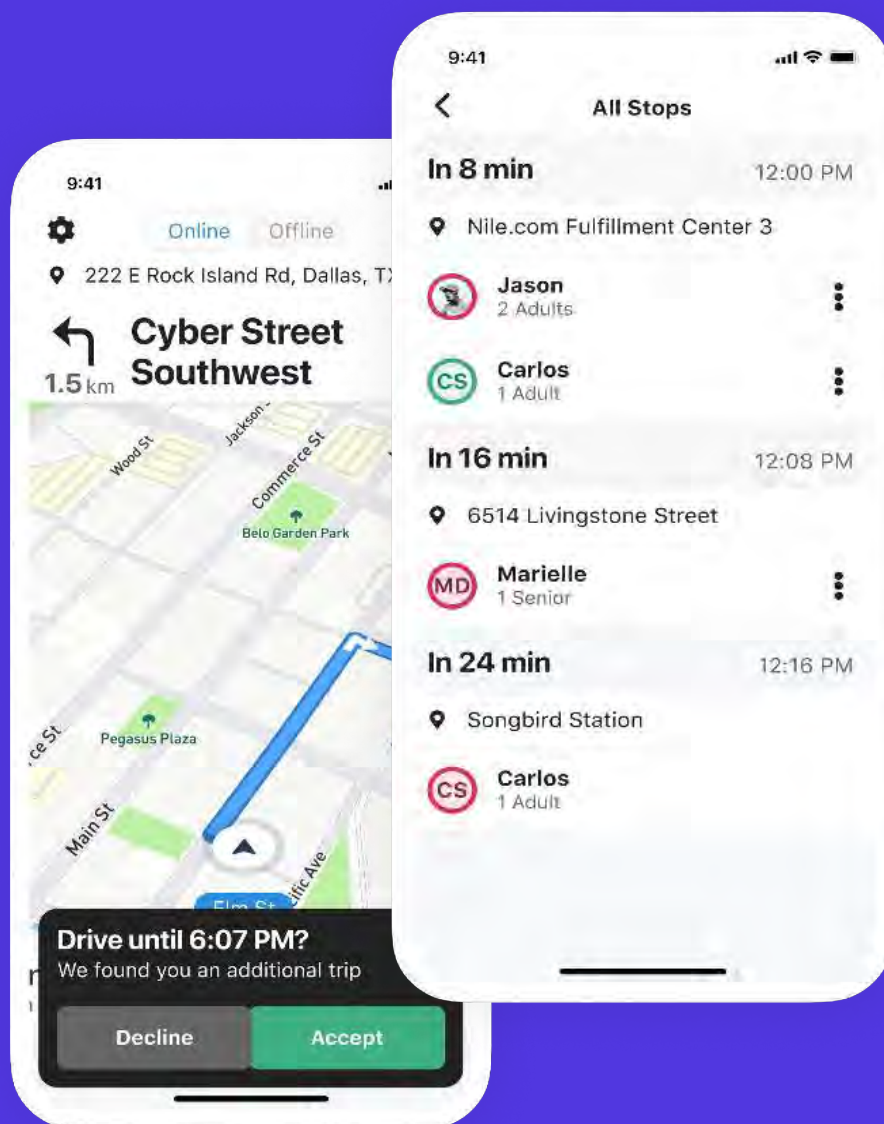
Trust is Twilio's most important security principle. It is founded on bold transparency, shared responsibility with our customers on the security journey, and our holistic approach to design, development and deployment. Your trust in Twilio is our top priority. PCI DSS Certification aligns with Twilio's continued effort to build customers trust in us to grow, support, and revolutionize their business.

Click below to learn more about Twilio's PCI DSS Certification and resources to build your business payment needs.

[Learn more](#)



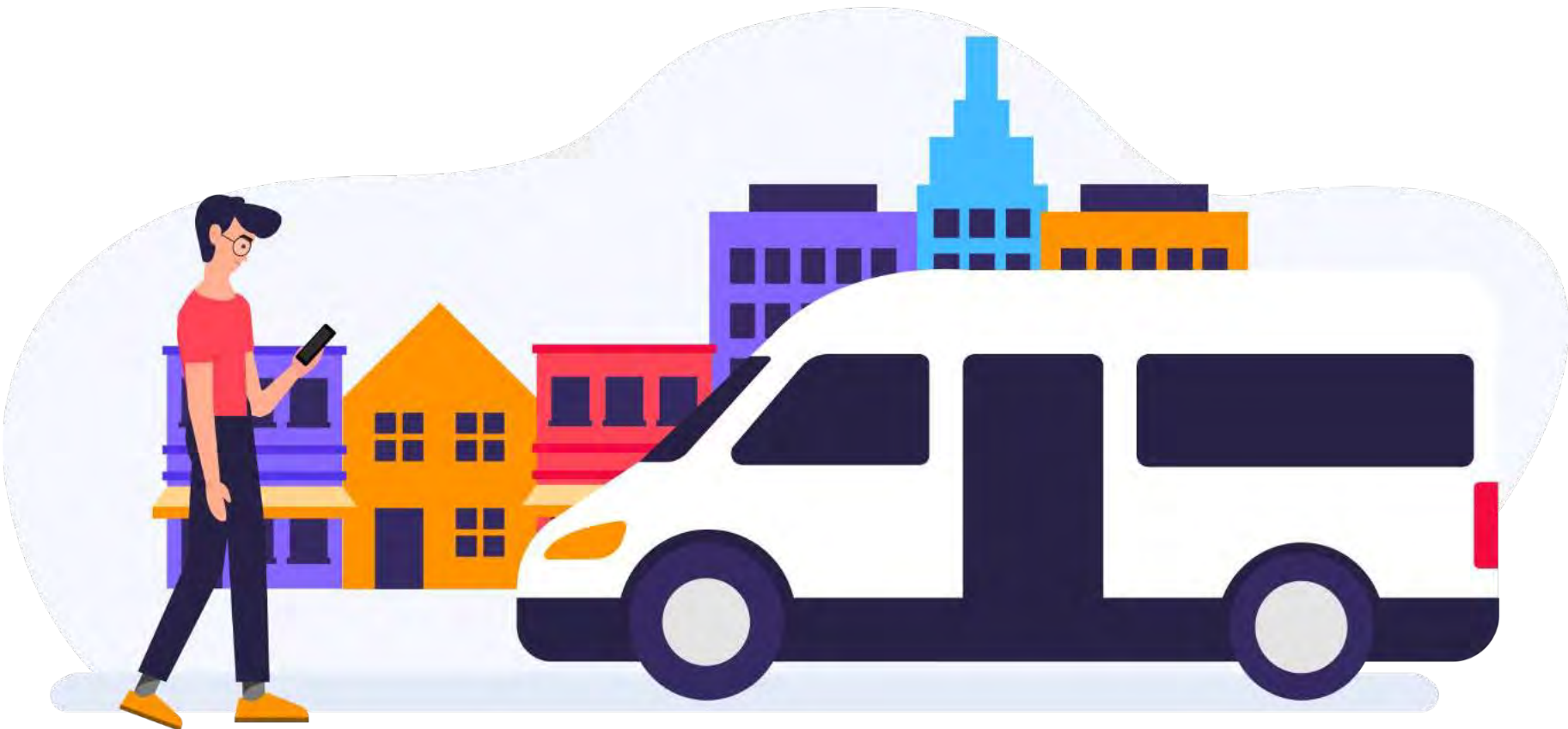
Twilio powers the future of business communications, enabling phones, VoIP, and messaging to be embedded into web, desktop, and mobile software. We take care of the messy telecom hardware and expose a globally available cloud API that developers can interact with to build intelligent and complex communications systems.

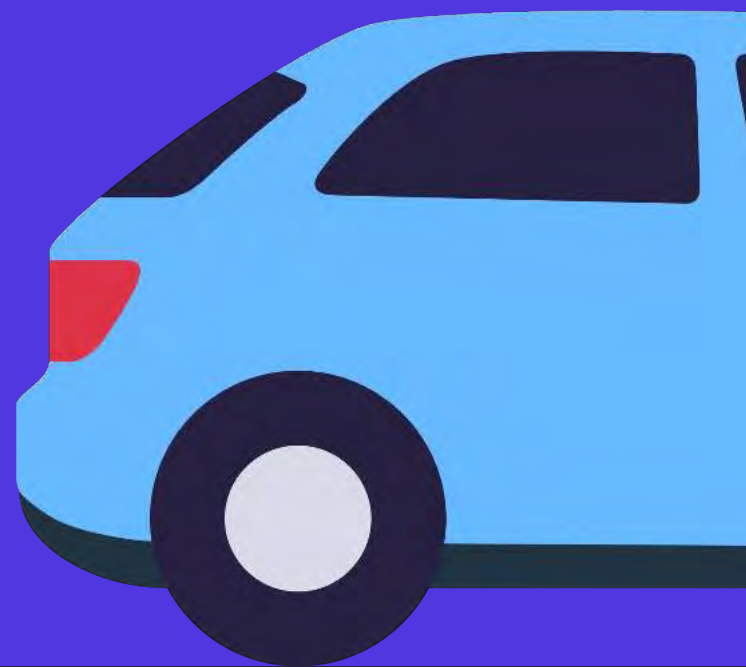
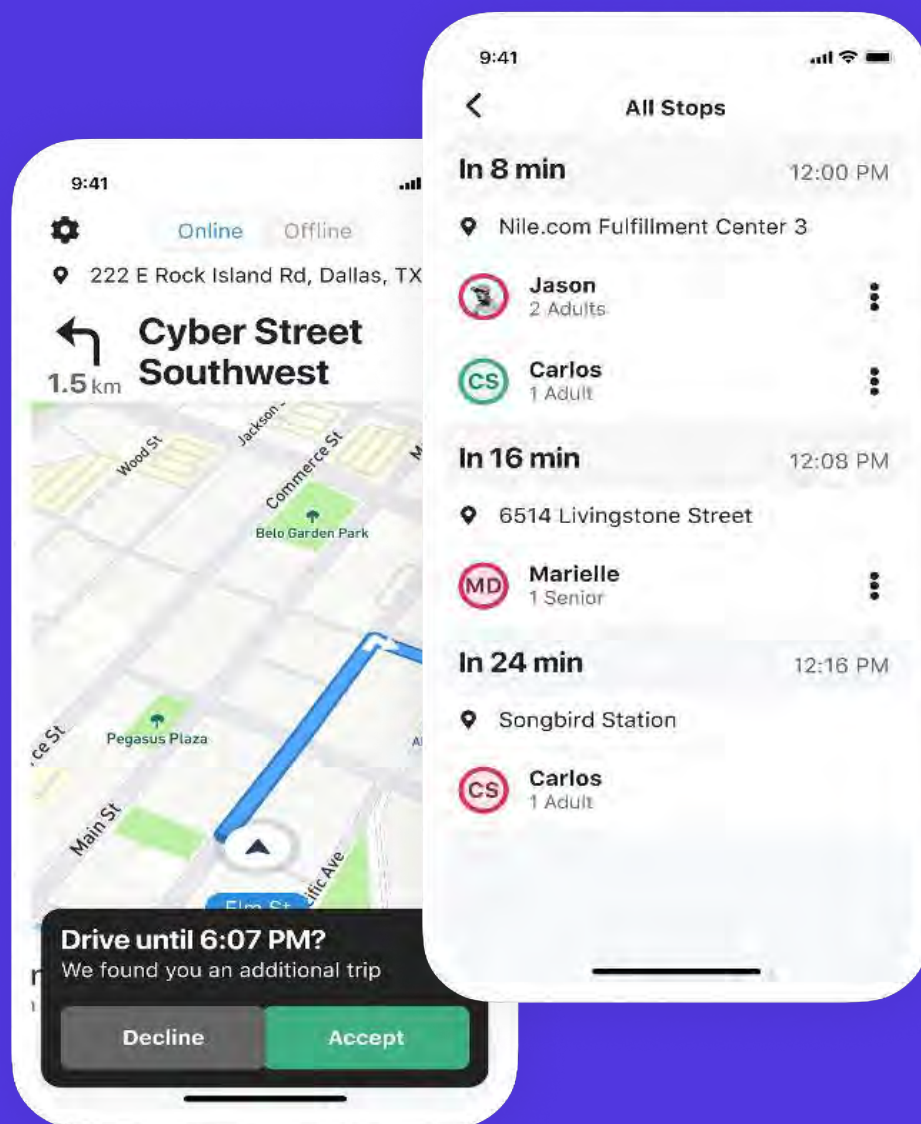


Spare Driver App Guide

Table of Contents

- 1. [Getting started](#) 3
 - 1.1. Downloading Spare Driver App 4
 - 1.2. Accessing Your Account 5
- 2. [Navigation & Main Settings](#) 6
 - 2.1. Setting Up Your Profile 7
 - 2.2. Main Settings Overview 8
- 3. [Driving with Spare Driver App](#) 10
 - 3.1. Starting the Duty 11
 - 3.2. Completing Your First Trip 14
 - 3.3. Trip Cancellation 18
 - 3.4. Adding a Walk-on Rider 19
 - 3.5. Ending Your Duty 21
- 4. [Troubleshooting](#) 22

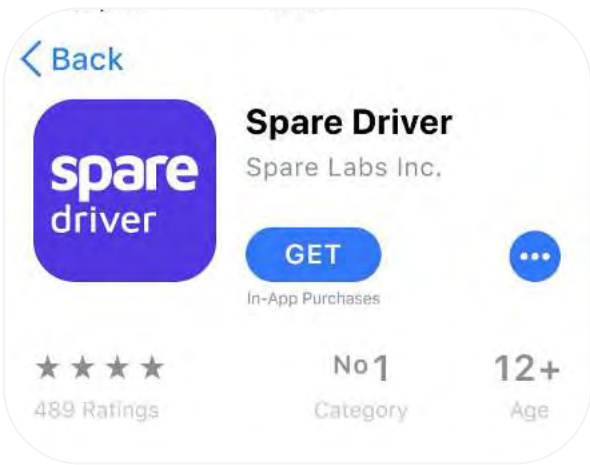




[1] Getting Started

- Downloading Spare App
- Accessing Your Account

1.1. Downloading Spare Driver App



1 Download the App on your device

From your phone or tablet, search for “Spare Driver App” in Google Play (for Android devices) or App Store (for iOS devices).

← This is how the Spare Driver App will look in the App Store.

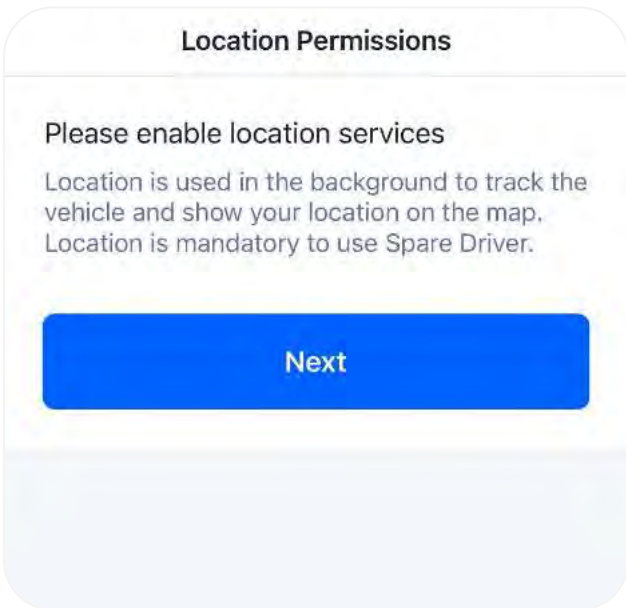


2 Check the App Settings

From your device Settings, tap on the Spare Driver App and make sure that:

- The **Location Settings** are changed to “**Always**”;
- The **Notifications** are **enabled** (this will allow you to receive instant notifications);
- **Motion and Fitness** setting is **enabled**;
- **Background App Refresh** is **enabled**;

i Enabling all of these settings will ensure that your device stays connected to the network and that you will be notified when changes are made to your manifest.



3 Follow Spare Driver App recommendations

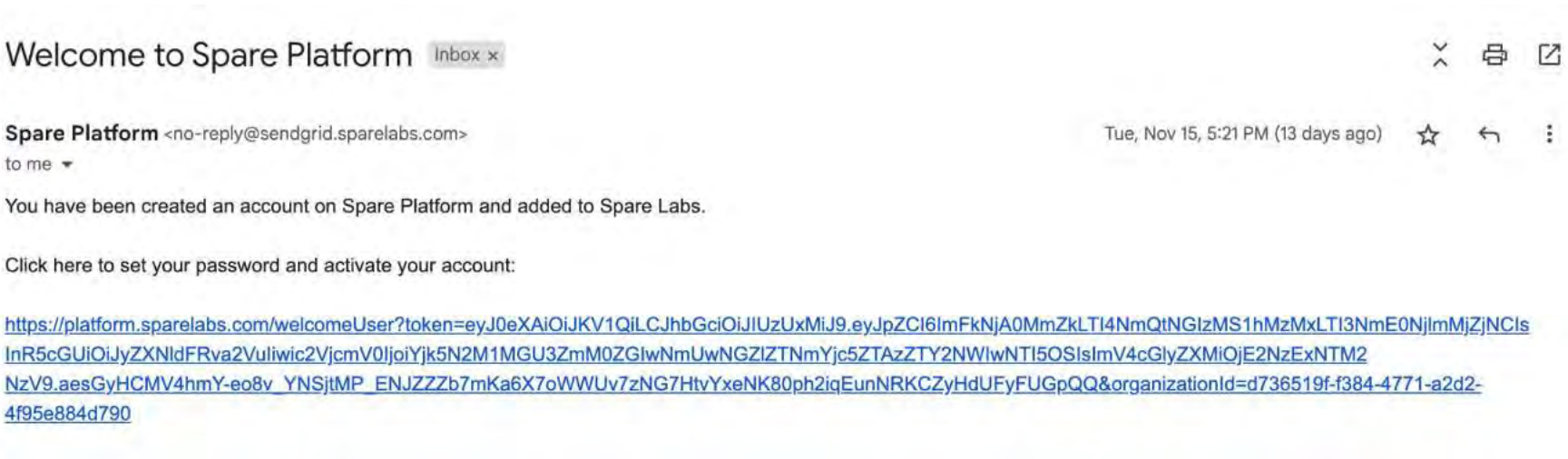
Spare Driver App will remind you if you forget to set up any of the settings above. Follow the App instructions to proceed.

1.2. Accessing your Account

1 Setup your account

You should have received an invitation email from sparelabs.com.
An invitation link will redirect you to the Spare Driver app and the account setup.

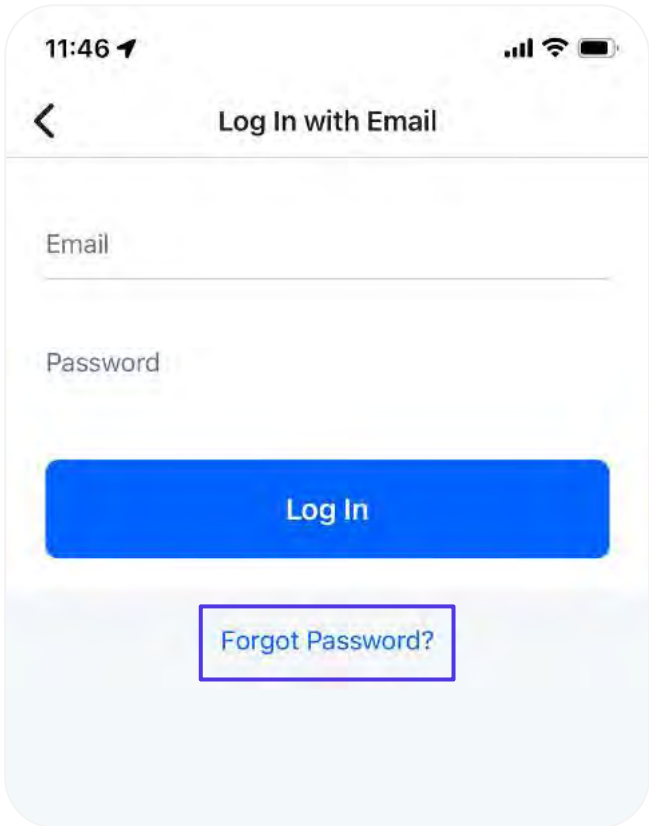
You can log into your account via your email and a password you will set the first time.



 Please contact your **administrator** if you don't have login credentials or did not receive a registration email.

2 Log in to your account

You can log into your account via your email and a password you will set at the first time.

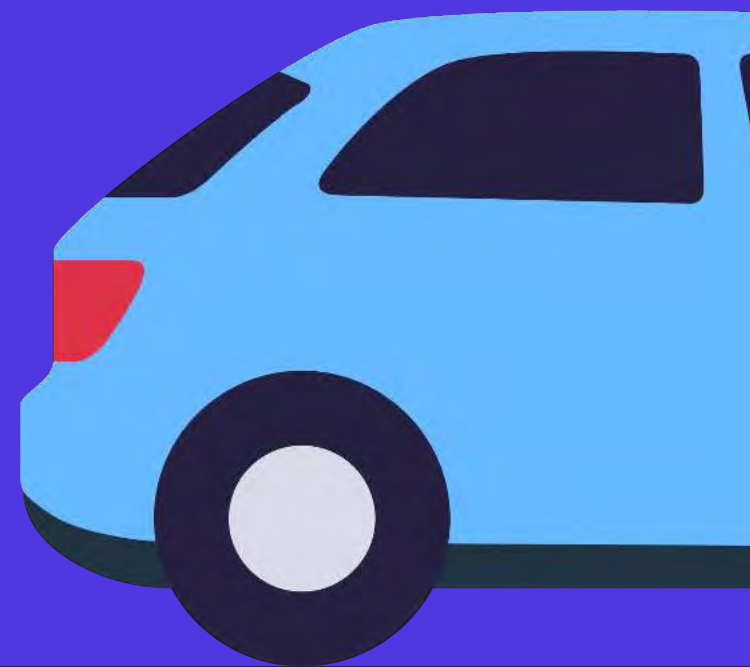
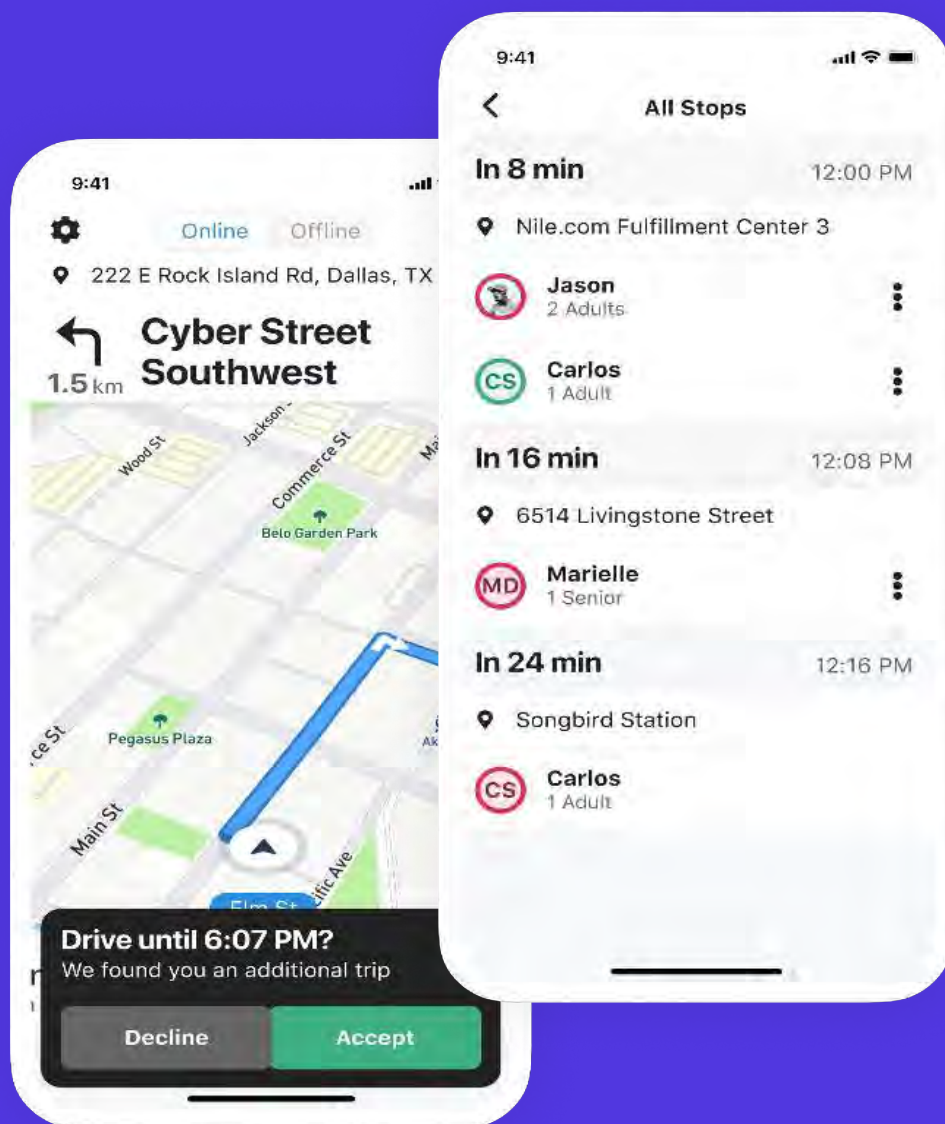


Reset your password

If you don't remember your password, you can tap on the **"Forgot Password?"** button. You will receive an email with a password reset link.

If you request a password reset too many times, the system might no longer send you a password reset email. Please get in touch with your administrator instead.

 Remember to follow your manager's instructions and **log out** after your duty if instructed to do so.



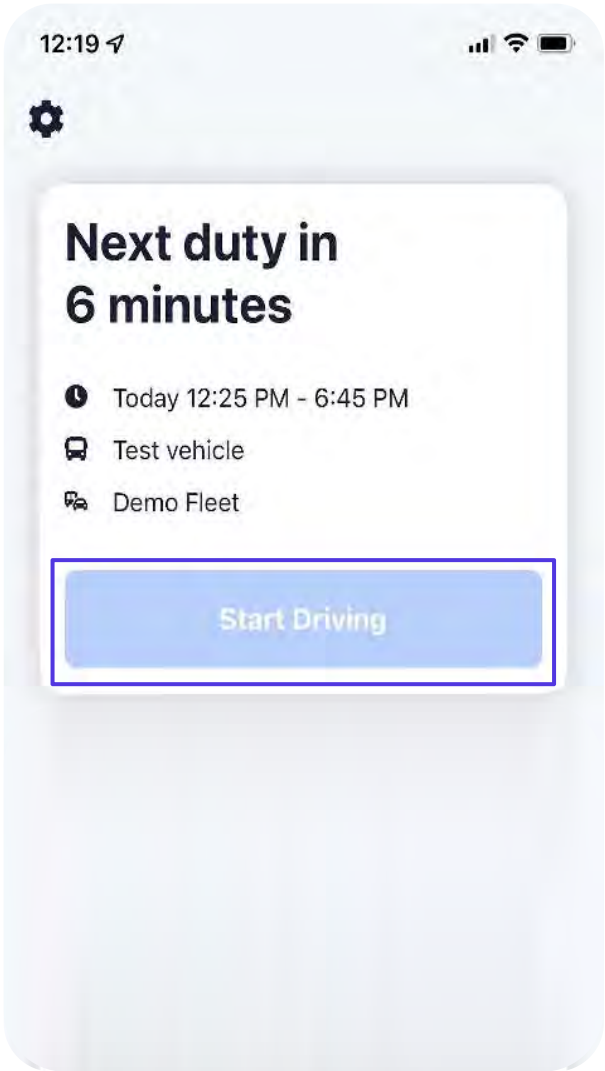
[2] Navigation & Main Settings

- Setting Up Your Profile
- Main Settings Overview

2.1. Setting Up Your Profile

This section will help you review the main settings of the Spare Driver App, learn how to view your trip history, and find help resources.

1 Check your next duty information



Once you log in to your account and select your organization name, you'll see your duty information on the home screen.

The information includes:

- 1. Your shift time today
- 2. The vehicle you're driving
- 3. The fleet your duty is associated with

Please note that you can start your duty **up to 5 minutes before** your duty start time indicated in the app.

i If you can't see your duty or it looks incorrect, contact your administrator.

Once you hit the **"Start Driving"** button, you'll activate the GPS, and your duty will officially start.

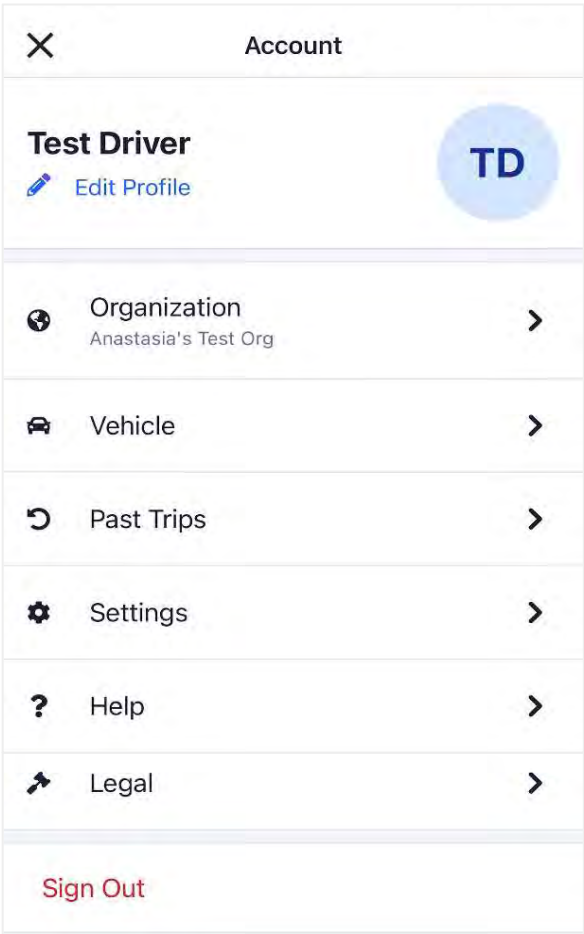
As the screenshot on the left indicates, it's too early to start the duty. Let's explore the overall settings while waiting. ↓

2 Check the main settings

Tap on the  icon to go to the main settings page. From there, you can do the following:

-  Fill in your Driver Profile, add personal information and photo;
-  View your organization details or switch between different organizations, if applicable;
-  View your vehicle information, including its features (wheelchairs, car seats, etc.);
-  Review Past Trips history* (Today | Last 30 days | All Time);
-  Set the screen mode (light/dark) and enable sound notifications;
-  Browse help articles and resources;
-  Get familiar with the Terms of Service and Privacy Policy;

You can also **Sign Out** from your account here →



*The "Review Past Trip History" is an optional function and may be disabled on certain devices.

2.2. Main Settings Overview

1 Edit Profile

You can update your contact information and upload your photo here.

<

Update Your Profile



Change Profile Photo

First Name

Test

Last Name

Driver

Email

sample@gmail.com

Phone Number

+12369711618

Confirm

2 View Organization

Switch between the organizations here. Tap on the organization name to select it.

<

Select Organization

Demo Organization 1

>

Demo Organization 2

>

3 Vehicle

You will have the information already pre-filled. Please contact your administrator if any changes need to be made.

<

Vehicle Settings

Make

Model

License Plate

Color

Passenger Seats

Passenger Seats

-

4

+

Vehicle Features

Add a new feature

+

Save

4 Past Trips *

If your organization enabled this function, you will be able to view the past trips' history. Tap on each trip for a short description.

<

Past Trips

Today

Last 30 Days

All Time

2 completed trips

\$0.00 total

\$0.00 fares + \$0.00 tips

Wed, November 30, 2022

1:48 PM

⚠

 Ride Cancelled

Tue, November 29, 2022

1:55 PM

\$0.00 + \$0.00 tip

Tue, November 29, 2022

1:34 PM

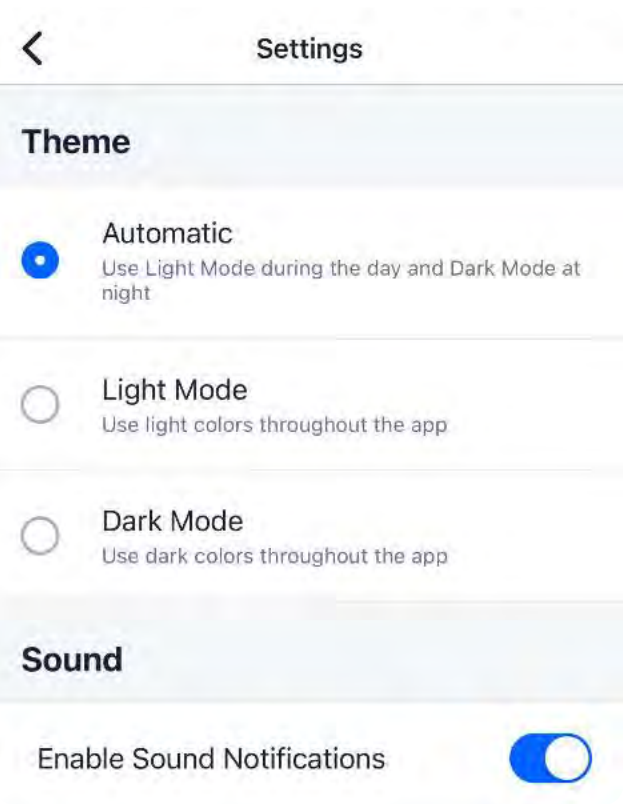
\$0.00 + \$0.00 tip

*The "Past Trip" function is optional and may be disabled on certain devices.

2.2. Main Settings Overview

5 Settings ⚙️

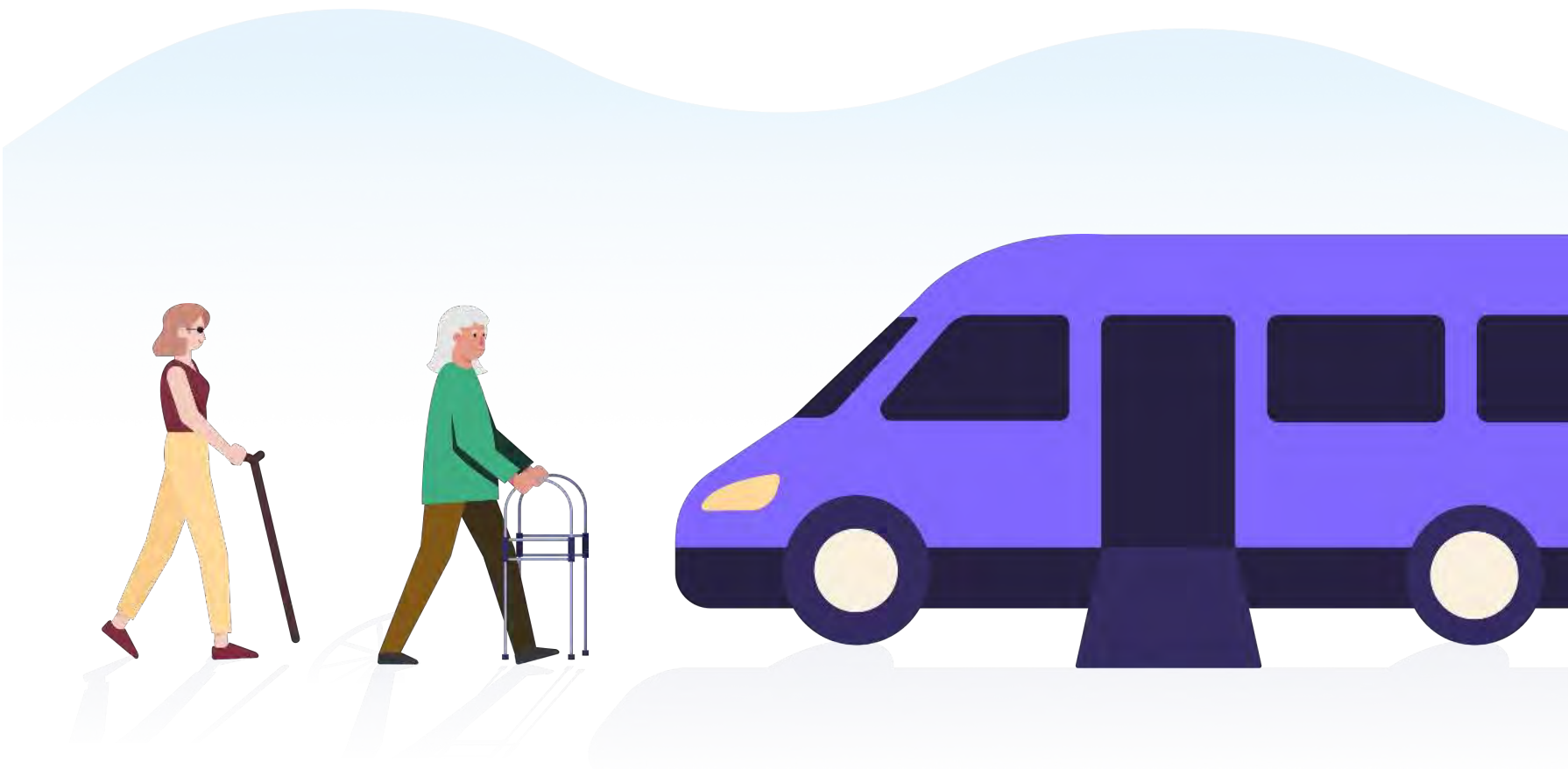
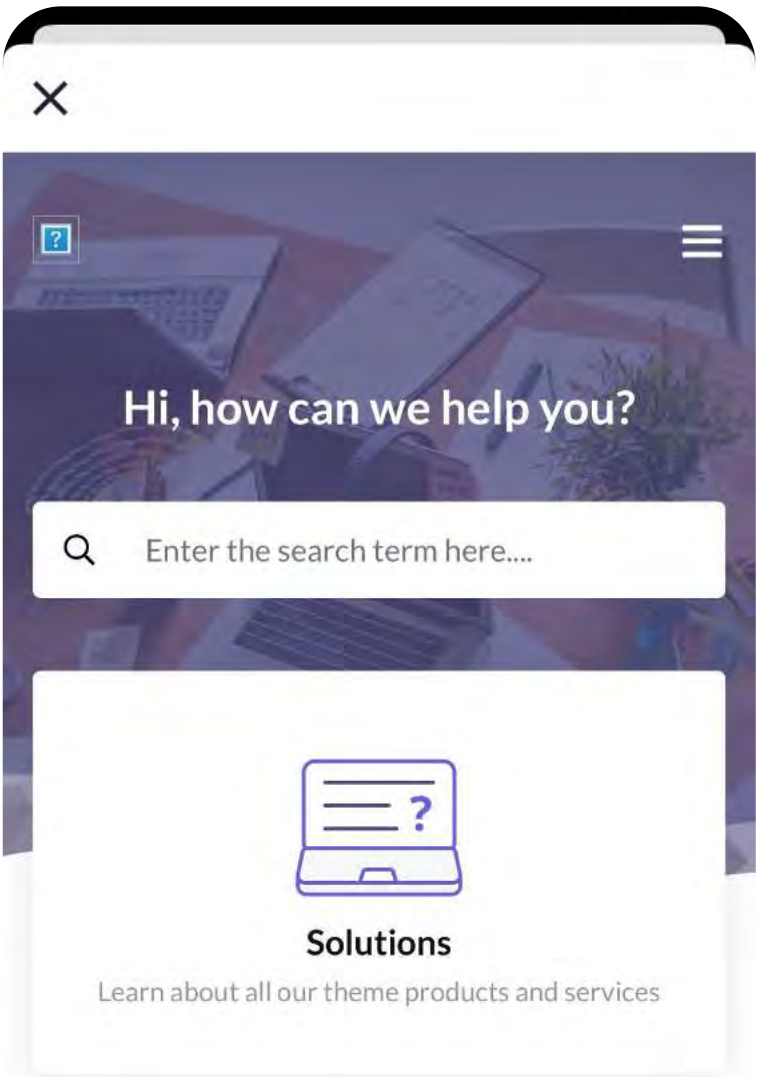
Choose the light mode and Sound Notification settings here.

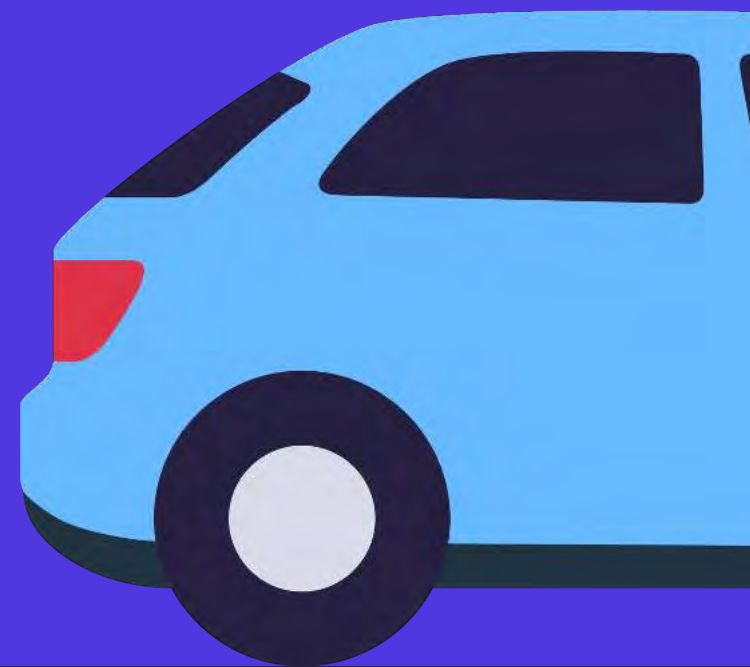
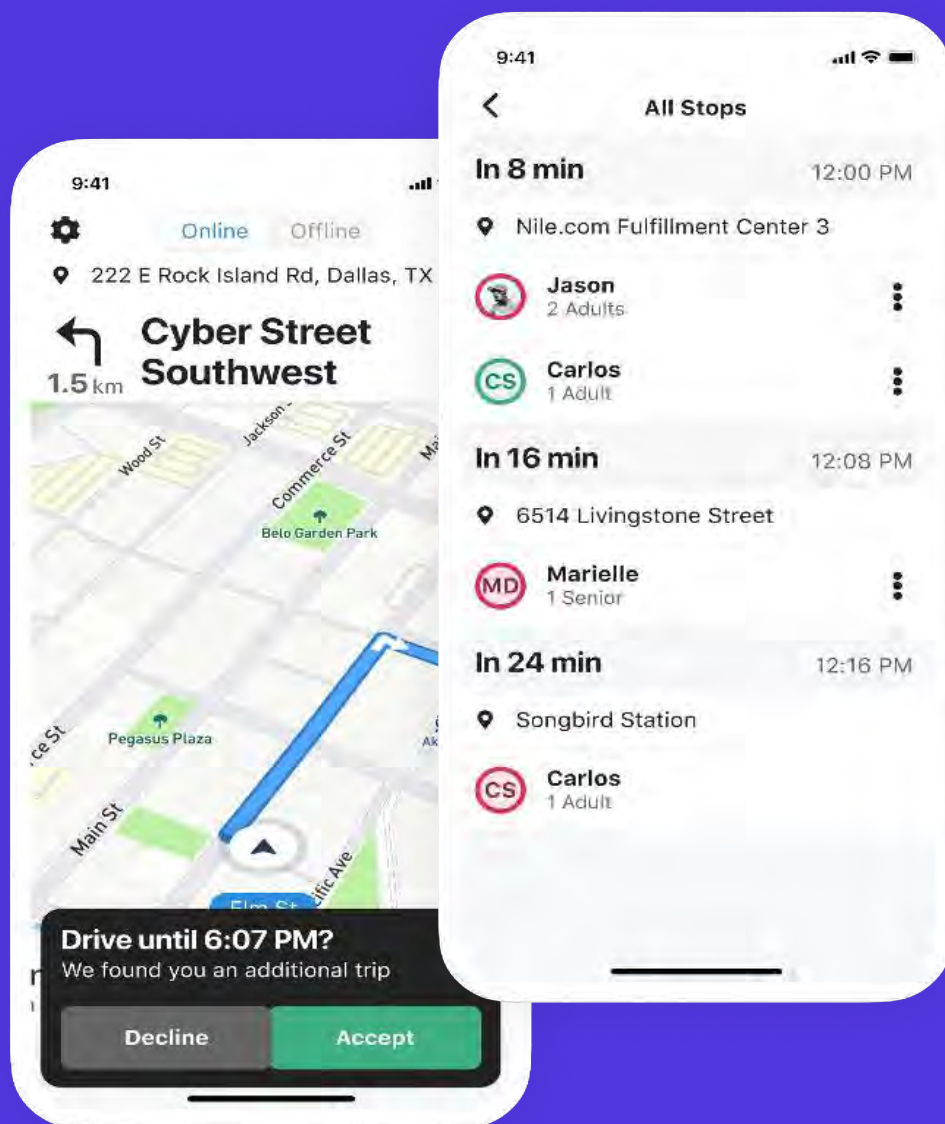


 We highly recommend that the Sound Notifications are turned on.

6 Help ?

This button leads to Spare Help Centre. Type your question in the search bar and read the help articles available.





[3] Driving with Spare Driver App

- Starting the Duty
- Completing Your First Trip
- Trip Cancellation
- Adding a Walk-on Rider
- Ending Your Duty

3.1. Starting the Duty

In this section, you will learn how to start your first duty, check your driver break policy and stay informed about your duty changes.

1 Start your Duty

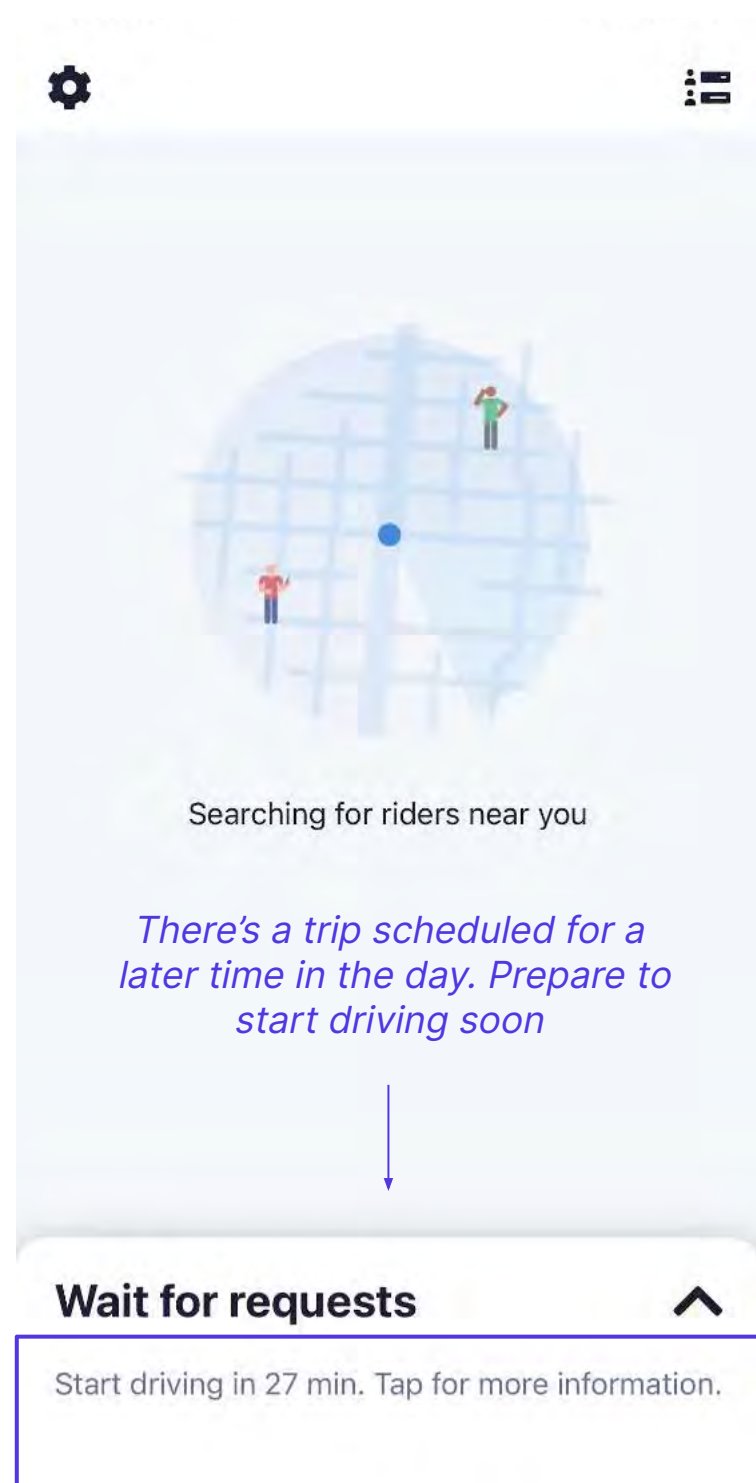
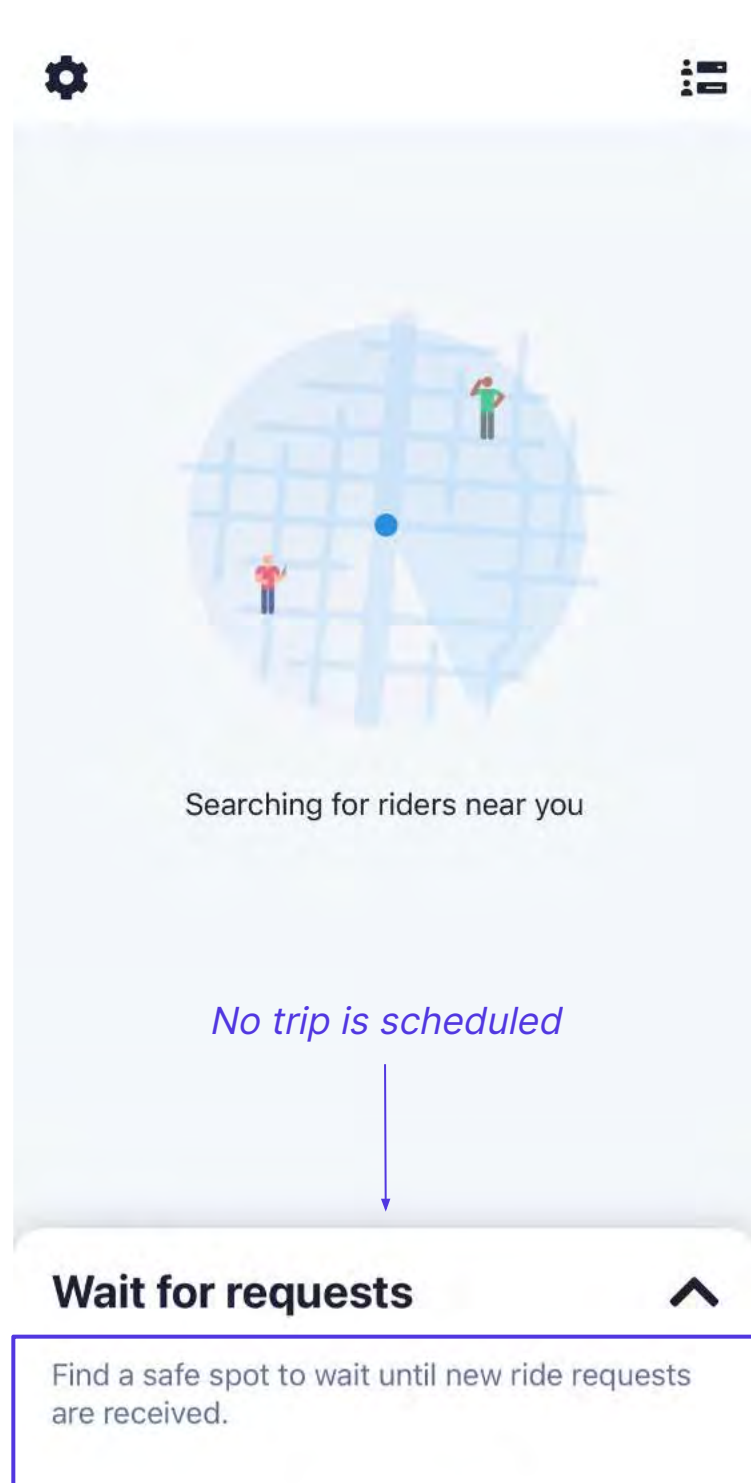
Once you begin your duty, you will be taken to the main screen of the Spare Driver App.

2 Wait for you First Trip

→ If there are no immediate pre-booked trips, your screen will look like this.

When you have no trips, find a safe spot to park and wait for the navigation to your next stop to appear. Your organization may provide specific waiting/staging locations.

→ If your first trip is scheduled for a later time in the day, you will see the amount of time until you need to start driving to the pickup location.

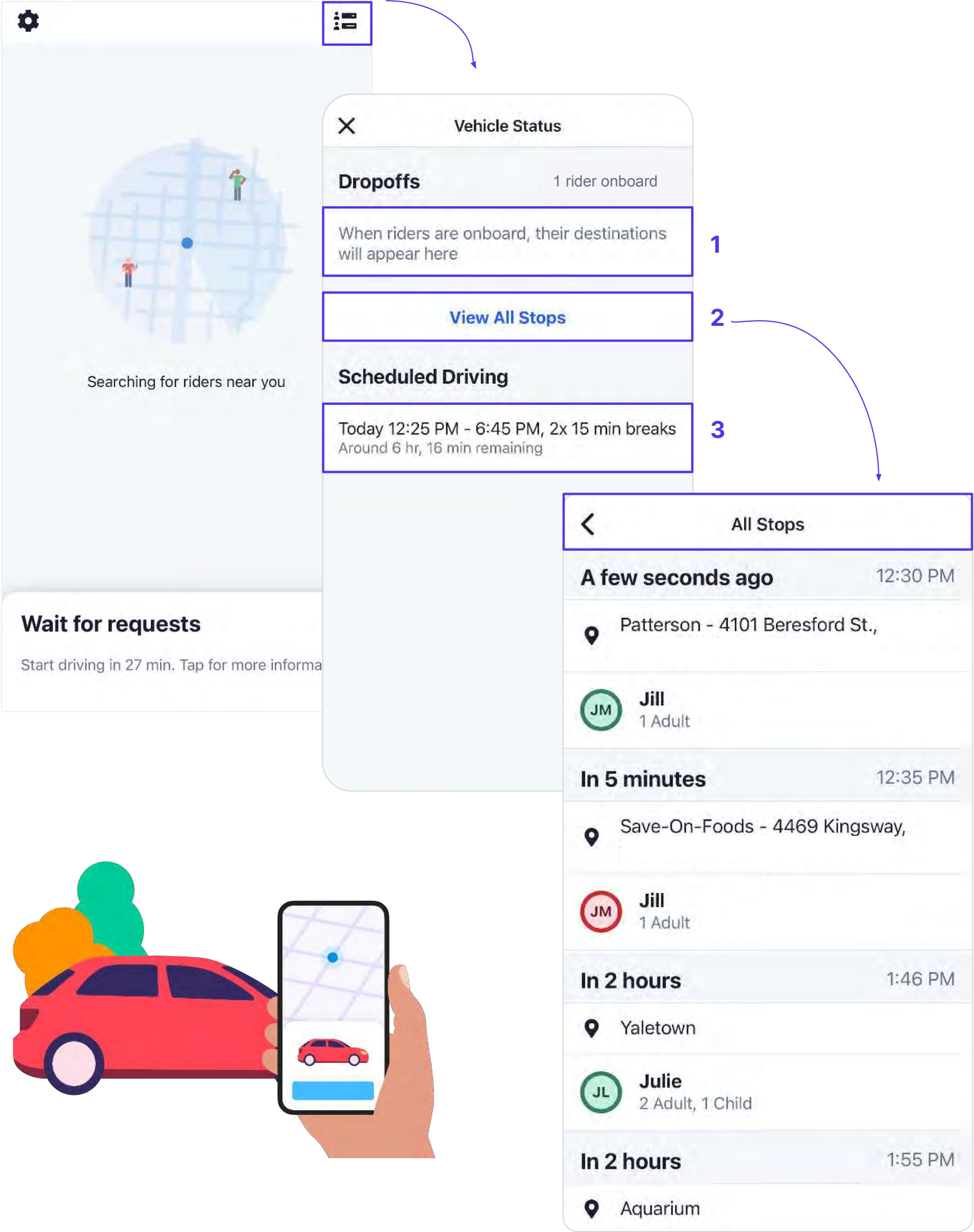


3.1. Starting the Duty

3 View your vehicle status

Tap on the  con in the top right corner to view:

- [1] **Dropoffs:** dropoff information for any riders on board
- [2] **Scheduled Driving:** information about your duty hours + breaks policy
- [3] **View All Stops:** your trip itinerary for the day. Note that this setting is optional; you might need to reach out to your administrator to enable it.



The screenshot illustrates the 'Vehicle Status' menu and the 'All Stops' list. The 'Vehicle Status' menu is shown as a modal overlay on a map background. It contains three sections: 'Dropoffs' (1 rider onboard), 'View All Stops' (a blue button), and 'Scheduled Driving' (Today 12:25 PM - 6:45 PM, 2x 15 min breaks, Around 6 hr, 16 min remaining). The 'All Stops' list is shown as a separate modal overlay, listing stops with their times, locations, and rider information.

Vehicle Status

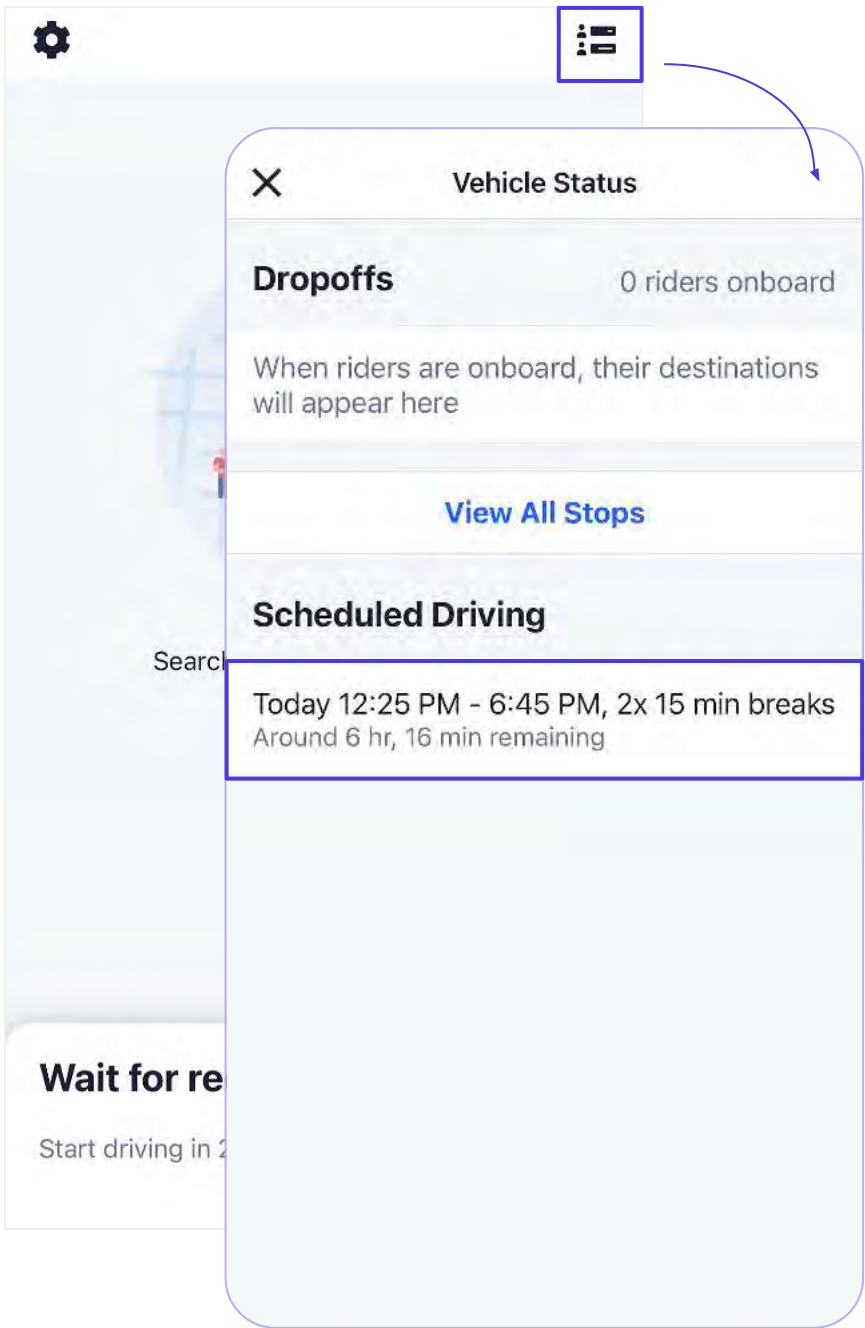
- Dropoffs** 1 rider onboard
- When riders are onboard, their destinations will appear here
- [View All Stops](#)
- Scheduled Driving**
- Today 12:25 PM - 6:45 PM, 2x 15 min breaks
Around 6 hr, 16 min remaining

All Stops

- A few seconds ago** 12:30 PM
-  Patterson - 4101 Beresford St.,
-  **Jill**
1 Adult
- In 5 minutes** 12:35 PM
-  Save-On-Foods - 4469 Kingsway,
-  **Jill**
1 Adult
- In 2 hours** 1:46 PM
-  Yaletown
-  **Julie**
2 Adult, 1 Child
- In 2 hours** 1:55 PM
-  Aquarium

3.1. Starting the Duty

4 View the automated driver breaks policy



If the Driver Breaks function is enabled by your organization, you will see the breaks information in your **Vehicle Status**.

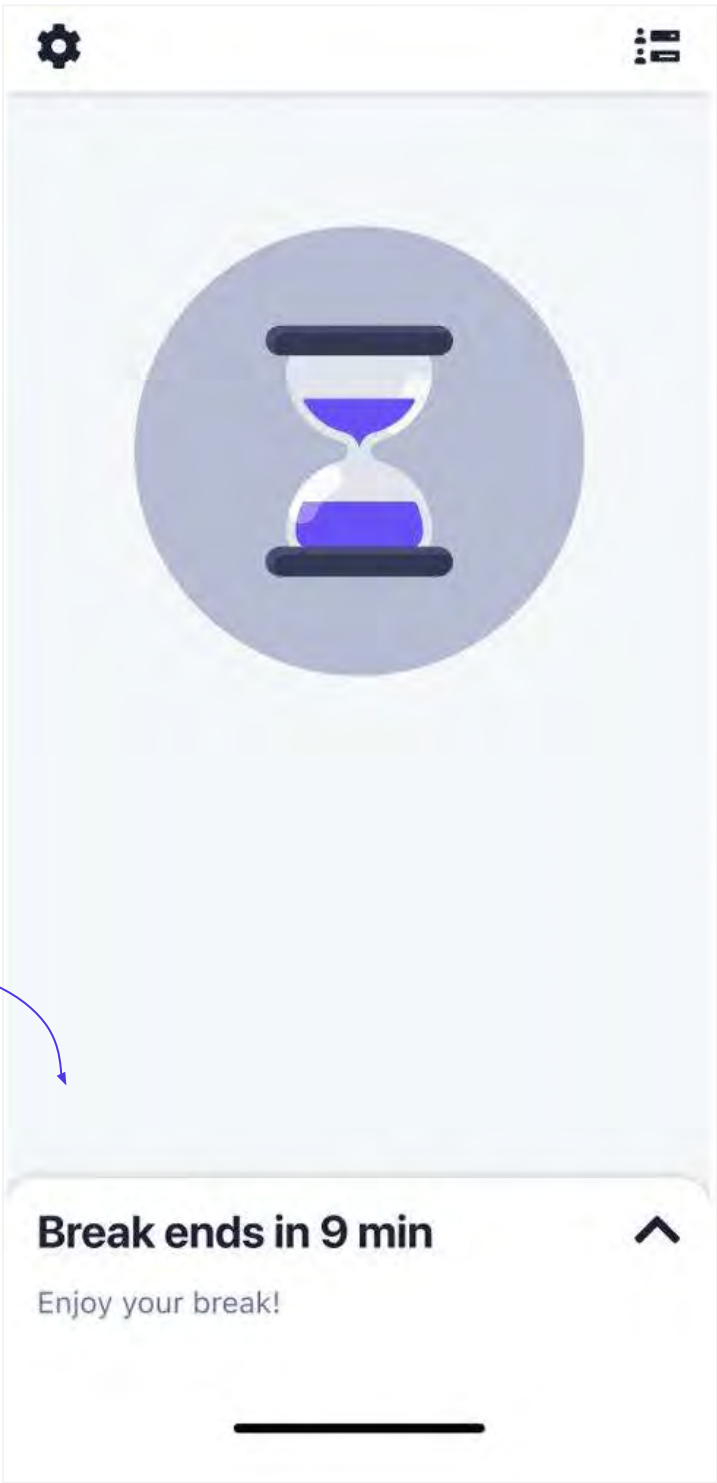
For example, the screenshot on the left says that there are two 15 min breaks scheduled for the shift.



Please note that **breaks automatically move around** to maximize your schedule's overall efficiency.

Once the break starts, a notification will pop up. You will also see how much time is left until the end of the break. You will not receive any new trip alerts during the break.

Once the break is over, another notification will appear, inviting you to come back to driving.

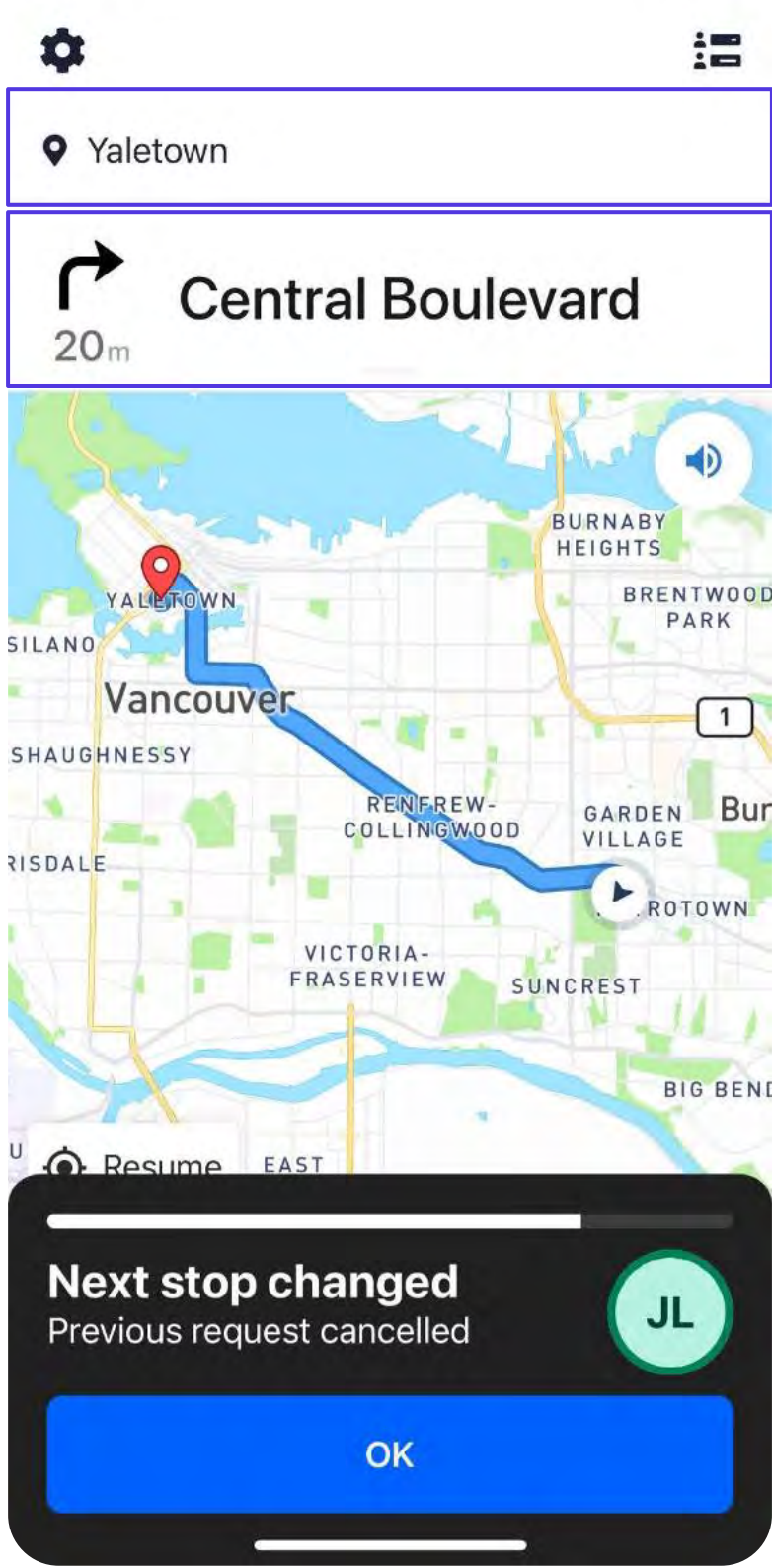


3.2. Completing your First Trip

This section will give you step-by-step instructions on how to complete your first trip, including navigating to your destination, confirming the rider's pickup/dropoff, adding a walk-on rider, or canceling the trip.

1 Get notified about a new trip

When a trip request comes in that changes your next stop, the notification below will pop up to let you know. The notification will disappear after a few seconds, or you can tap **OK** at the bottom to dismiss it.

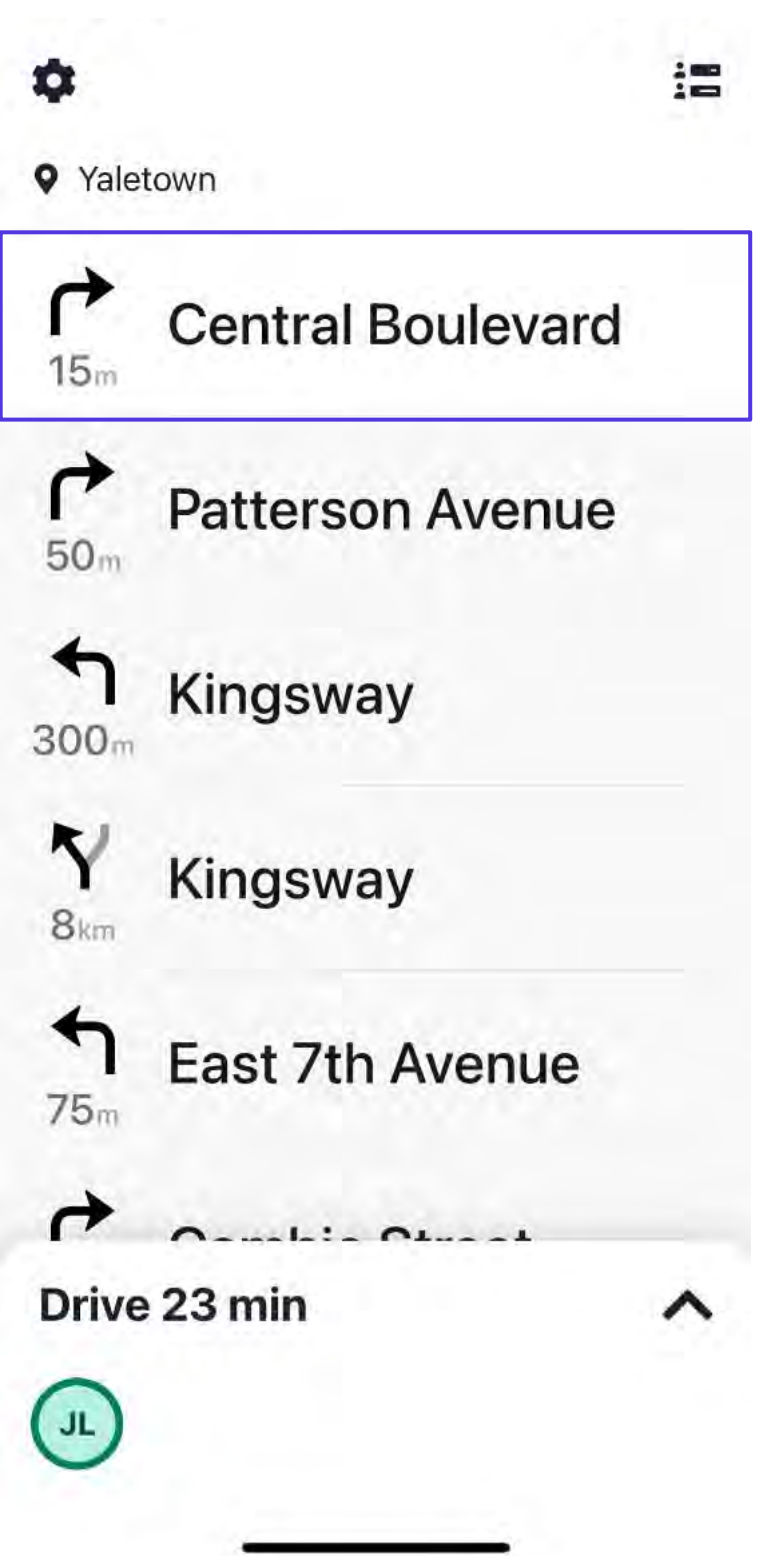


At the bottom of the main screen view, you'll find the **initials or a profile picture of your next pickup or dropoff** [3].

You will also see the **estimated time to arrive at your next stop** [4].

Now that there is a ride request, the map will automatically route you to your **next stop [1]**, which is listed at the top of the screen.

Tap on your **next turn [2]** to see a list of all your directions. Tap on the **next turn [2]** again to hide the details.



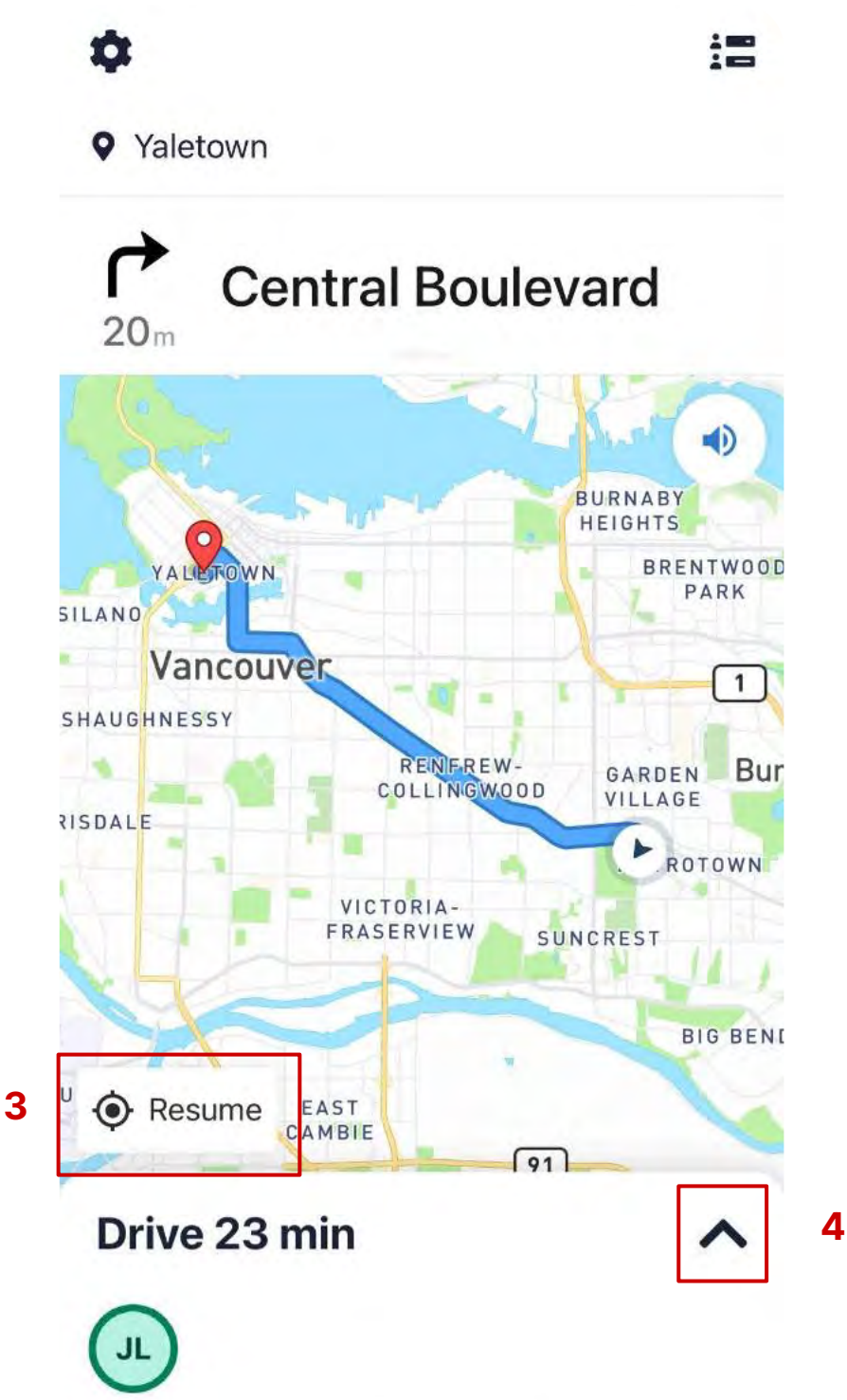
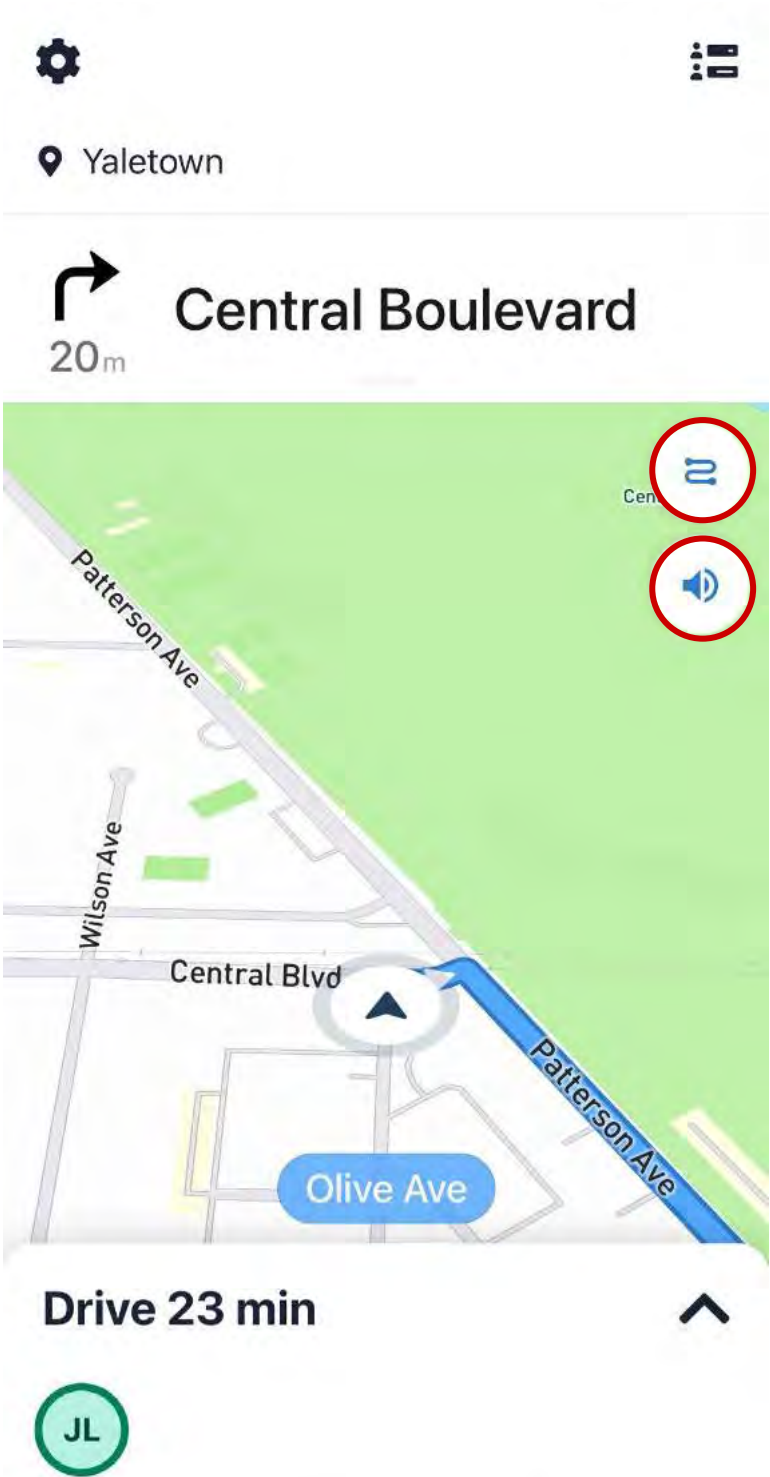
3.2. Completing your First Trip

2 Navigate to the pickup location

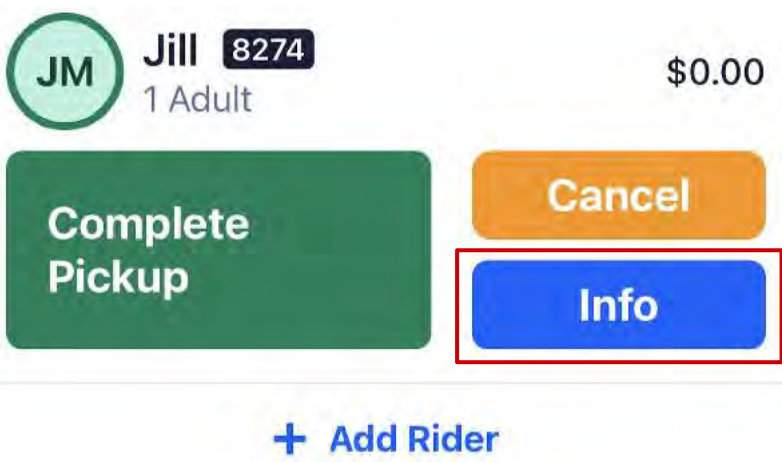
You can **mute/unmute** your navigation by tapping on the  **icon [1]** in the top right.

You can also **see a bird's eye view of your trip** by tapping on the  **icon [2]**.

Tap on the  **Resume button [3]** to return to the **turn-by-turn view**.



3 View your rider information



Tap the arrow at the bottom of the screen **[4]** **to view the passenger(s) details**.

Here you will see information about the riders at your next stop as well as the Complete Pickup and Complete Dropoff buttons.

If your organization policy permits it, you can **contact the rider** from this pop-up menu by tapping on the **"Info" button [5]**.

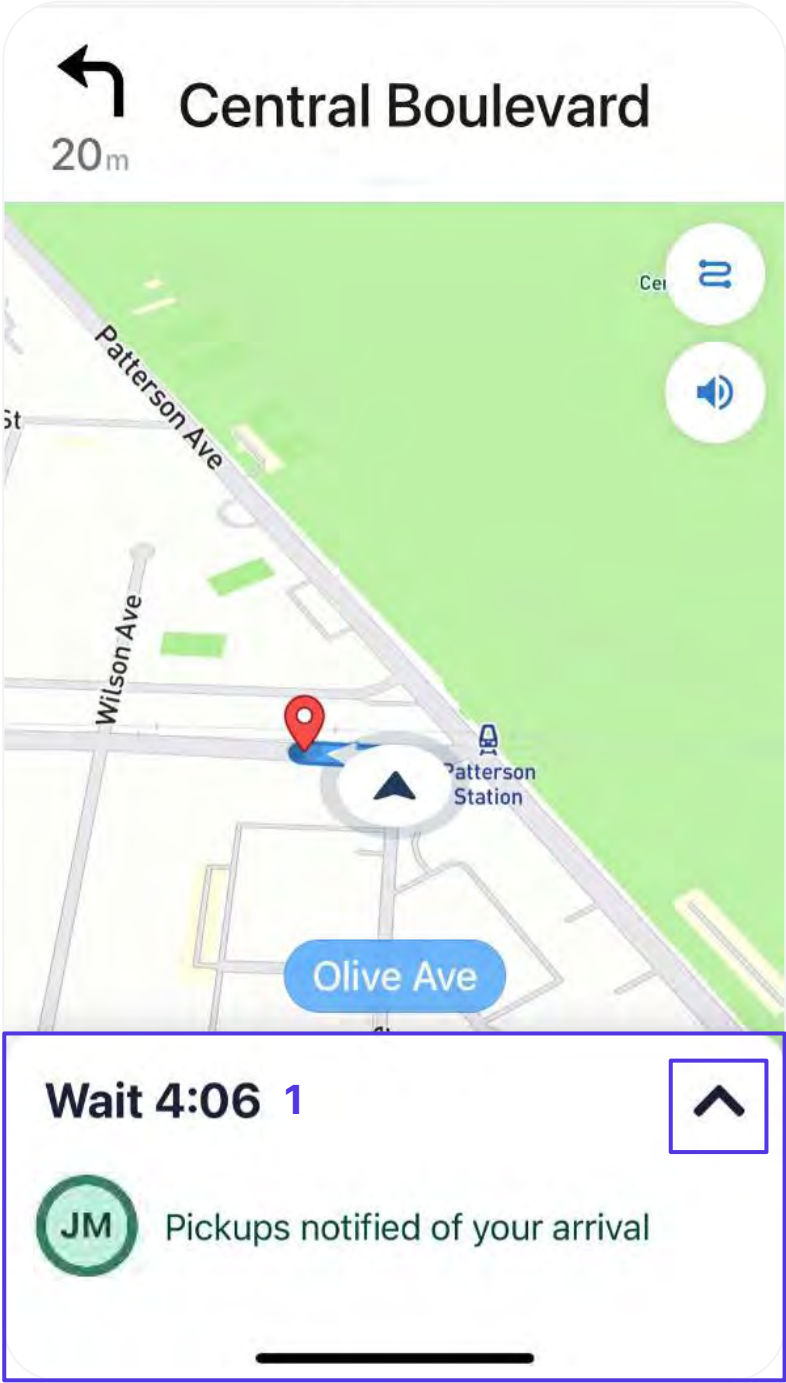
3.2. Completing your First Trip

4 Board your rider(s)

Once you arrive at the pickup location, your rider will be notified of your arrival and the **wait time countdown [1]** will begin.

i The amount of **wait time** is set by your organization. If you get to the stop early, the amount of time you are early is added to the timer.

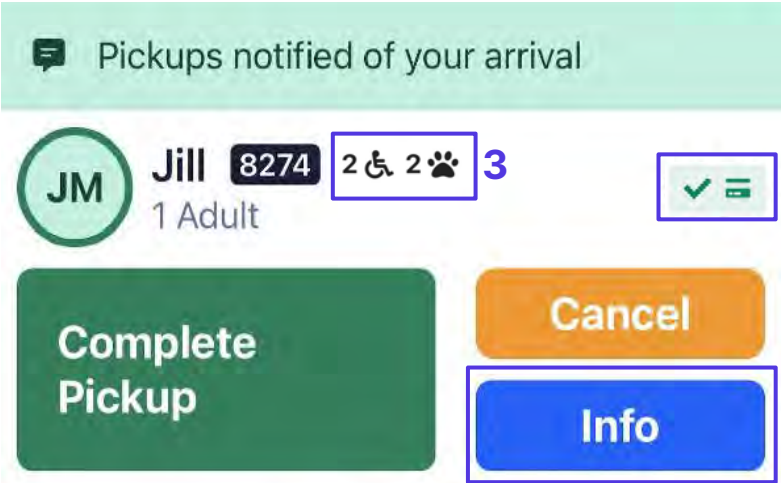
See p.19 of this guide for instructions on what to do when **the rider is running late**.



Tap the **arrow [2]** at the bottom of the **screen** to view the passenger(s) details and how much wait time is left.

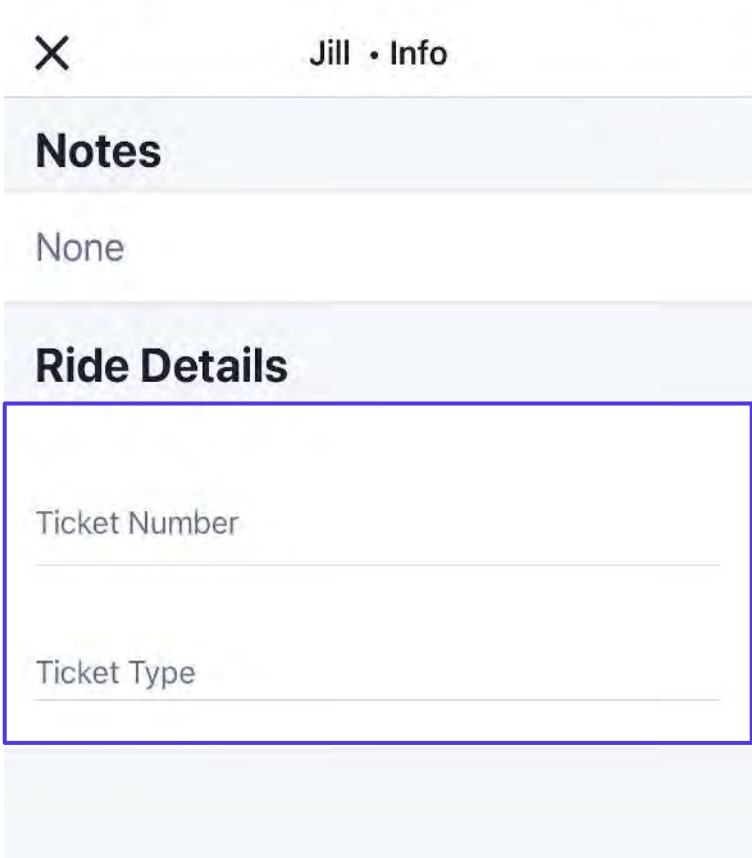
If a rider has **multiple passengers [3]** or requires an **accessibility accommodation**, like a wheelchair, it will be listed by their name.

The **fare [4]** to be collected also appears to the far right. If any dollar value is shown, that amount must be collected from the rider on the vehicle. If a checkmark is shown, the rider has already paid their fare



i You might need to fill in or check the rider's information to complete their boarding.

Tap on the **"Info"[5]** button to view any notes about the rider and fill in any information your organization requires to be collected, such as **ticket number and/or type [6]**.

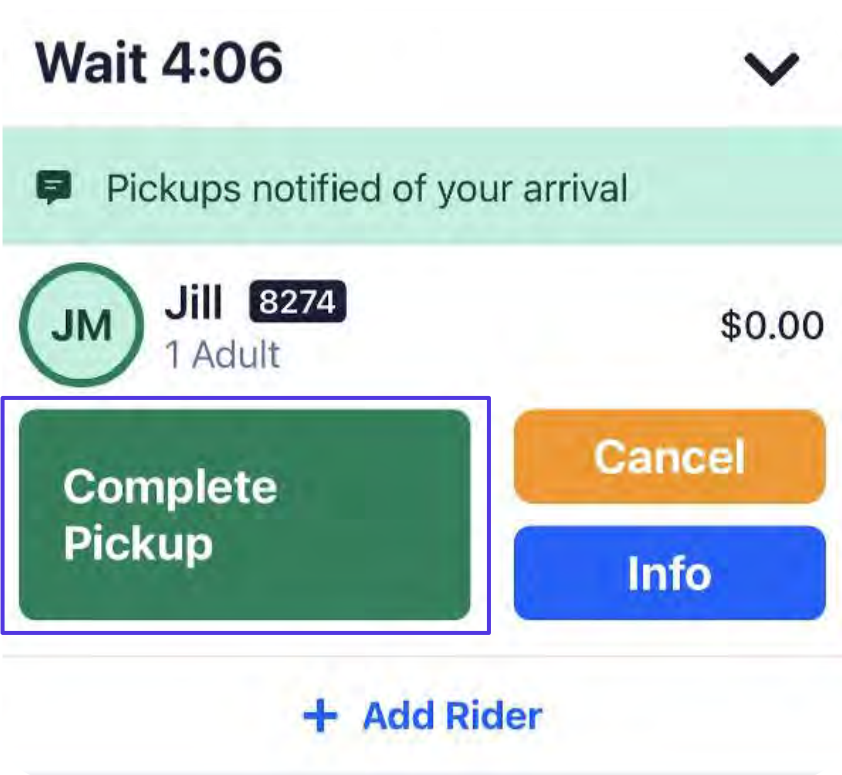


3.2. Completing your First Trip

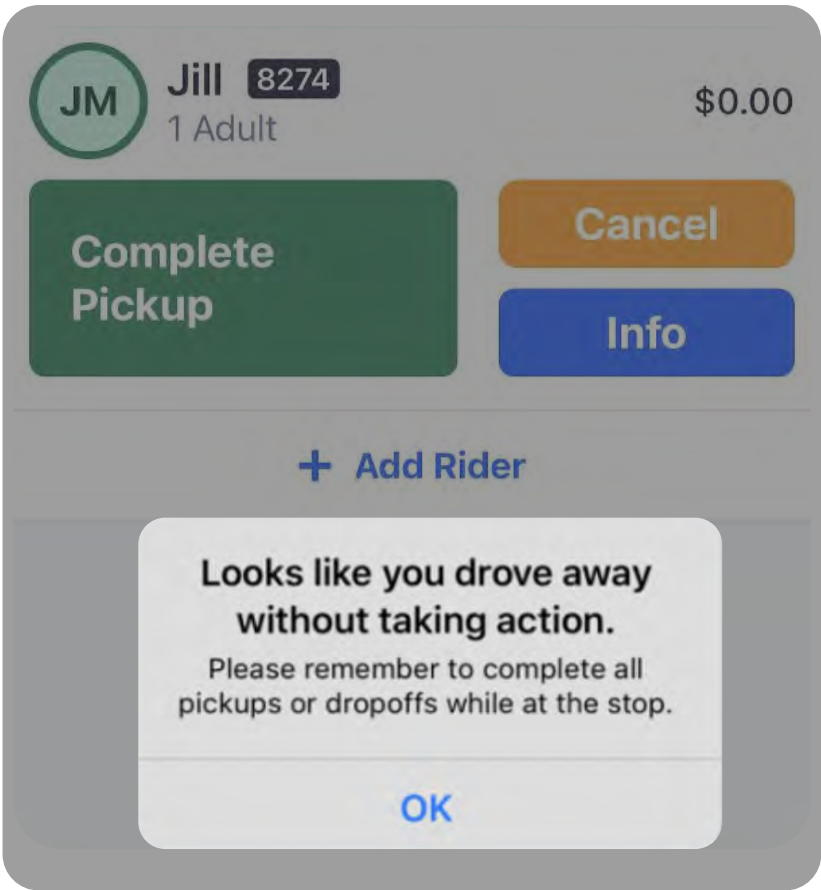
5 Confirm the pickup

Tap on the **“Complete Pickup”** button to confirm your rider is now on board.

Please make sure to come to a complete stop before completing your pickup or dropoff.



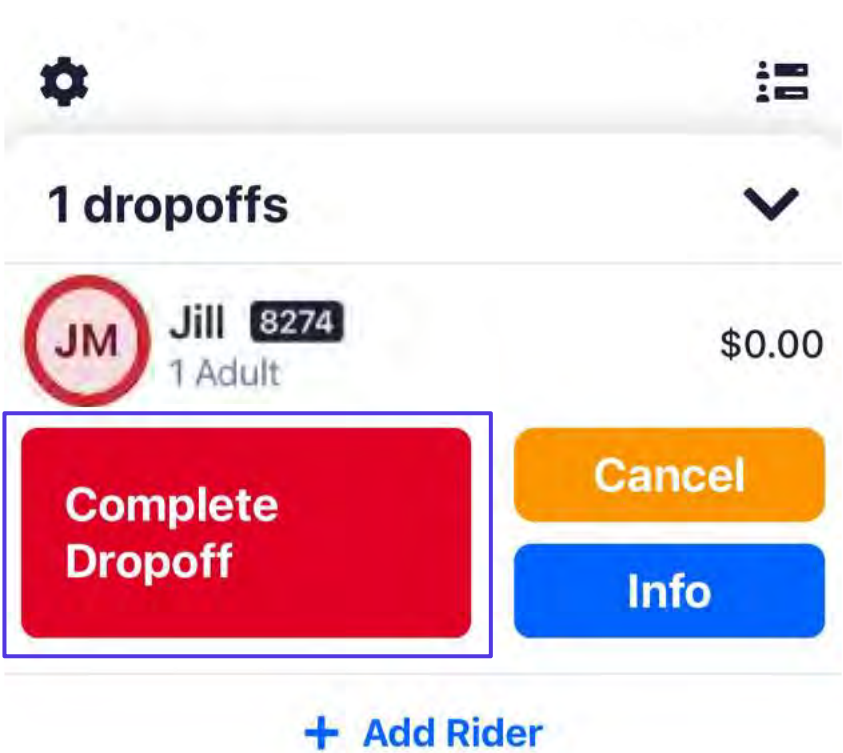
If you forget to complete your pickup or dropoff before leaving the stop, the system will notify you ↓.



6 Complete the dropoff

Once the pickup is marked as complete, follow the navigation to **navigate** to the dropoff location.

When you arrive at your destination and the rider has exited the vehicle, tap the **“Complete Dropoff”** button.



i When pooling several riders, pickups and dropoffs can come in a different order.

To avoid confusion, remember that trip pickup segments are marked in green, and trip dropoff segments are marked in red.

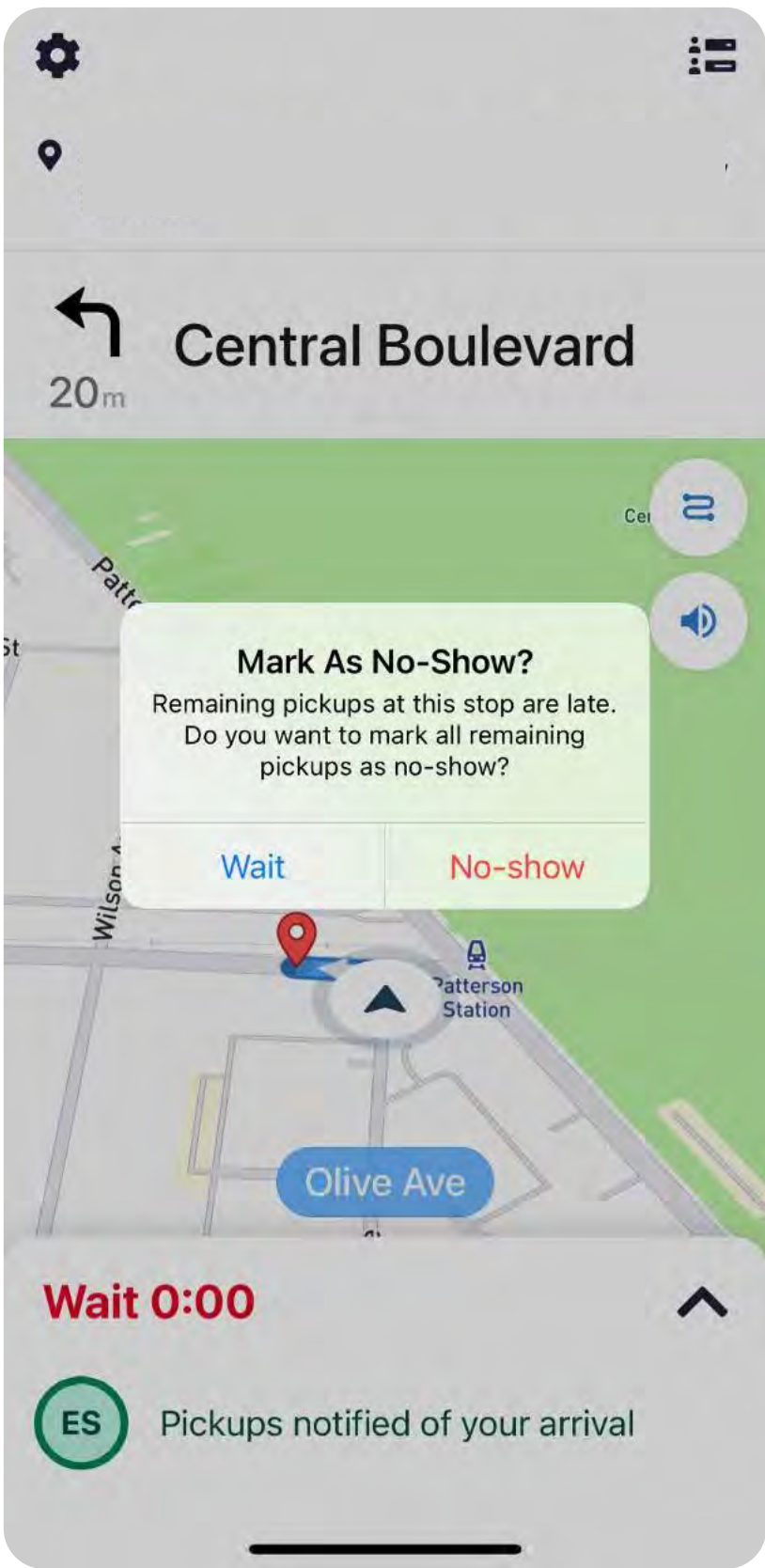
3.3. Trip Cancellation

This section gives an overview of how to cancel a trip due to a rider's No-Show or any other reason.

1 Mark as No-Show

When you arrive at your pickup location, a wait timer automatically begins. Once the timer has finished, the app will ask if you want to **No-Show Cancel** all of the remaining pickups at this stop **or extend the timer for another minute**.

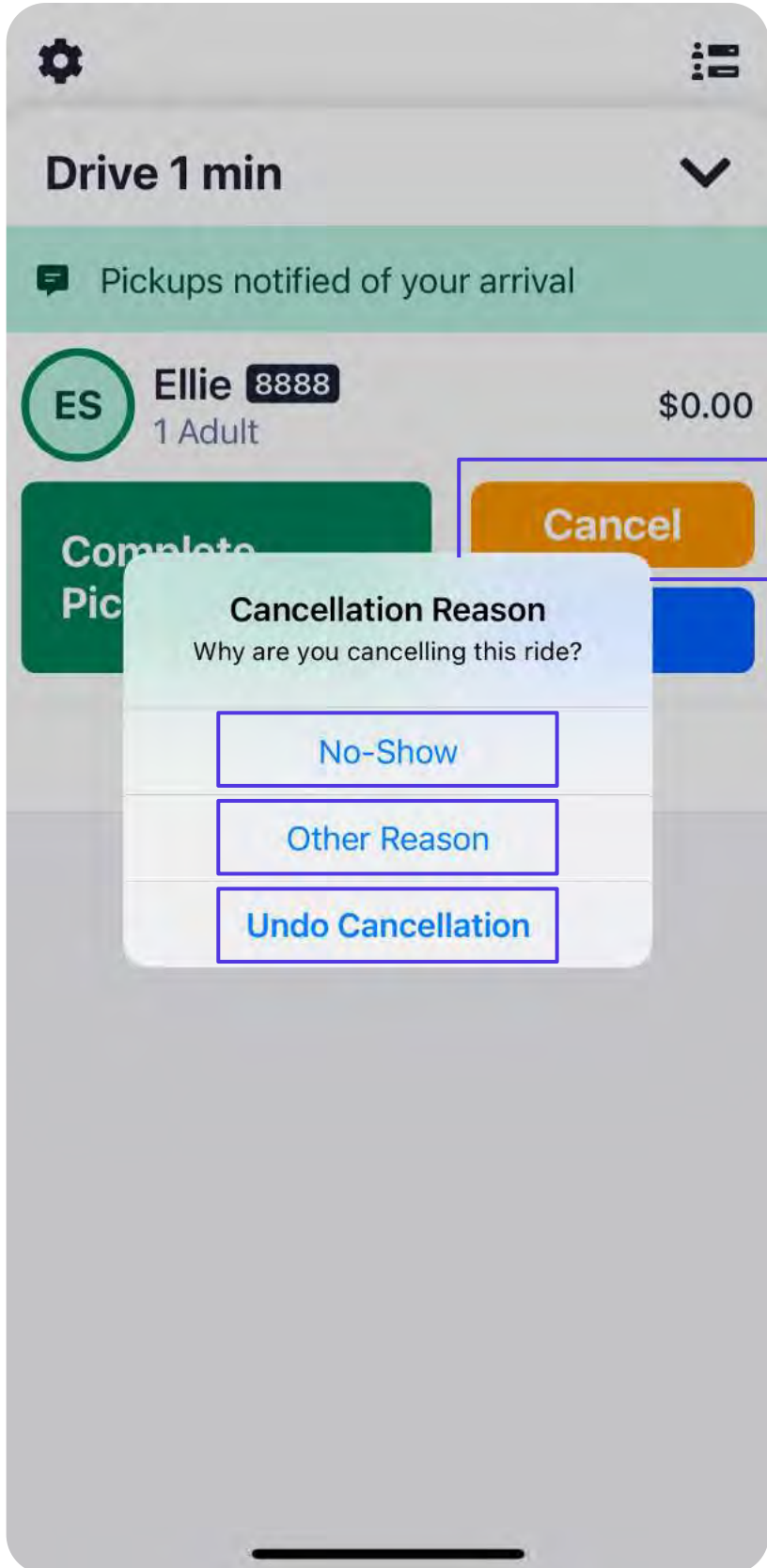
 Follow your organization's policy.



2 Cancel the Trip

To cancel a rider's trip from the action panel, tap **Cancel**. If you are canceling the trip because the rider isn't at the stop, tap **No-Show**. Otherwise, tap **Other Reason**. To go back, tap **Undo Cancellation**.

 Once the trip is canceled, the action cannot be undone.

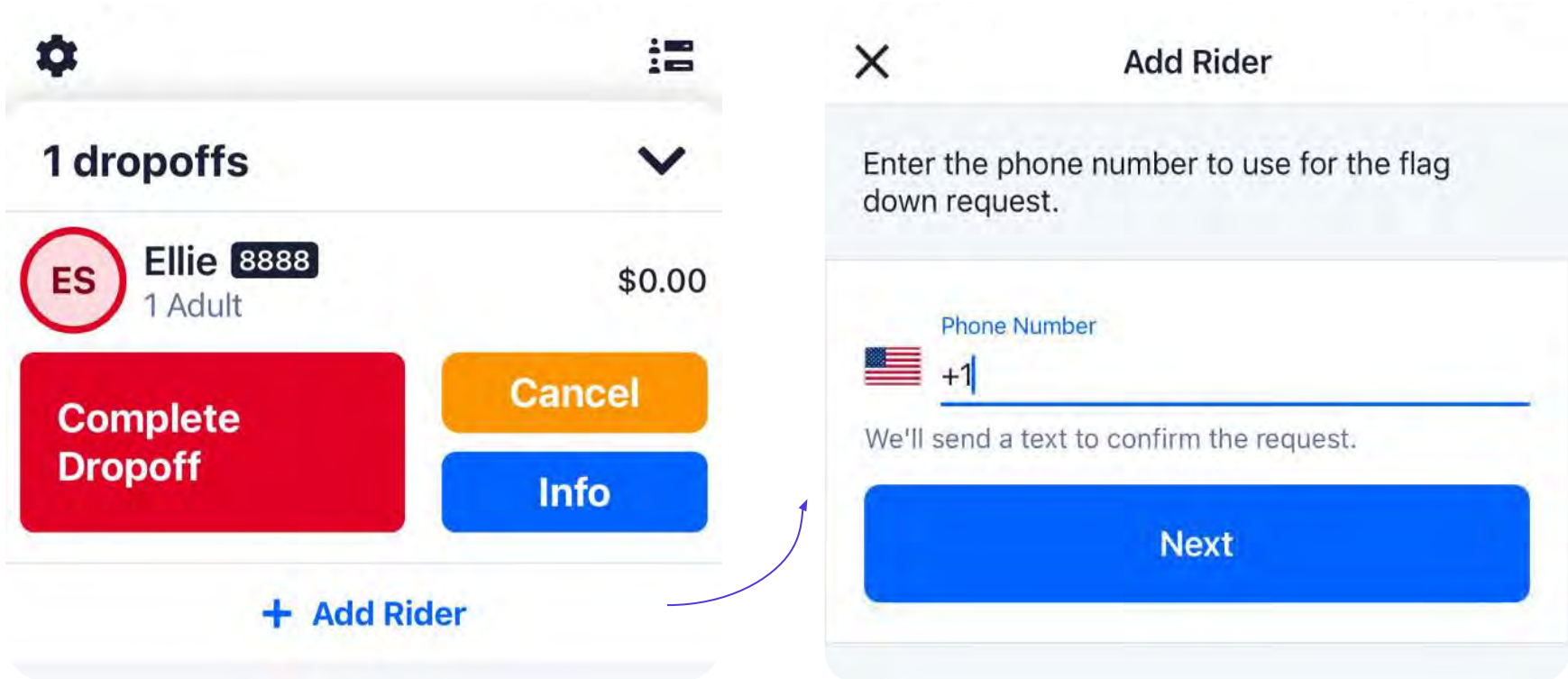


3.4. Adding a Walk-on Rider

In this section, you will learn how to add a Walk-On Rider at your pickup or dropoff location.

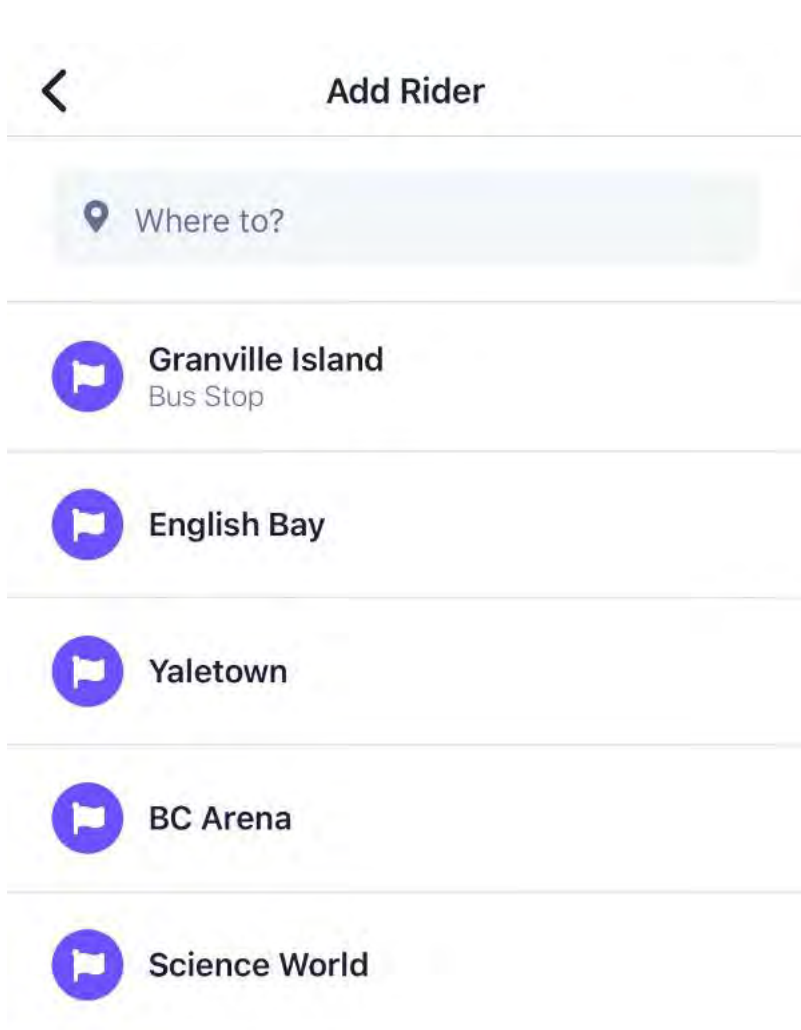
1 Add Contact Information

To add a walk-on passenger, tap **+ Add Rider** from the rider information card. Enter the **rider's cell phone number** and then tap **Next**.



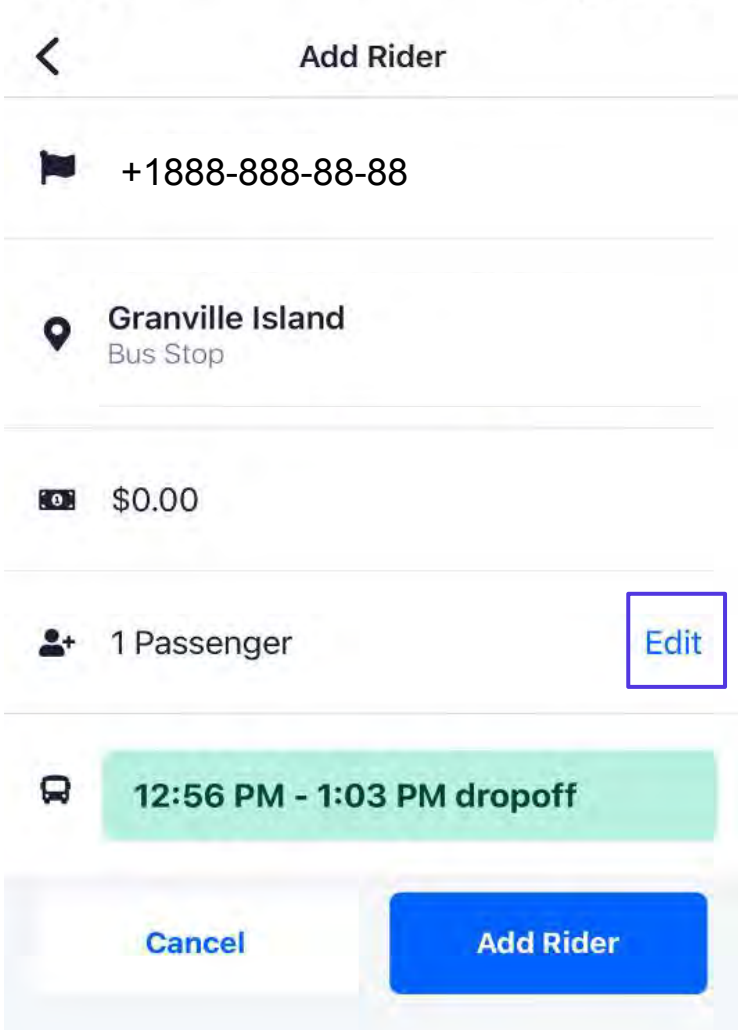
2 Add Destination

Enter the rider's destination in the **"Where to?"** bar and then tap on the address to confirm.



3 Edit Rider Information

Tap **"Edit"** to enter the number of riders. Tap **"Confirm Seats"** to update the information.



3.4. Adding a Walk-on Rider

4 Review the information and send the request

Add Rider

+1888-888-88-88

Granville Island

Bus Stop

\$0.00

2 Passengers

1:07 PM - 1:29 PM dropoff

Cancel

Add Rider

Review the rider information and dropoff address. Confirm the dropoff time with the passenger and tap **Add Rider**.

Your request will be then sent to see if the trip can be added to your itinerary without violating other trip flexibility windows and/or your duty end time.

5 Board the Walk-on Rider and Confirm Pickup

Add Rider

+1888-888-88-88

Granville Island

Bus Stop

\$0.00

2 Passengers

1:07 PM - 1:29 PM dropoff

Cancel Request

Confirm Pickup

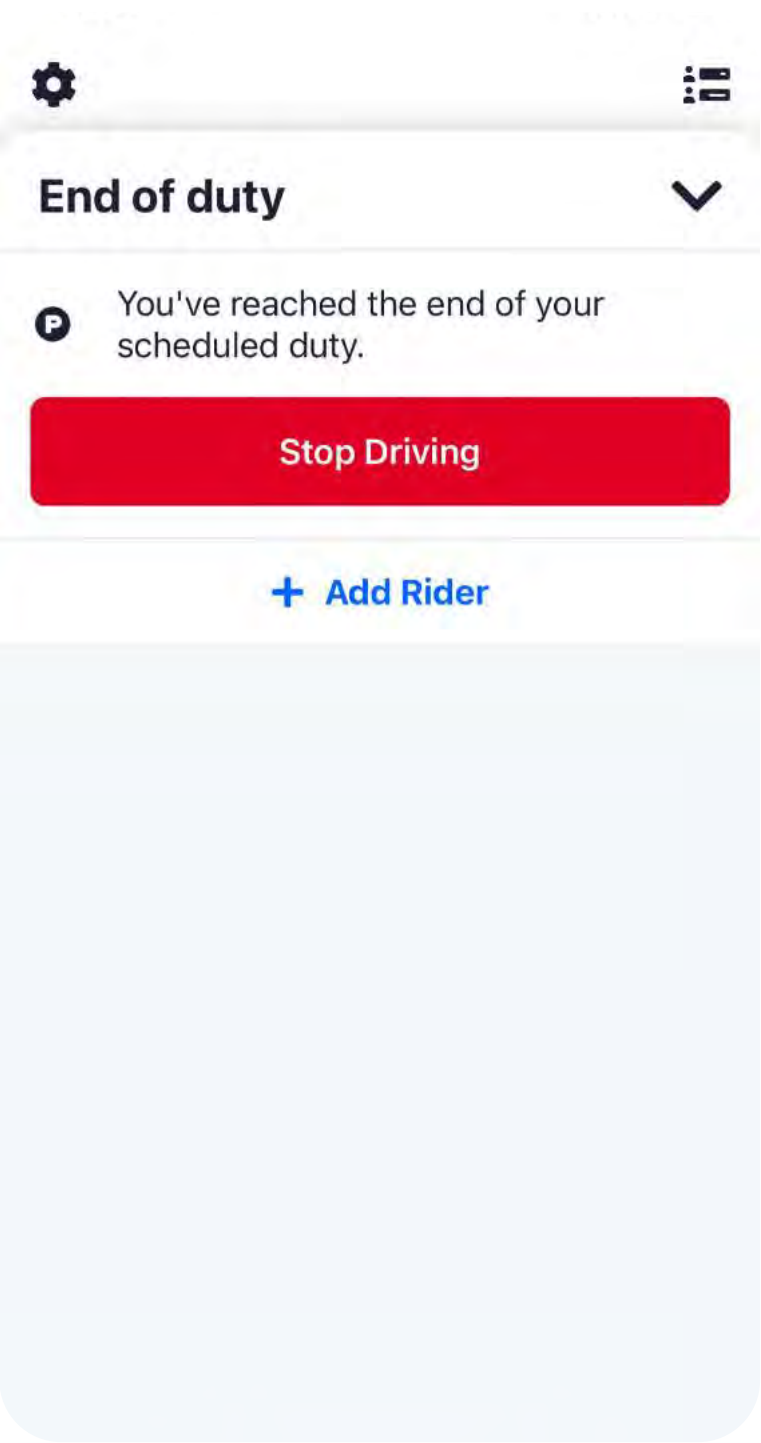
If the system identifies that adding a new rider is possible, a **“Confirm Pickup”** button will appear.

Board your walk-on rider and tap on the button to confirm their trip has started.



3.5. Ending your Duty

You made it! This section will tell you how to end your duty in the Spare Driver App.



When you near the end of your duty, you will be routed to your duty end location, and the “**Stop Driving**” button will appear.

You will be able to push the **Stop Driving** button once you have **cleared your manifest of all trips** and there is **less than 5 minutes** remaining until your duty end time.

When the button turns bright red, tap on it to end your duty.

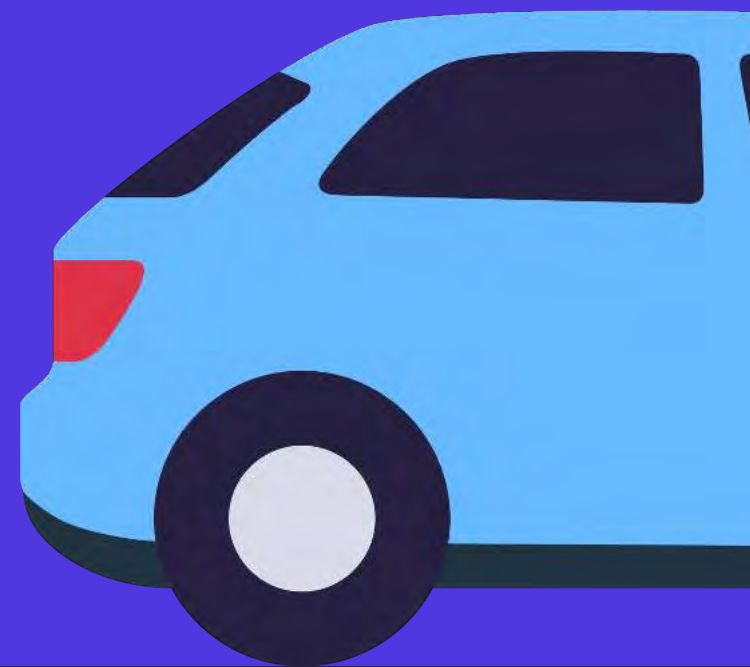
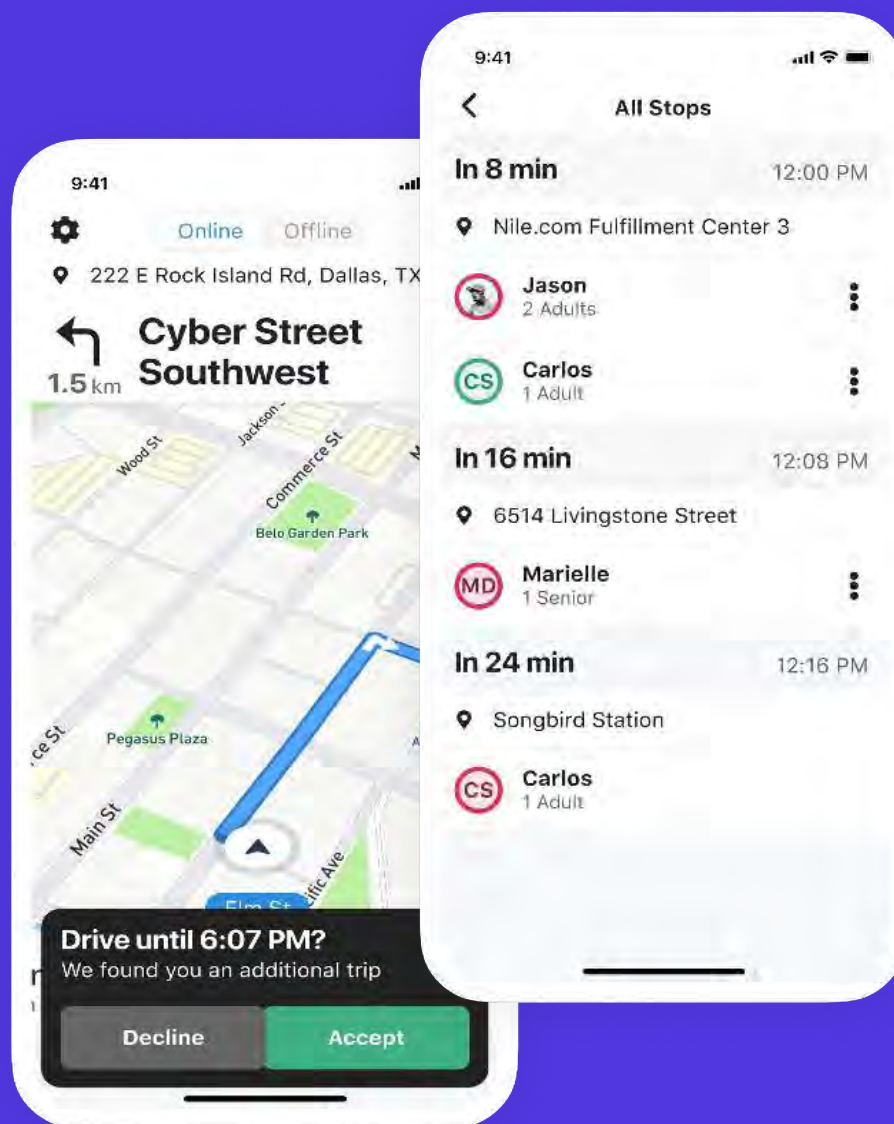
Note that a duty will **automatically end** if there are **no trips** left on the manifest and it’s **over 5 minutes past the end time**.



Please remember to follow any other procedures required by your administrator to complete your duty.

Please remember to **Sign out** of the Spare Driver App. You can do so by tapping the  icon at the top left corner of the main screen in the App and then selecting “**Sign Out**”.





Troubleshooting

→ When the App is not responding

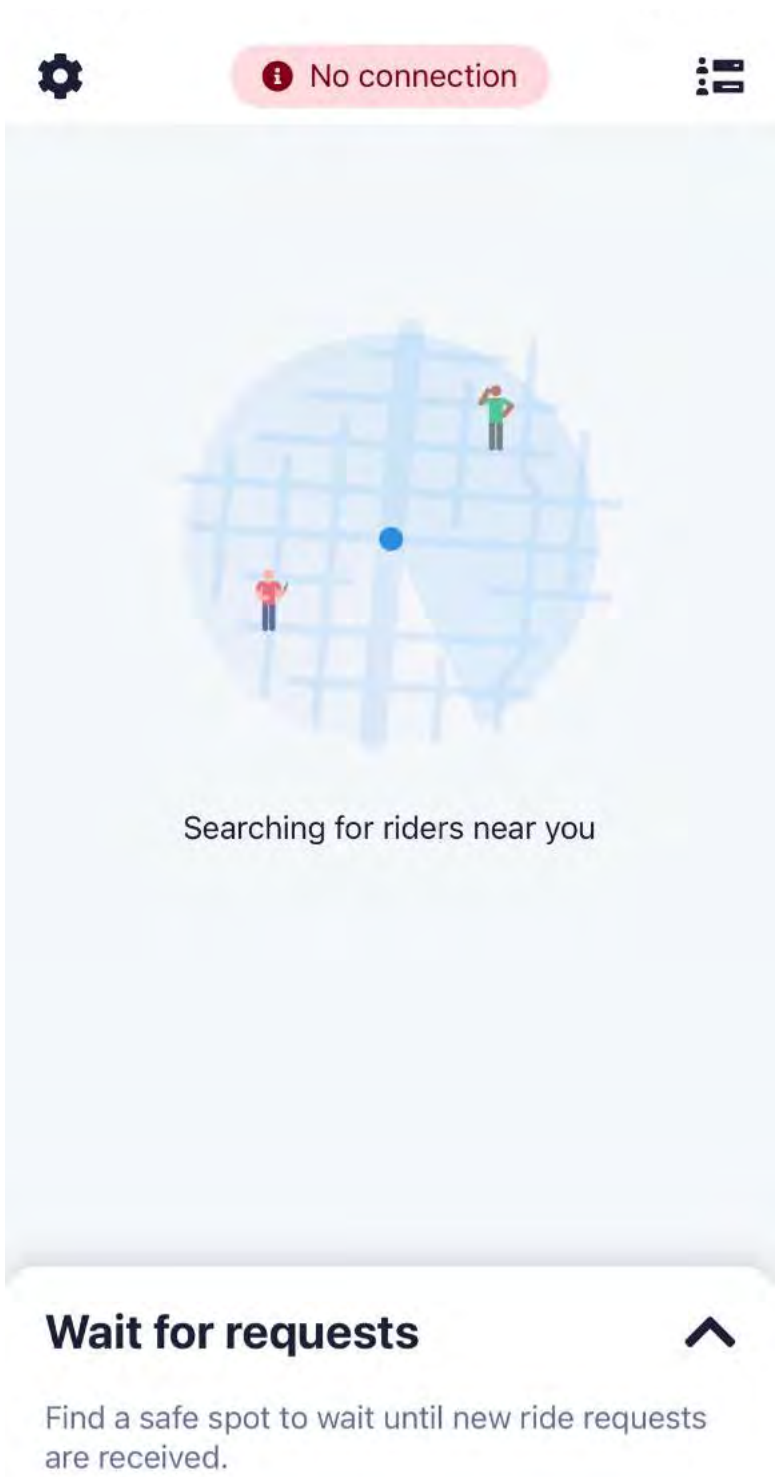
Troubleshooting

In this section, you will find ways to troubleshoot the Spare Driver App.

1 Check the Internet Connection

If your tablet/phone is not responding, it may be that you are no longer connected to the internet.

Look for the red **“No connection”** message at the top of the screen. This may mean that you have lost a cellular connection. Speak to your administrator.



 Remember you can also visit our help centre by tapping **“Help”** button in the **Settings** .

2 Reset the App

If for any reason the app is malfunctioning in any way, try restarting the app by closing it and reopening.

To close the app, swipe up from the bottom of the screen or double tap the home button of your device.

Next, tap and drag the Spare Driver app off the top of the screen to close it. After, find the app in the bottom dock and tap it to reopen it.

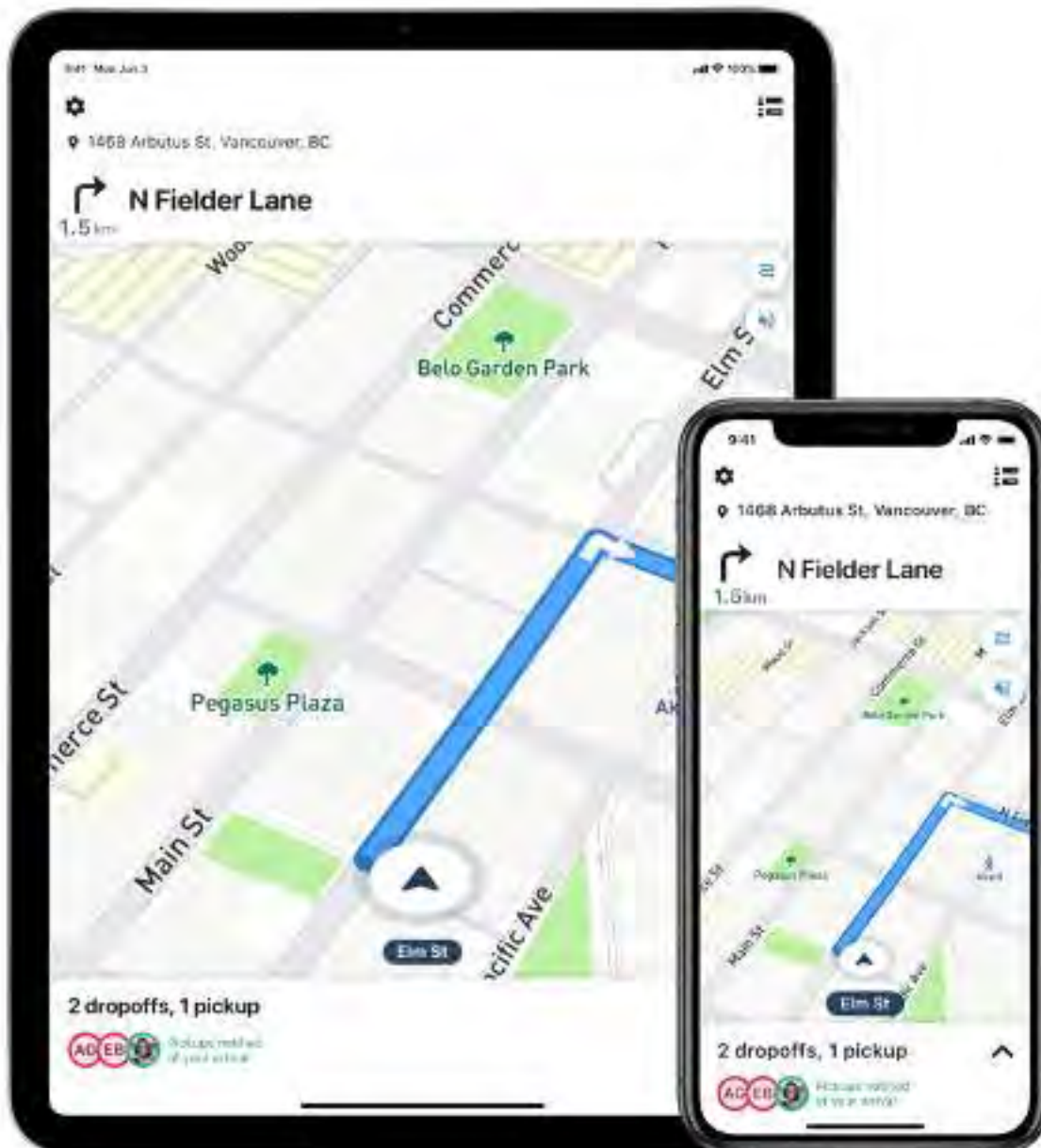
If that doesn't work, please contact your administrator.





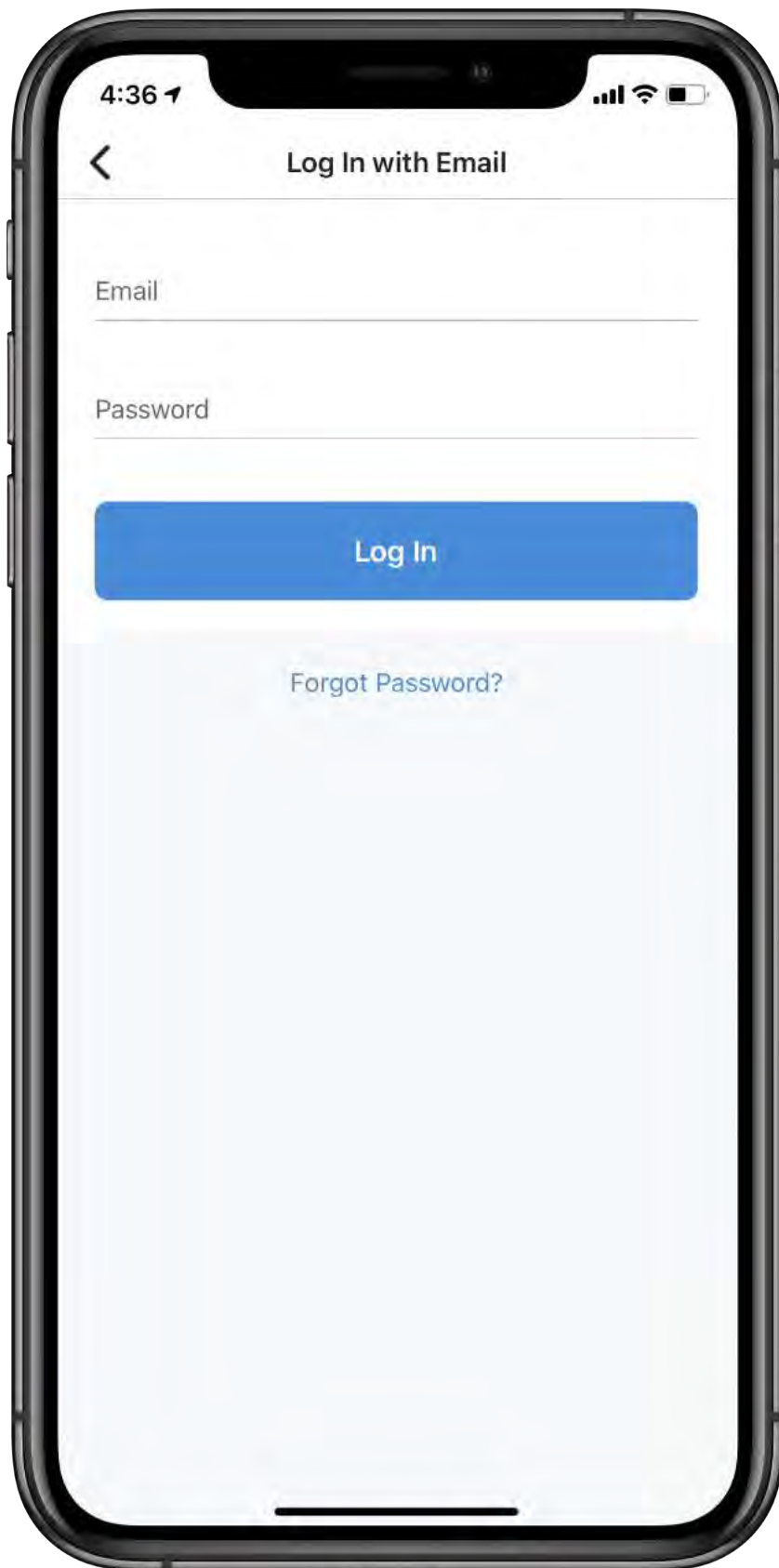
Spare Driver Reference Guide

Non-dedicated Edition

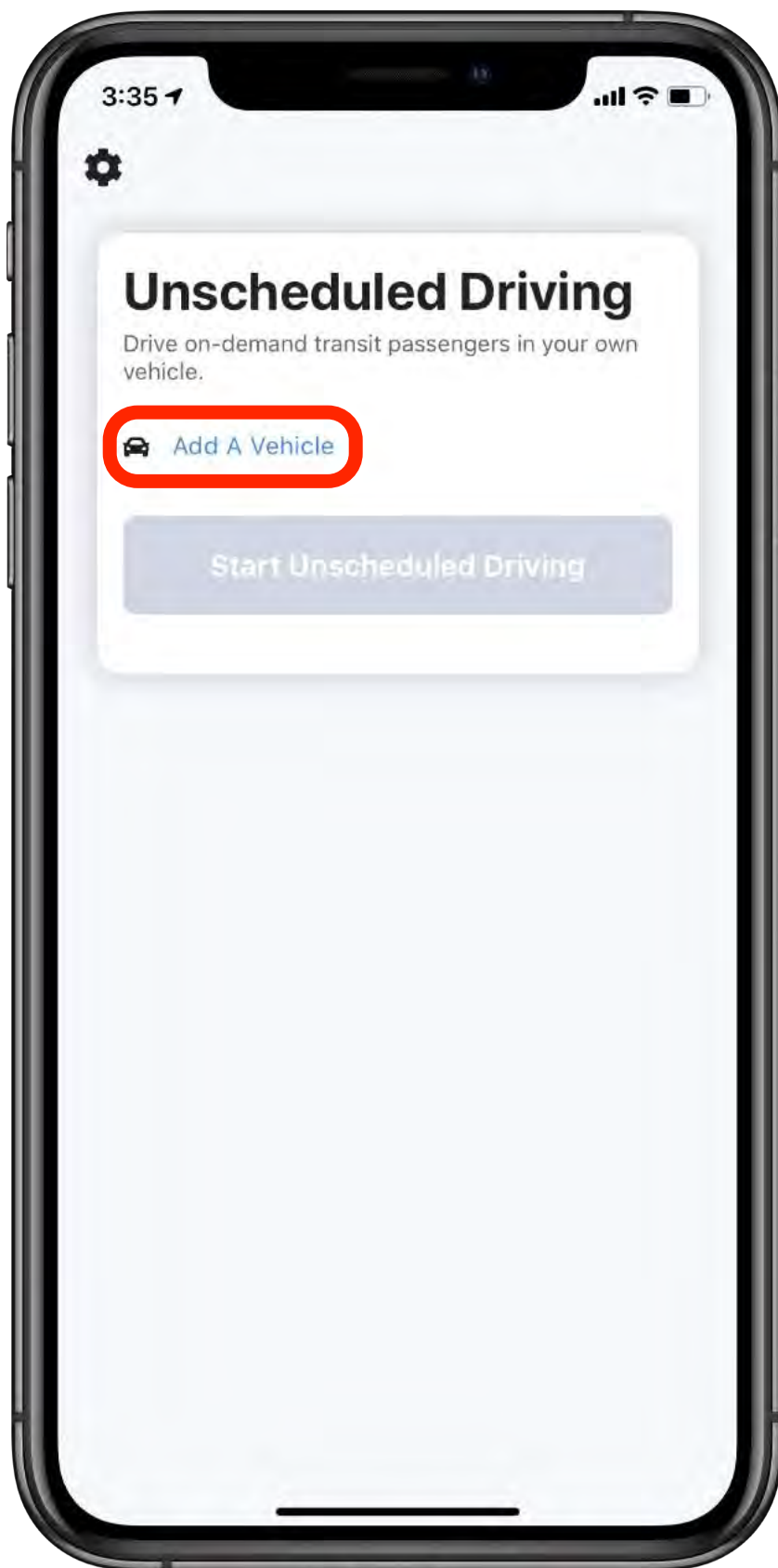




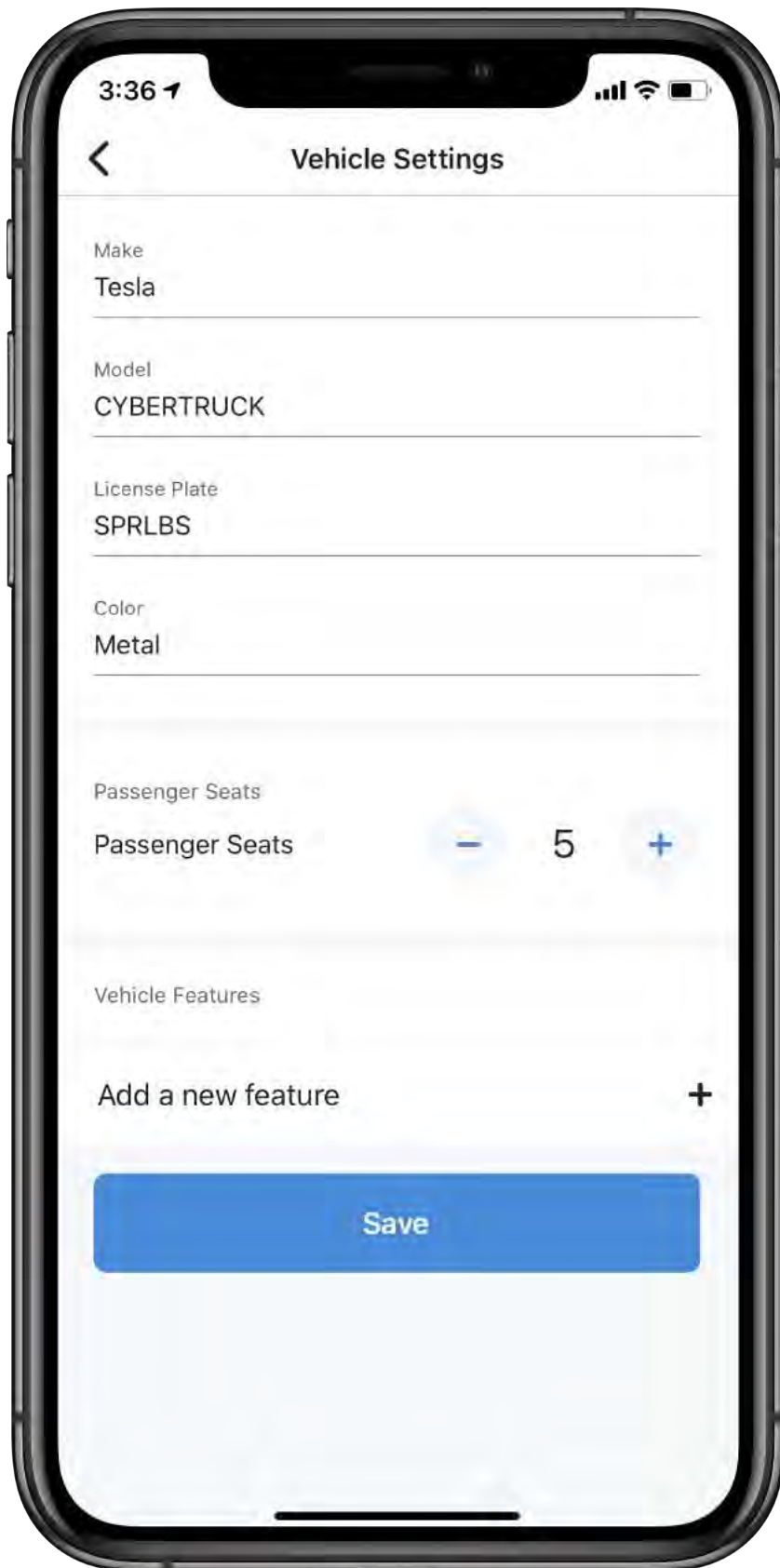
Open the Spare Driver app and tap Log In.



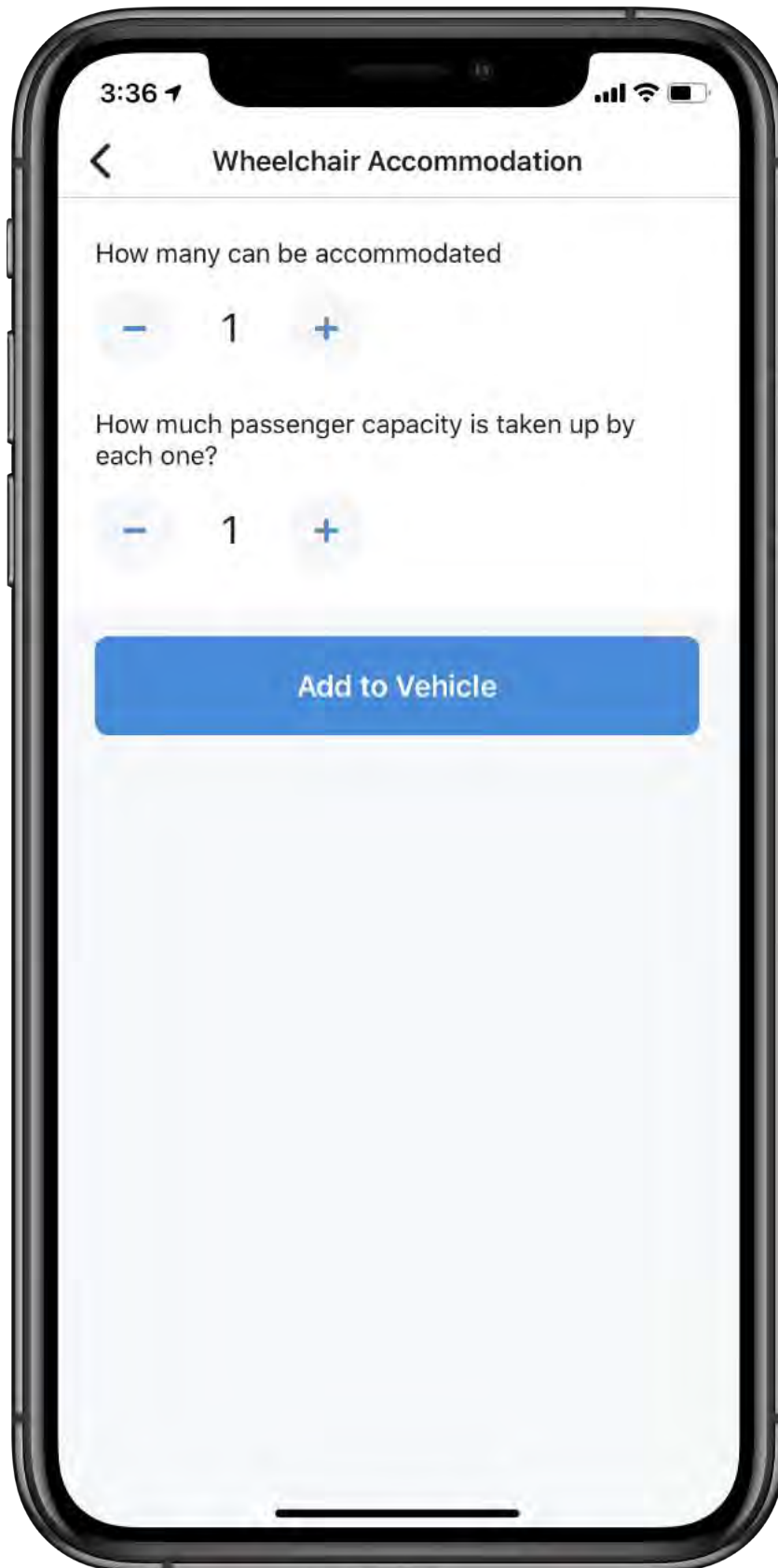
Enter your email address and password. If you don't have an account, contact your administrator.



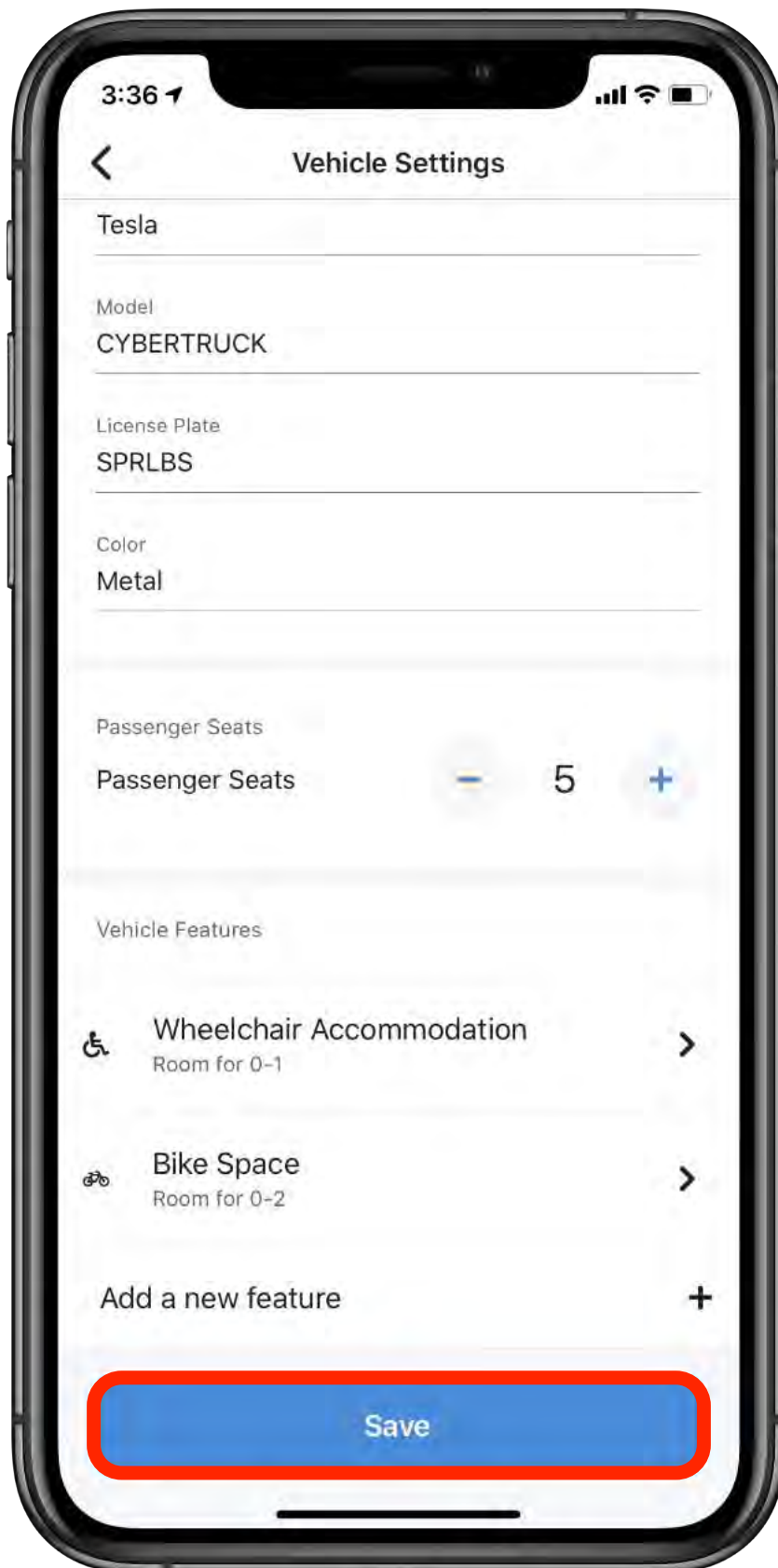
Click *Add A Vehicle*.



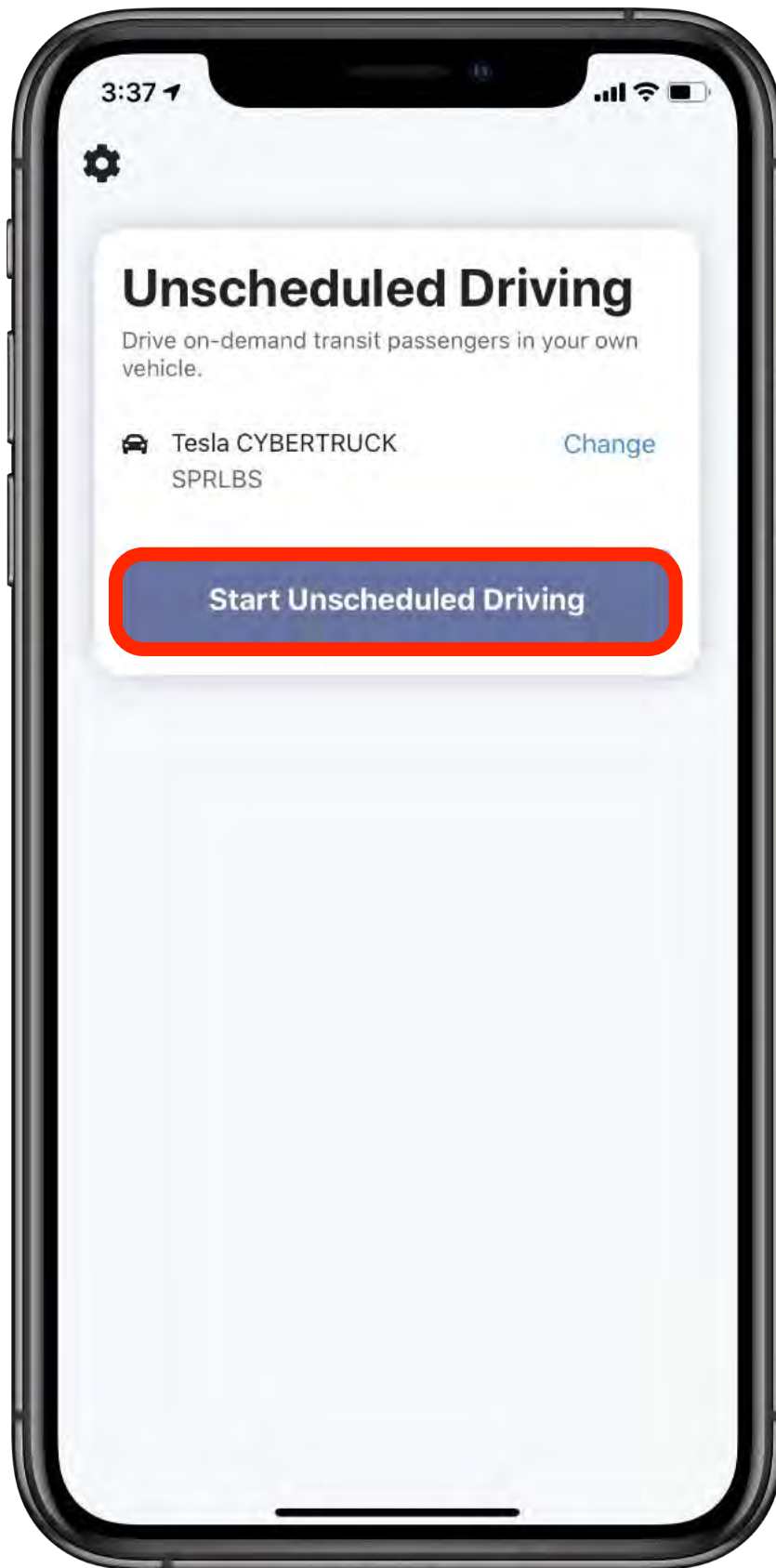
Fill in your vehicle's details, including the license plate and number of passenger seats.



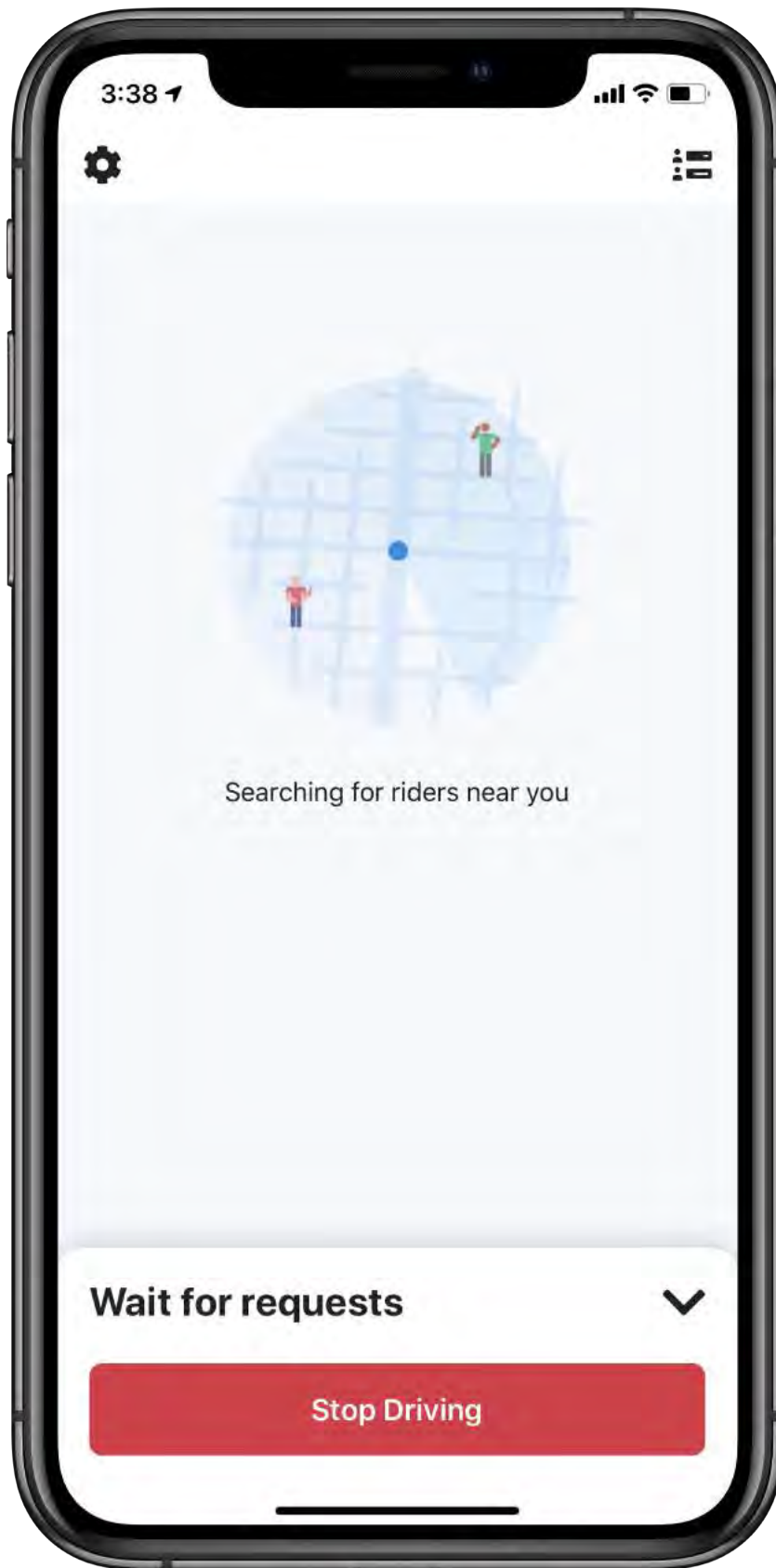
Enter in the accessibility devices your vehicle can accommodate and the number of passengers seats each device will remove.



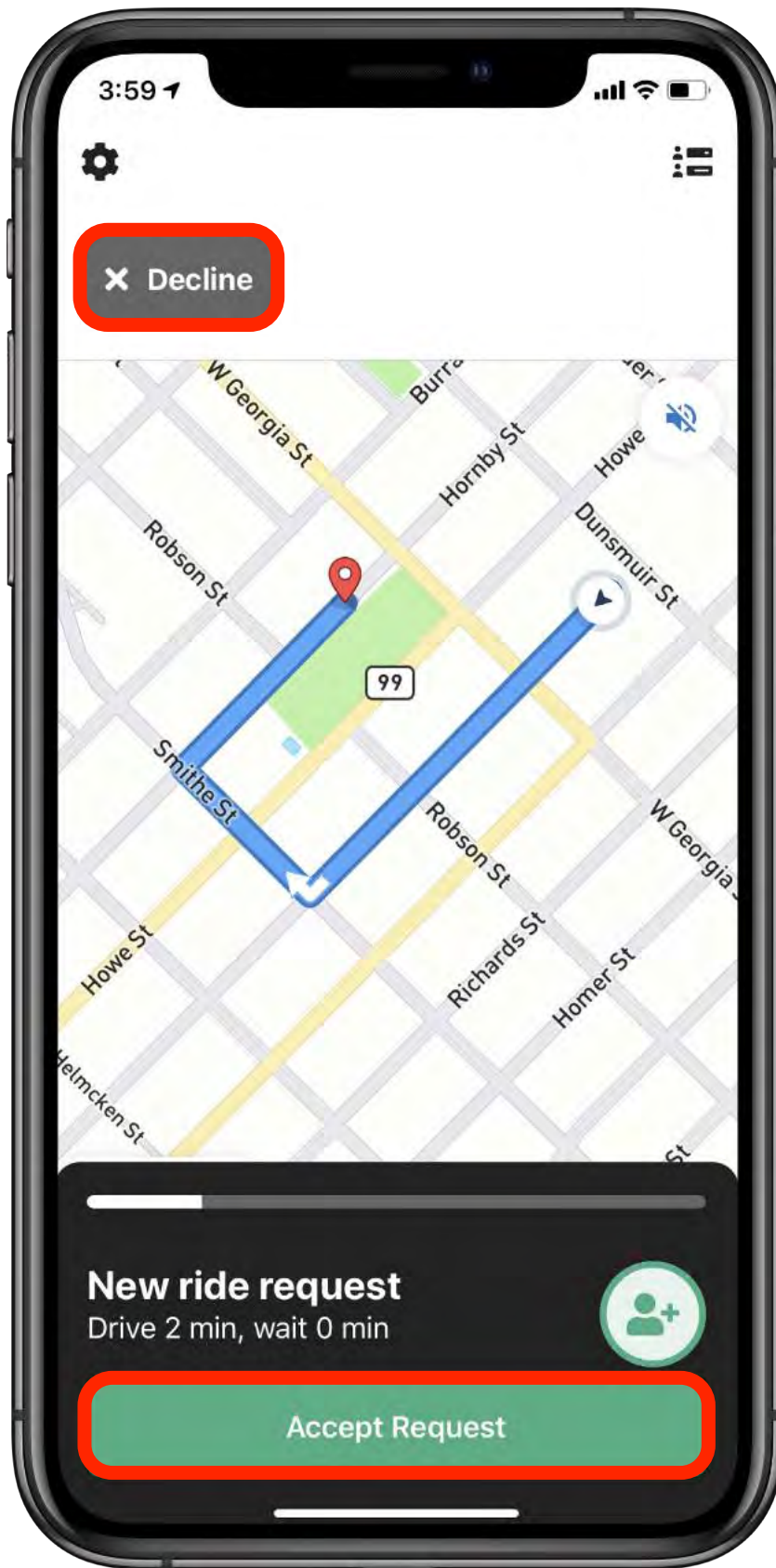
Hit Save when you're ready.



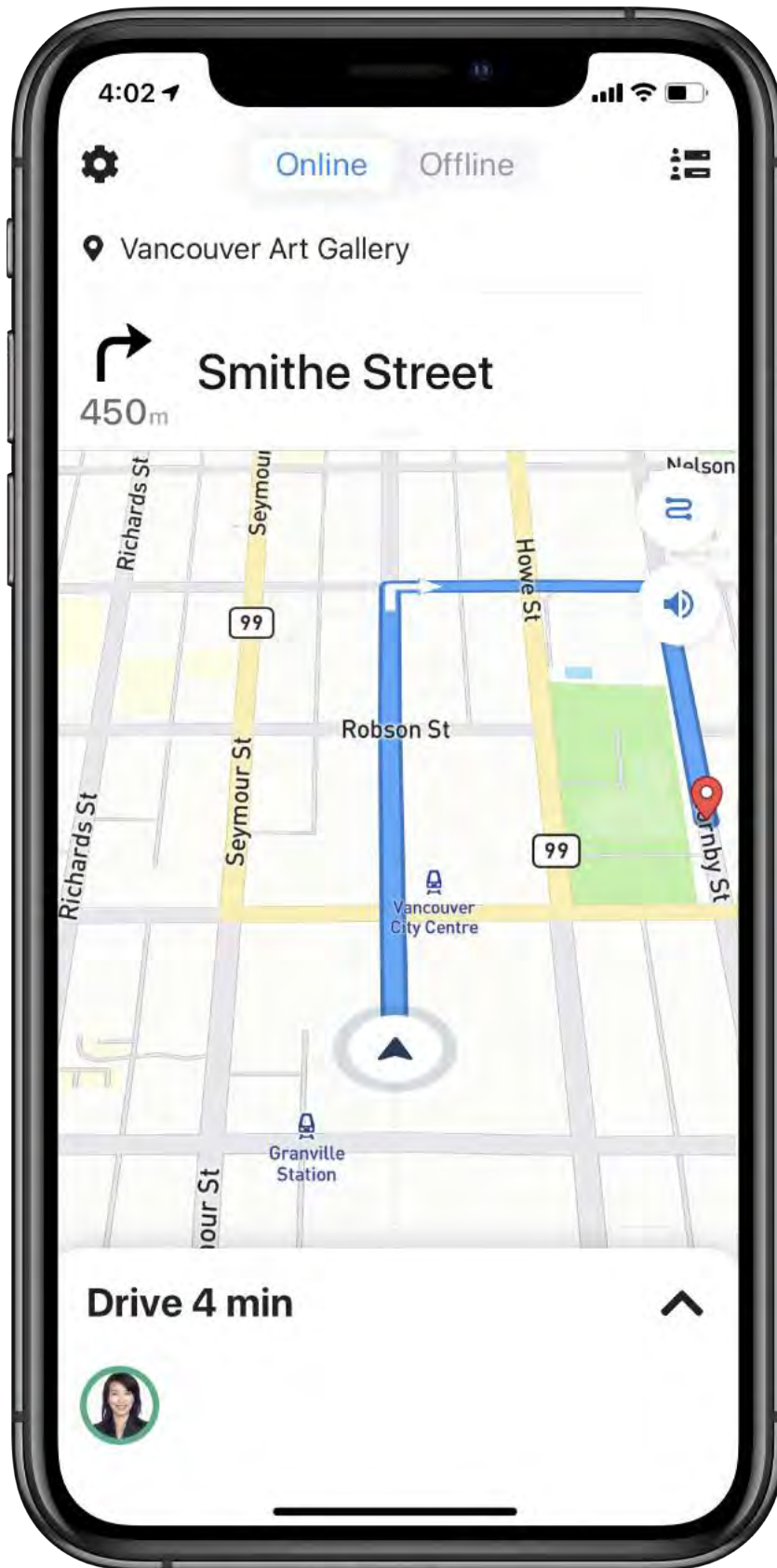
Tap "Start Unscheduled Driving" when you're ready to start being offered trips.



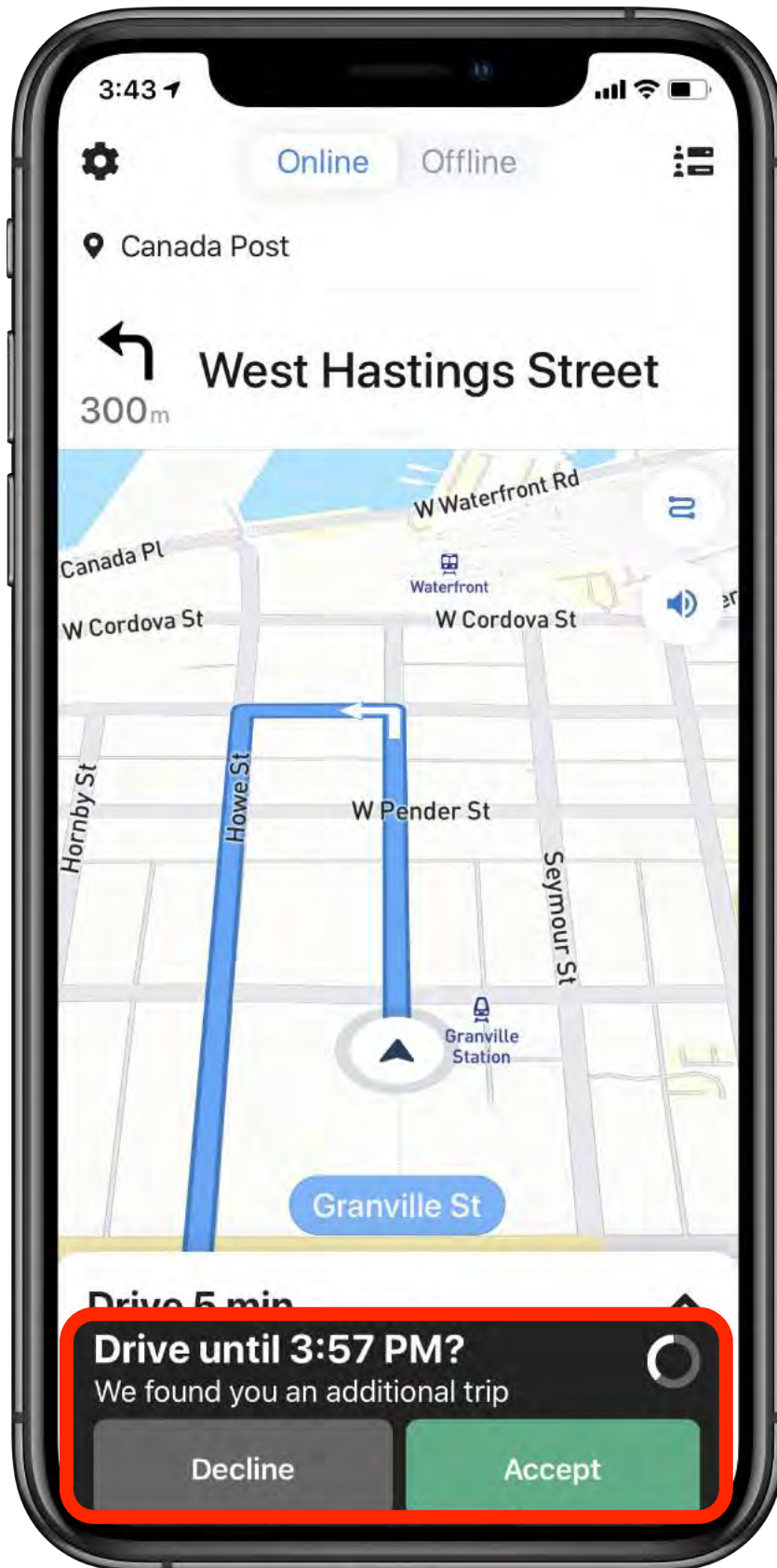
When you see this screen, wait for trip requests.



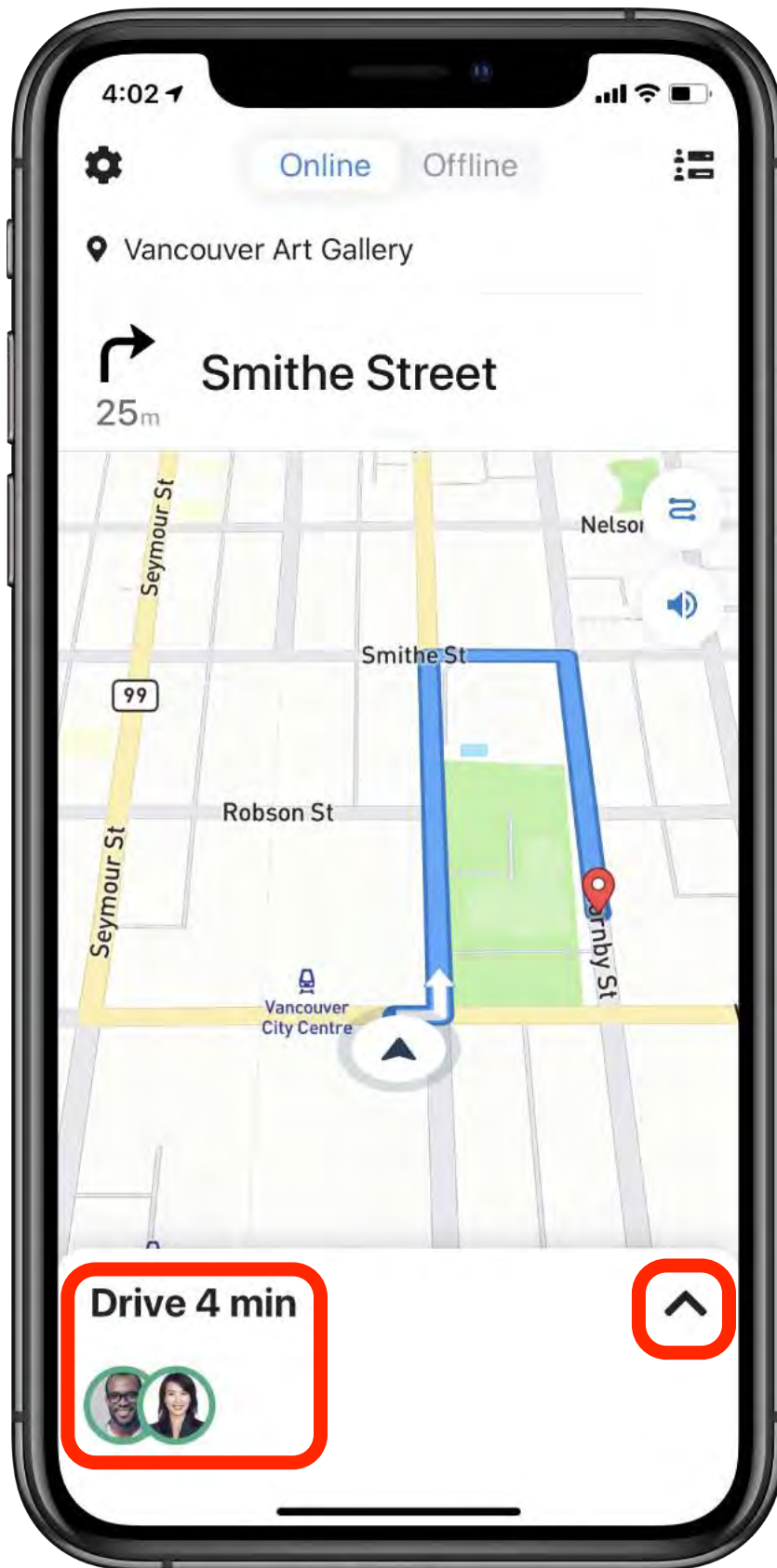
When a trip request is offered, you can either Accept or Decline the request. If the timer runs out, the trip will be offered to another driver.



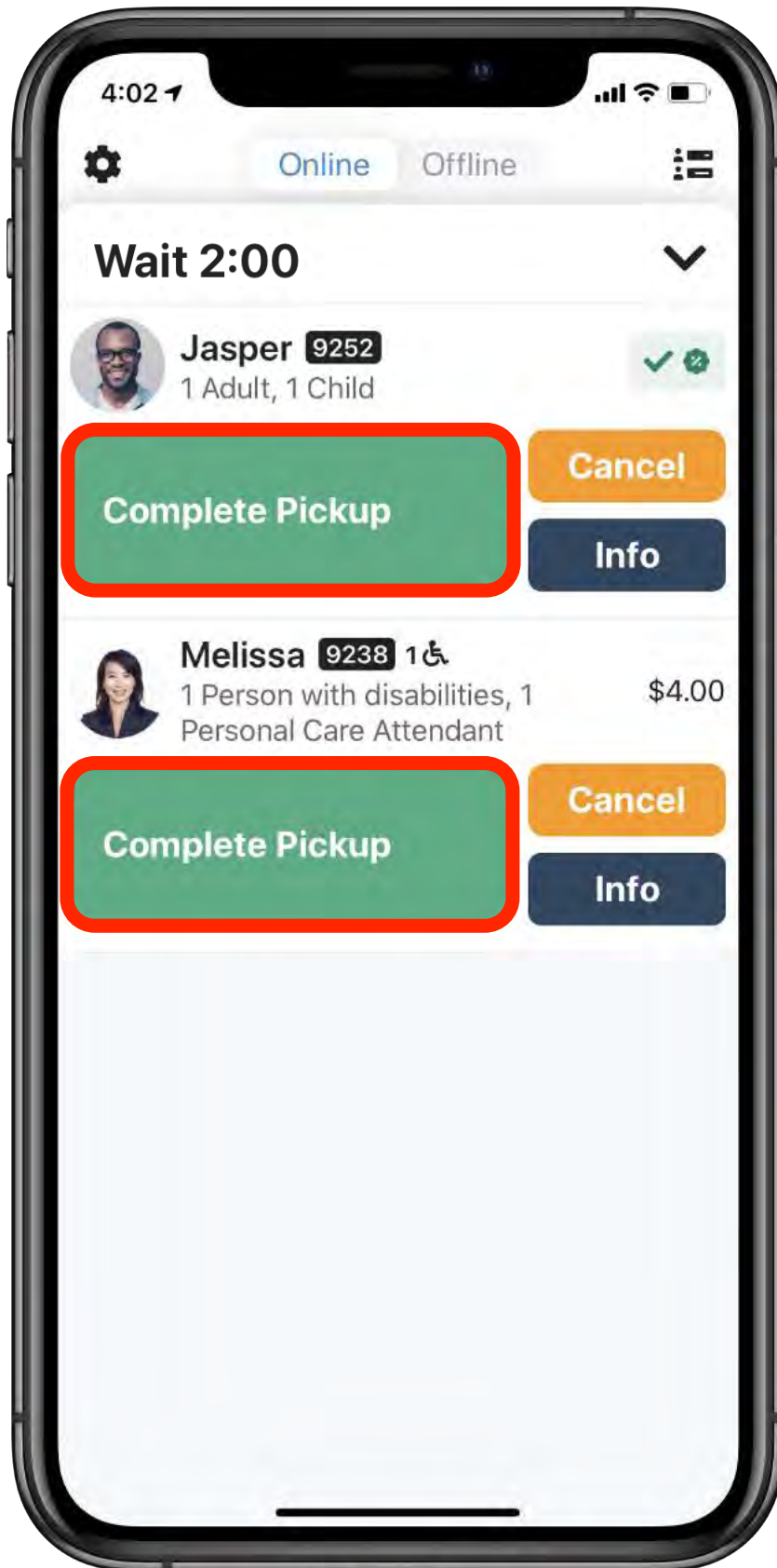
Now that you have a trip, follow the navigation.



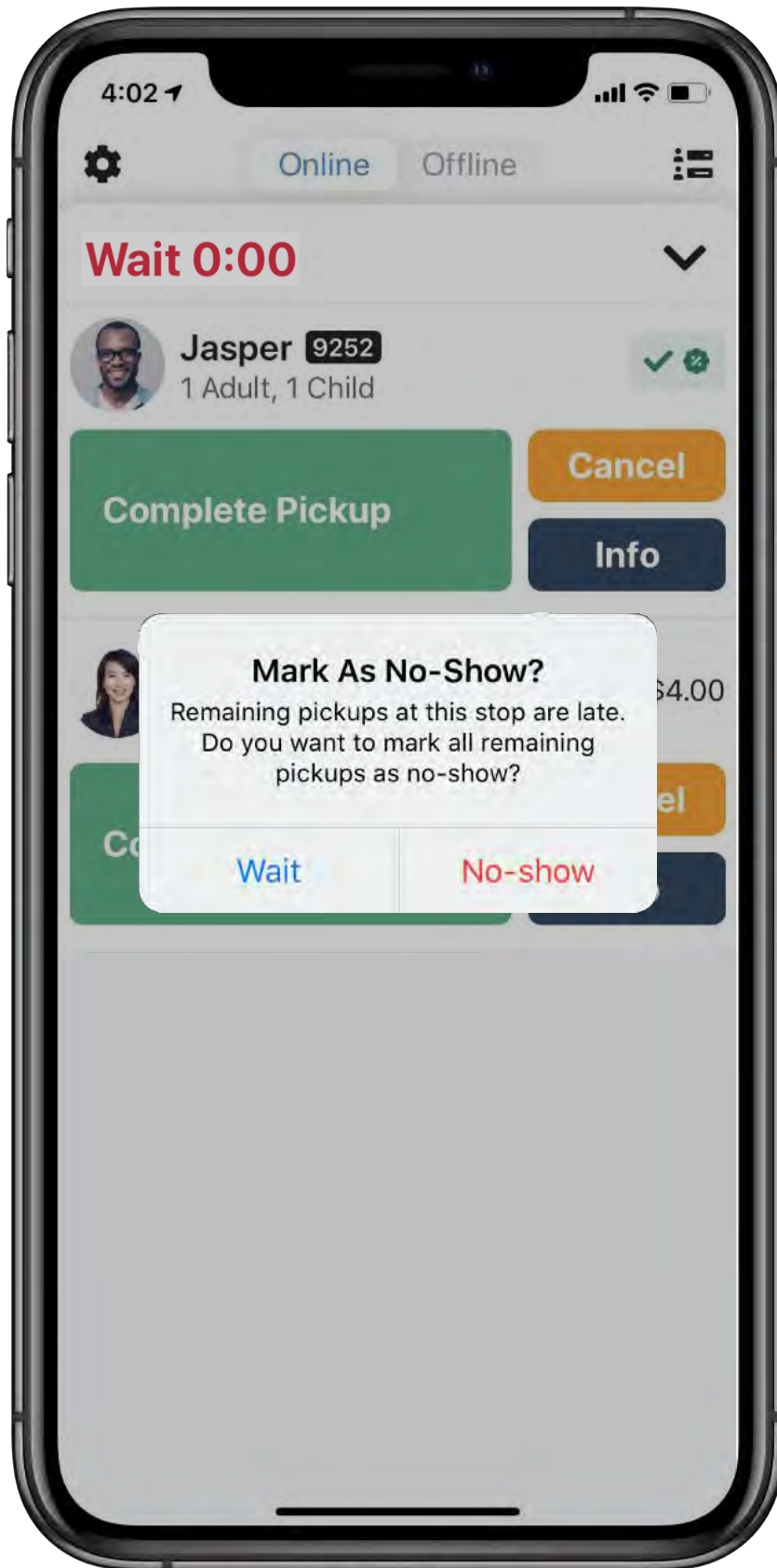
Additional trips can be offered to you while you're driving.
Tap **Accept** to add another trip to your manifest.



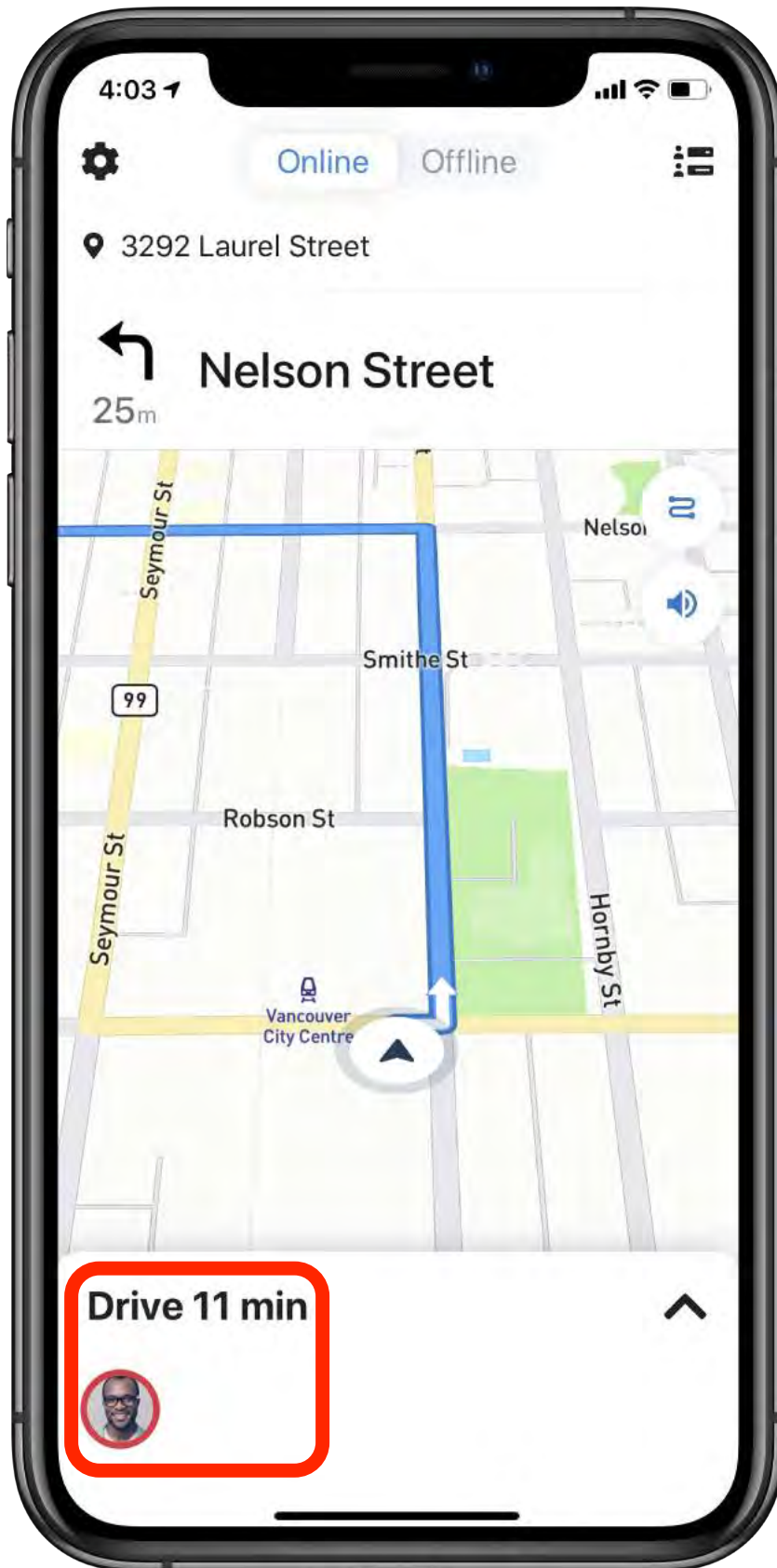
Now you have two pickups at your next stop.
Drive 4 minutes to the pickup location.



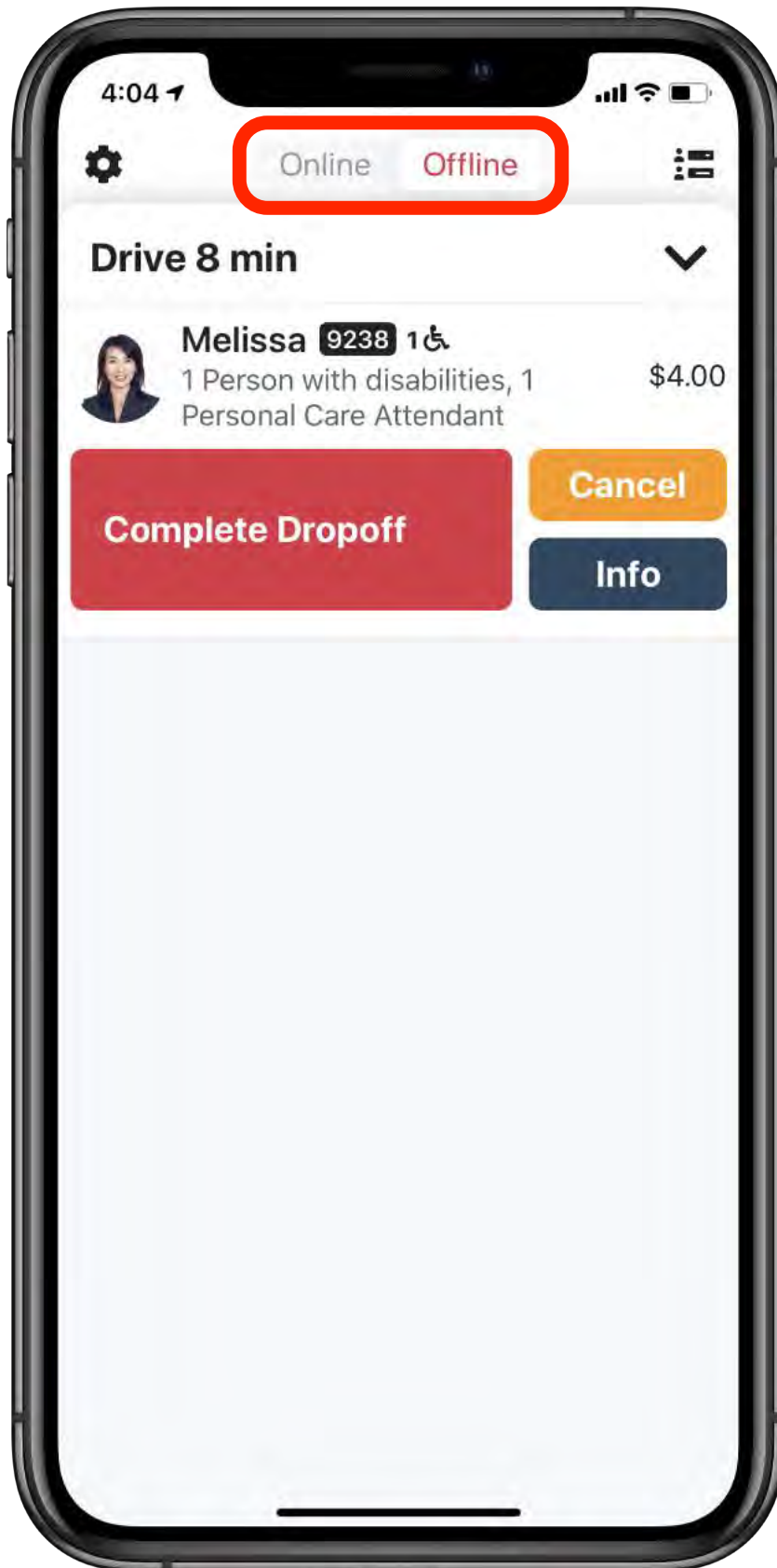
Once you arrive at the pickup location, the wait timer will begin.
Hit *Complete Pickup* to pickup your passengers.
If a fare is displayed, collect payment from the rider.



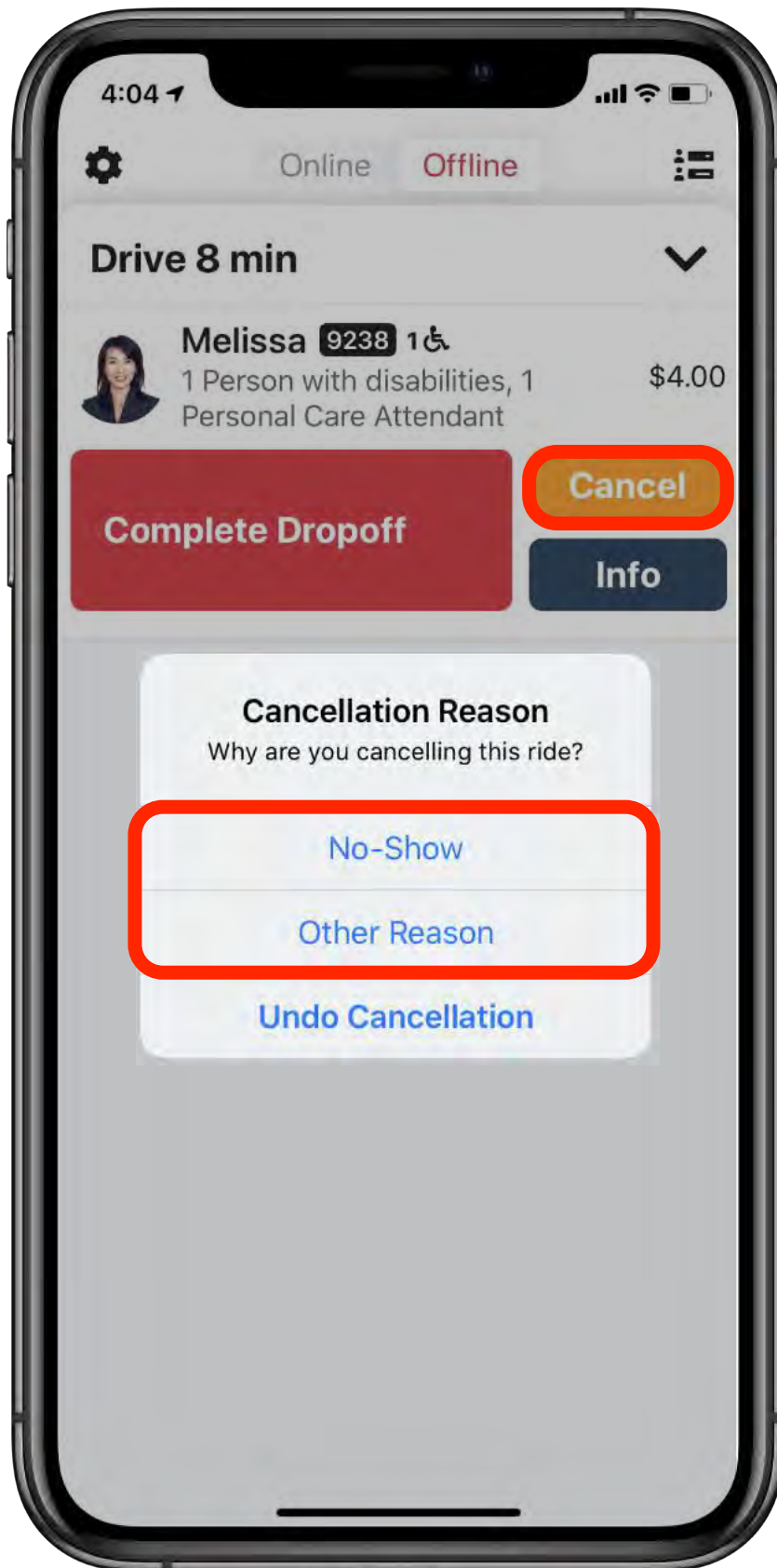
Once the timer runs out, it will ask you to wait longer or no-show all remaining passenger pickups. Hitting *Wait* will add another minute to the timer.



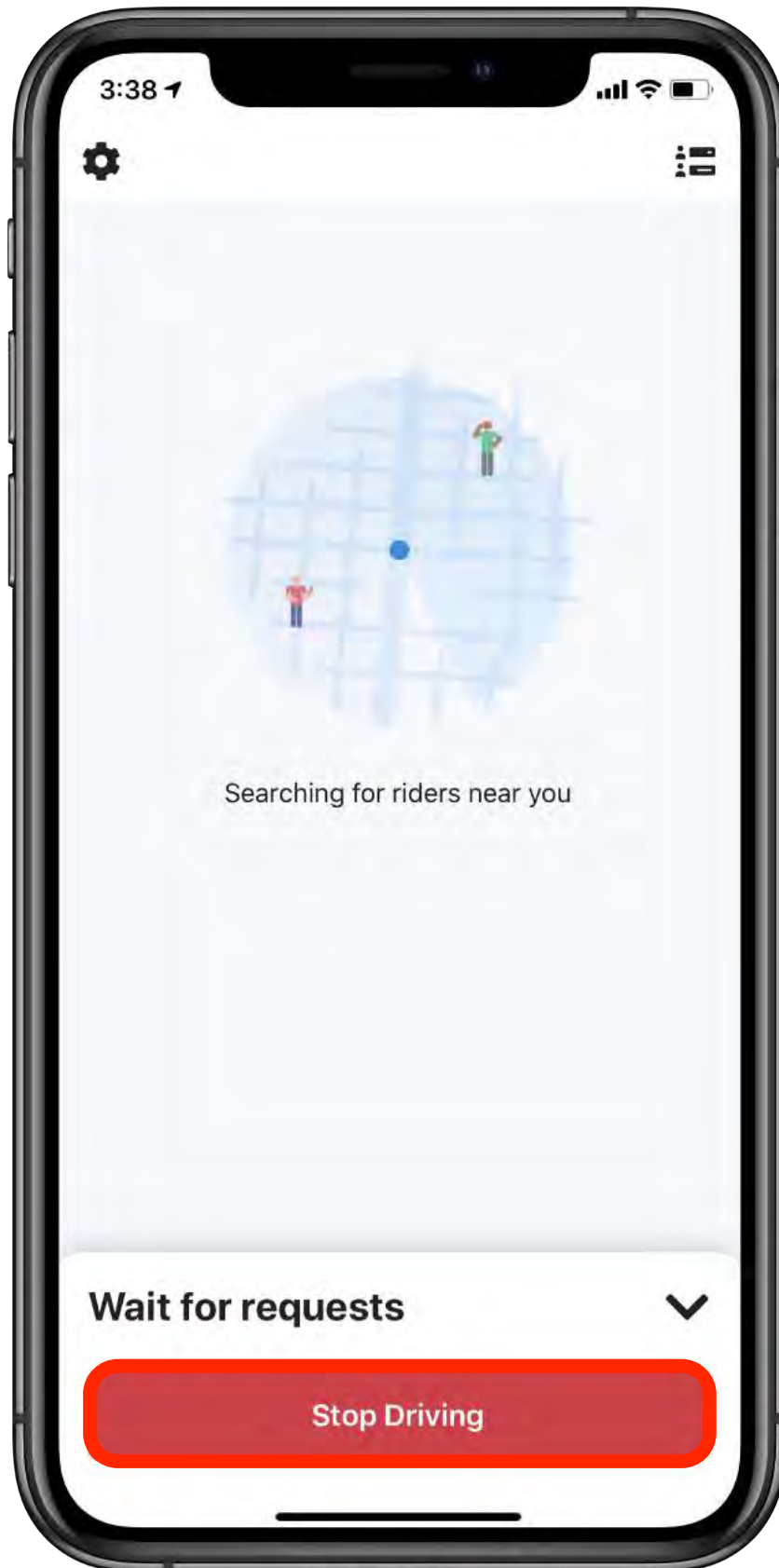
Once on board, drive your riders to their dropoff location(s).
Dropoffs will be shown in red.



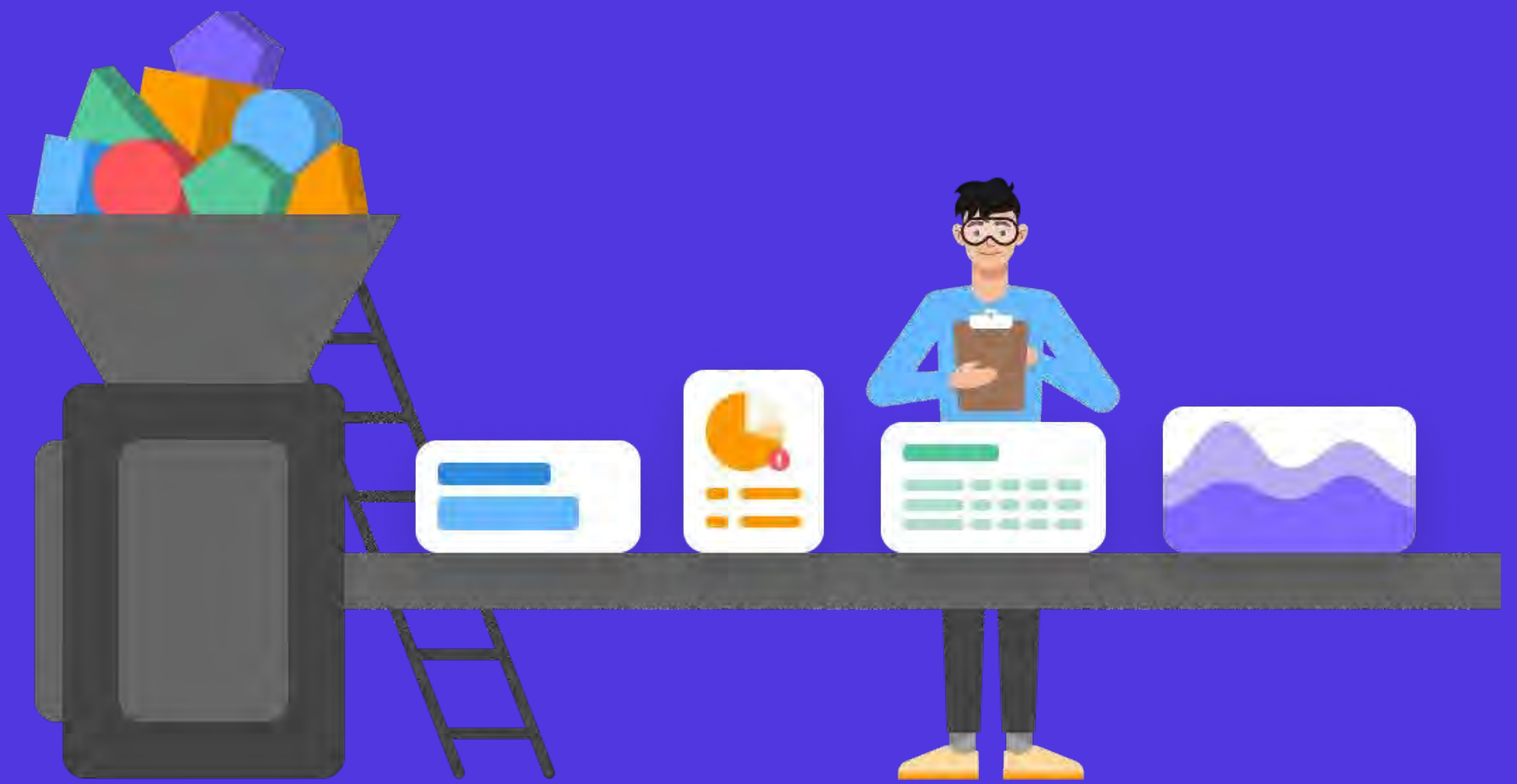
Tap *Offline* at the top to stop receiving trip requests.
Similarly, tap *Online* to start receiving trip requests.



If you need to cancel a passenger's trip, hit *Cancel* and provide the reason for the cancellation.



Once you have no more trips on your manifest, you can hit *Stop Driving* to go offline.

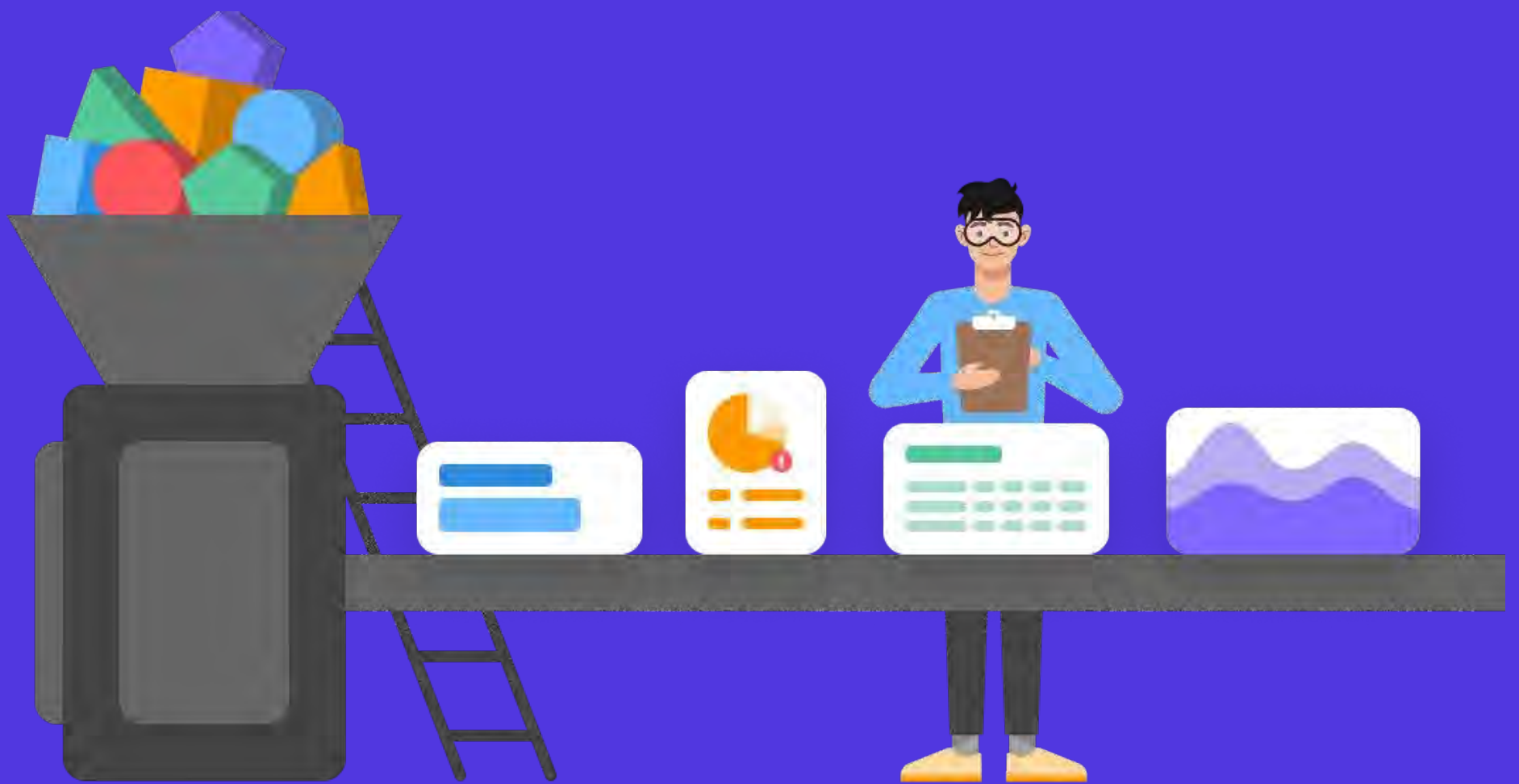


Spare Admin Data Guide

Visit sparelabs.com
815 W Hastings St Suite 810,
Vancouver, BC V6C 1B4
© Spare 2022

Table of Contents

- 1. Navigating Around Spare Platform..... 3**
 - 1.1. Accessing Your Account..... 4
 - 1.2. Spare Launch Dashboards Overview..... 5
 - 1.2. Spare Analyze Dashboards Overview..... 6
- 2. Service Analytics 7**
 - 2.1. Access Service Data..... 8
 - 2.2. View Ridership Data..... 9
 - 2.3. View Users Data..... 12
 - 2.2. View Rider Experience Data..... 13
 - 2.2. View Charges Data..... 14
- 3. Fleet Analytics 15**
 - 3.1. Access Fleet Data..... 16
 - 3.2. View Vehicles Data..... 17
 - 3.3. View On-Time Performance Data..... 19
- 4. Reporting 20**
 - 4.1. Access and Download Reports..... 21
 - 4.2. Build Custom Reports..... 23
 - 4.3. Set Up Automated Reports..... 25
- 5. Report Metrics Cheat Sheet 26**
 - 5.1. Ridership Metrics..... 27
 - 5.2. NTD Metrics..... 32
 - 5.3. Duty Metrics..... 33
- 6. Help and Troubleshooting..... 35**
 - 6.1. How to Reach out for Support..... 36



[1] Navigating around Spare Platform

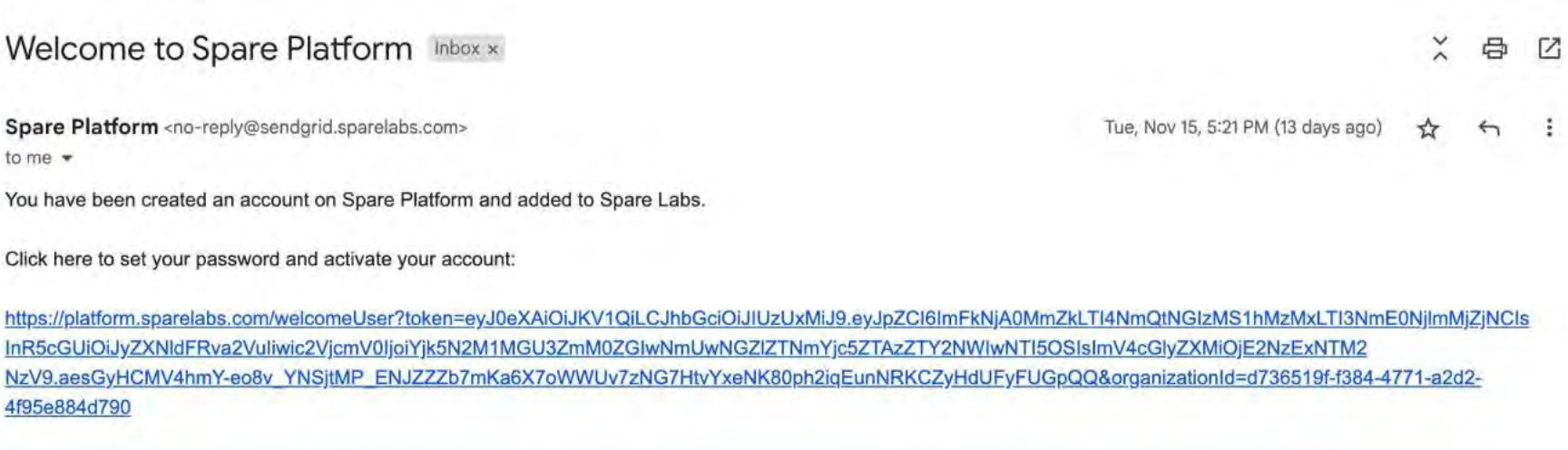
- Spare Platform Login Information
- Spare Launch Dashboards Overview
- Spare Analyze Dashboards Overview

1.1. Accessing your Account

1 Setup your account

You should have received an invitation email from sparelabs.com.
An invitation link will redirect you to the Spare Platform and the account setup.

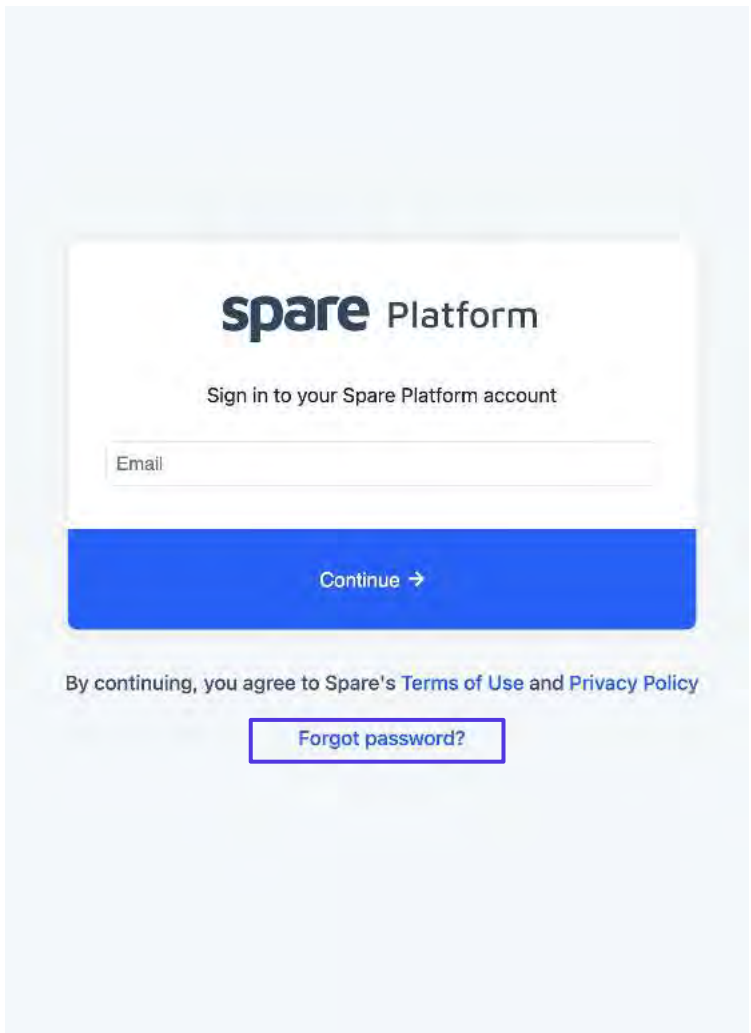
You can log into your account via your email and a password you will set the first time.



 Please contact your **administrator** if you don't have login credentials or did not receive a registration email.

2 Log in to your account

You can log into your account via your email and a password you will set at the first time.



Reset your password

If you don't remember your password, you can tap on the **“Forgot Password?”** button. You will receive an email with a password reset link.

If you request a password reset too many times, the system might no longer send you a password reset email. Please get in touch with your administrator instead.

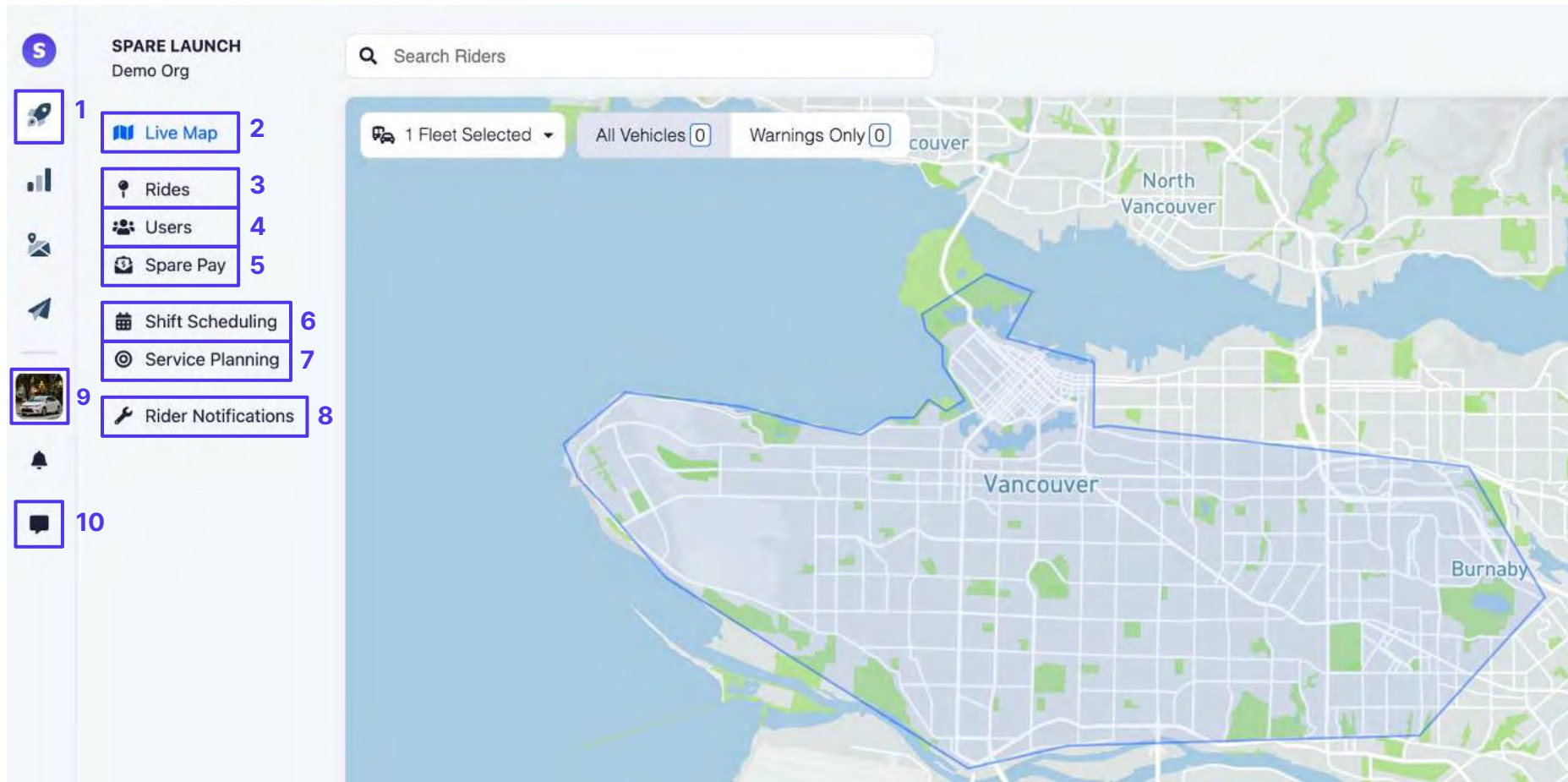
 Remember to follow your manager's instructions and **log out** after your duty if instructed to do so.

1.2. Spare Launch Dashboards Overview



Before you start working with Spare Analyze, our analytics tool, let’s refresh your knowledge about Spare Launch.

Spare Launch[1] is Spare’s core service where all the rides happen. From there, you can navigate to:



#	Name	Functionality
[2]	Spare Live Map	Track and investigate the service on-demand operations;
[3]	Rides	Create, edit, cancel, or investigate trip requests;
[4]	Users	Manage riders’ and drivers’ records;
[5]	Spare Pay	Select payment methods, set fare rules, and create promos;
[6]	Shift Scheduling	Create, edit, and investigate driver duties and vehicle activity;
[7]	Service Planning	Set up your service zones, routes, rules, and flexibilities;
[8]	Rider Notification	Inform your service riders about recent changes via SMS-text, app-based push, email, and automated phone call notifications



This guide is focused on Spare Analyze, Spare’s Analytics & Reporting tool. To learn more about Service Planning and Settings in Spare Launch, refer to Spare’s **Help Centre**.

There are several ways you can **access help resources**:



By clicking on the **message icon[10]**: it will redirect you to Spare’s Tech Support chat.

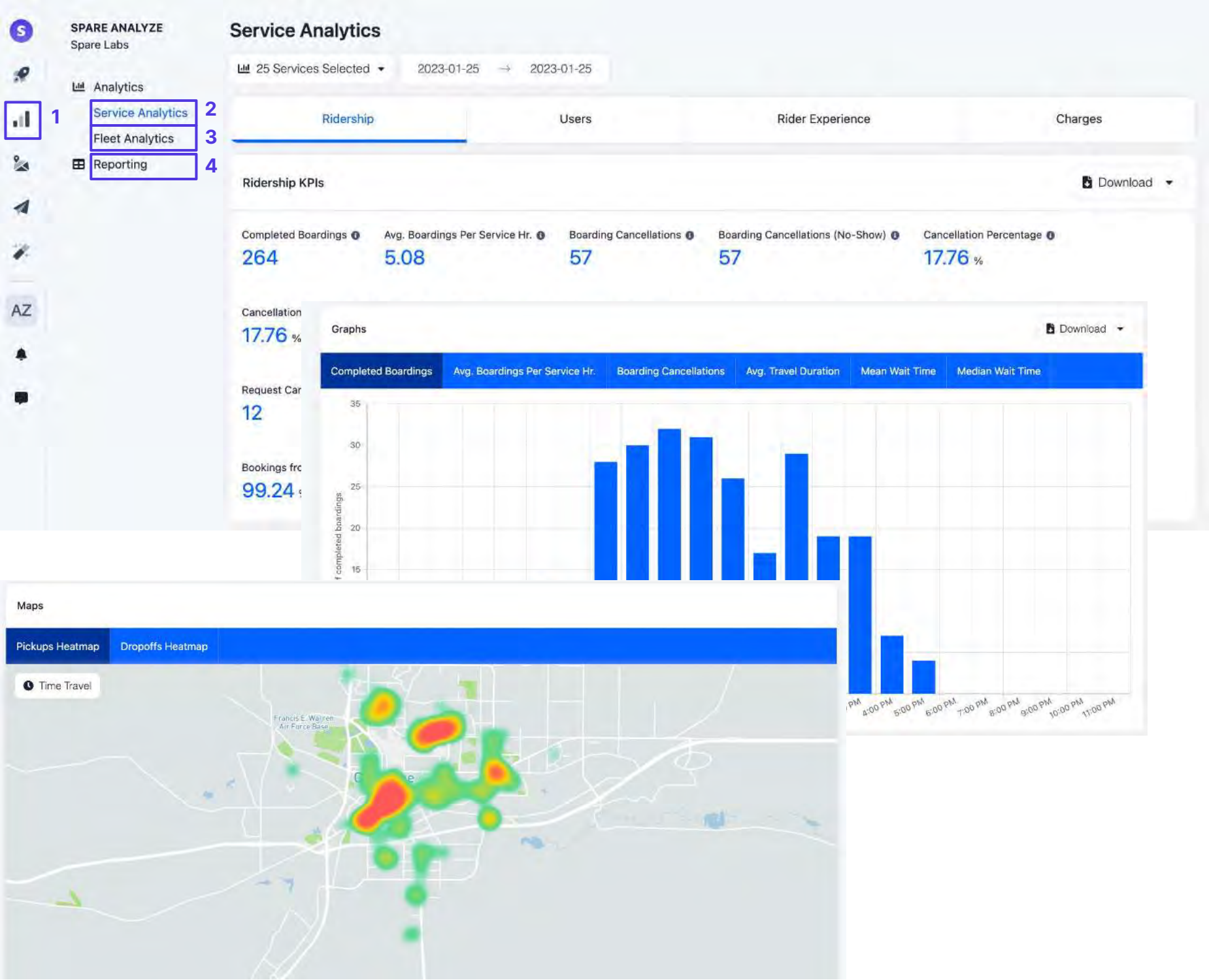


By going to your **Spare Account [9]** and selecting **Help**: it will redirect you to Spare’s Help Center.

1.2. Spare Analyze Dashboards Overview

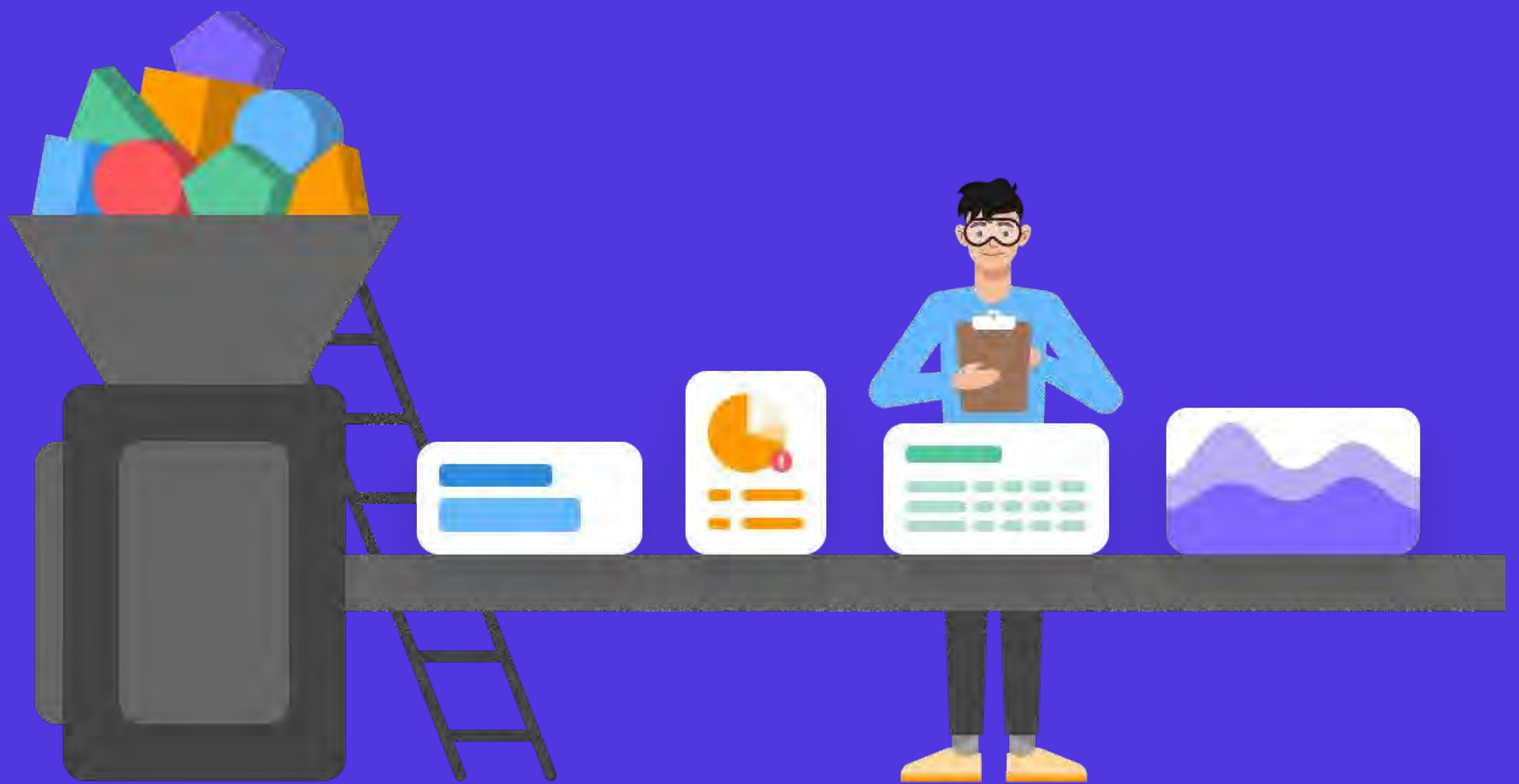
Spare Analyze[1] holds all of the data linked to your services and fleets. You can also access your service and fleet reports, including your National Transit Database (NTD) Report.

This is what Spare Analyze looks like:



Here is the data you can find in Sapre Analyze:

#	Tab	Functionality
[1]	Service Analytics	This area contains data about requests, users, rider experience, and charges. The data is provided in numeric and visual formats.
[2]	Fleet Analytics	This area included data about vehicles and their on-time performance. The data is provided in numeric and graphic formats.
[3]	Reporting	This area allows you to build custom Service and Fleet reports and download them as CSV or XLXs files.



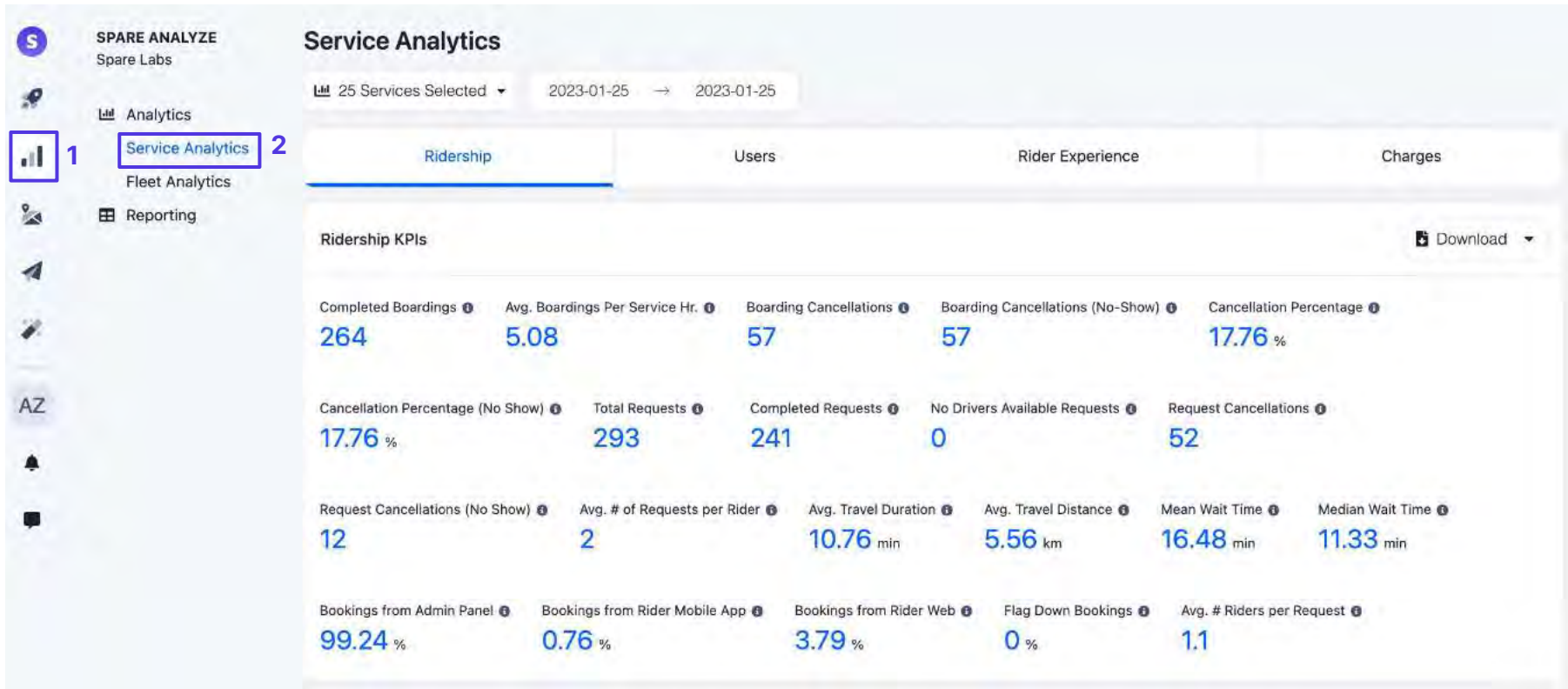
[2] Service Analytics

- Accessing Service Data
- Ridership Data KPIs, Graphs, and Heat Maps
- Users Data KPIs and Graphs
- Rider Experience Data KPIs and Graphs
- Charges Data KPIs and Graphs

2.1. How to Access Service Data

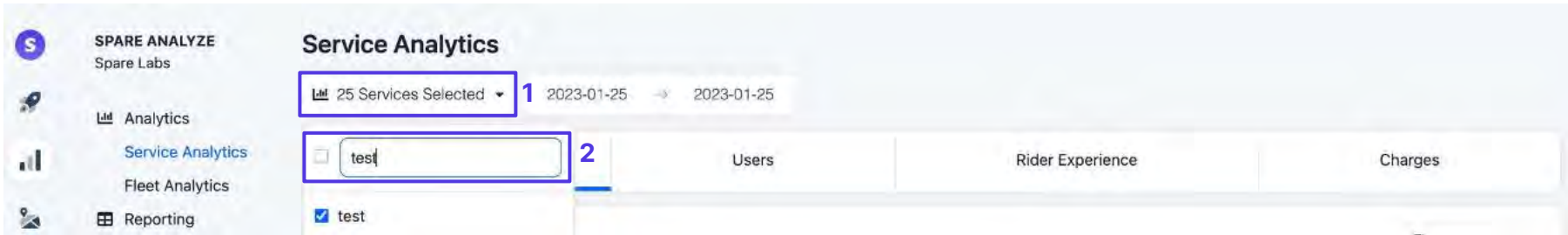
1 Access Service Analytics

To do so, go to **Spare Analyze [1]** and switch to the **Service Analytics tab [2]**. You will see a **Service Data dashboard**.



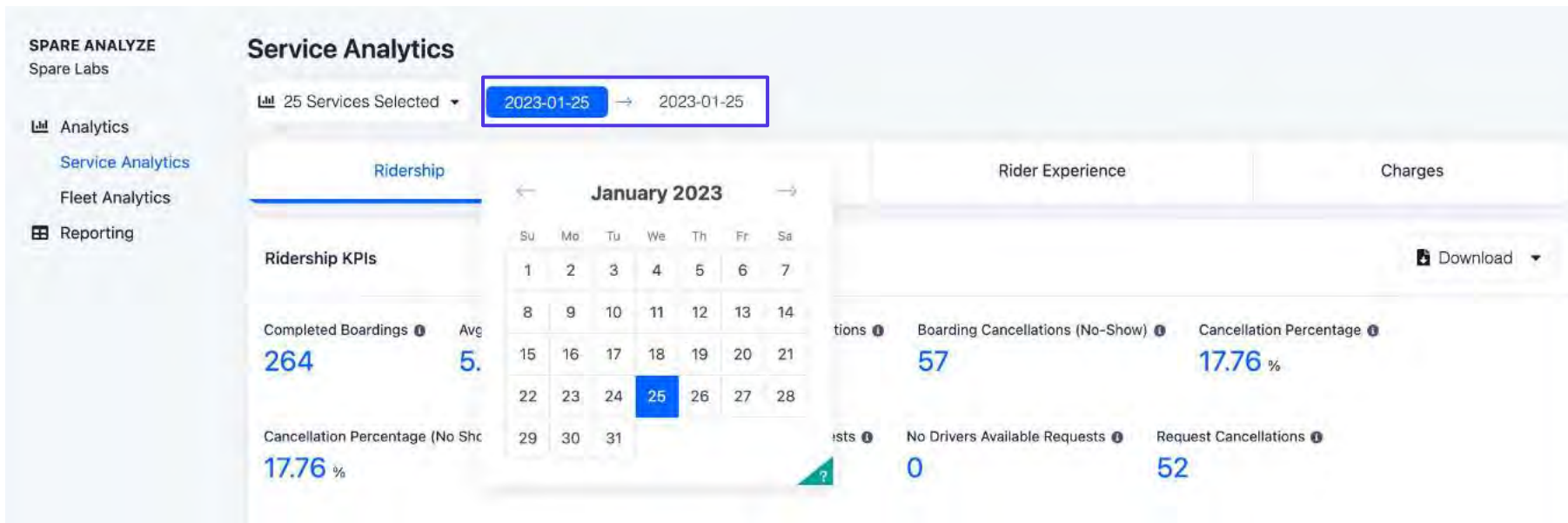
2 Select the Service(s)

To start working with the data, **select the service(s)** you would like to be analyzed. To do so, use the **toggle[1]** at the top of the screen. You can **deselect** all services by clicking the checkbox next to the **service search[2]**.



2 Set the Time Range

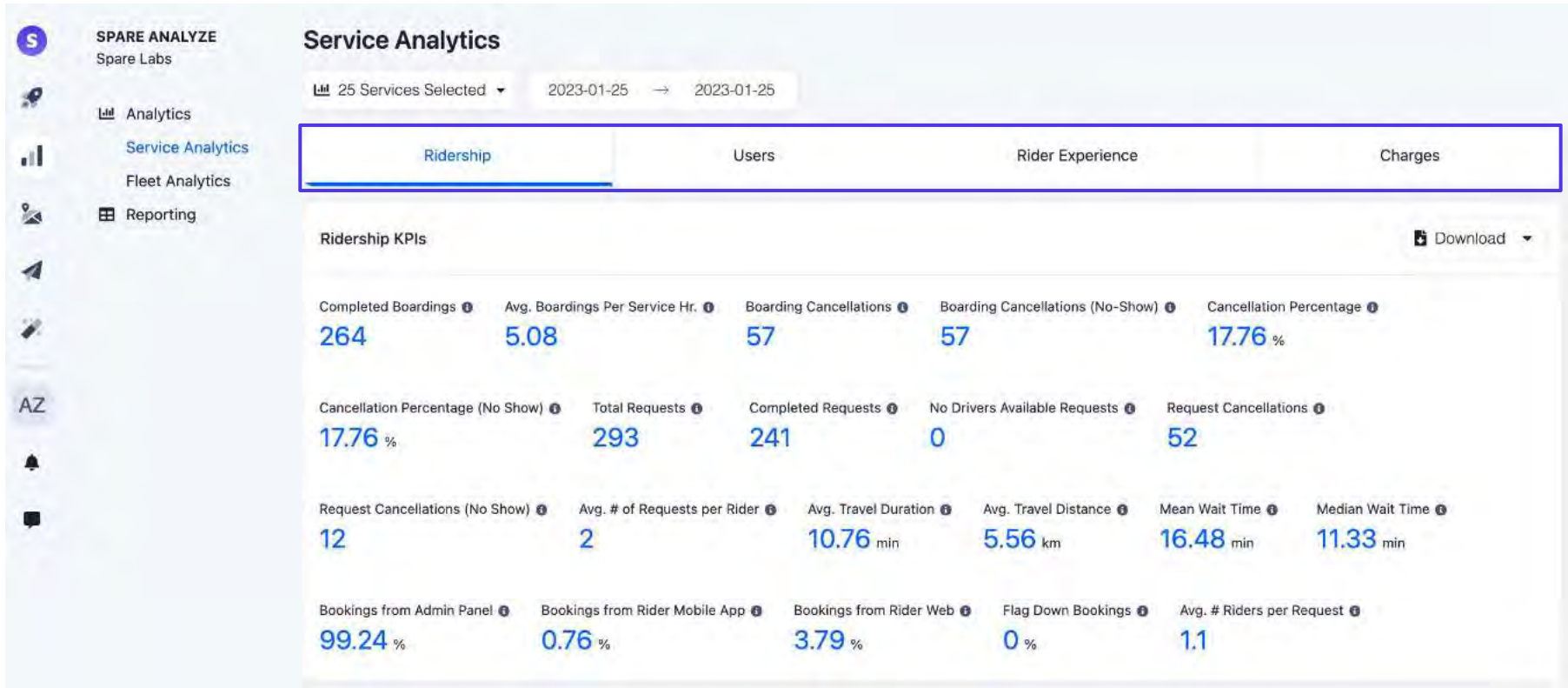
Now select the time period. To do so, use the **toggle** at the top of the screen.



2.2. How to View Ridership Data

1 Explore Ridership KPIs

Below the toggles, there are 4 different tabs where KPI information is displayed: Ridership, Users, Rider Experience, and Charges. Make sure that you are in the **Ridership tab**.



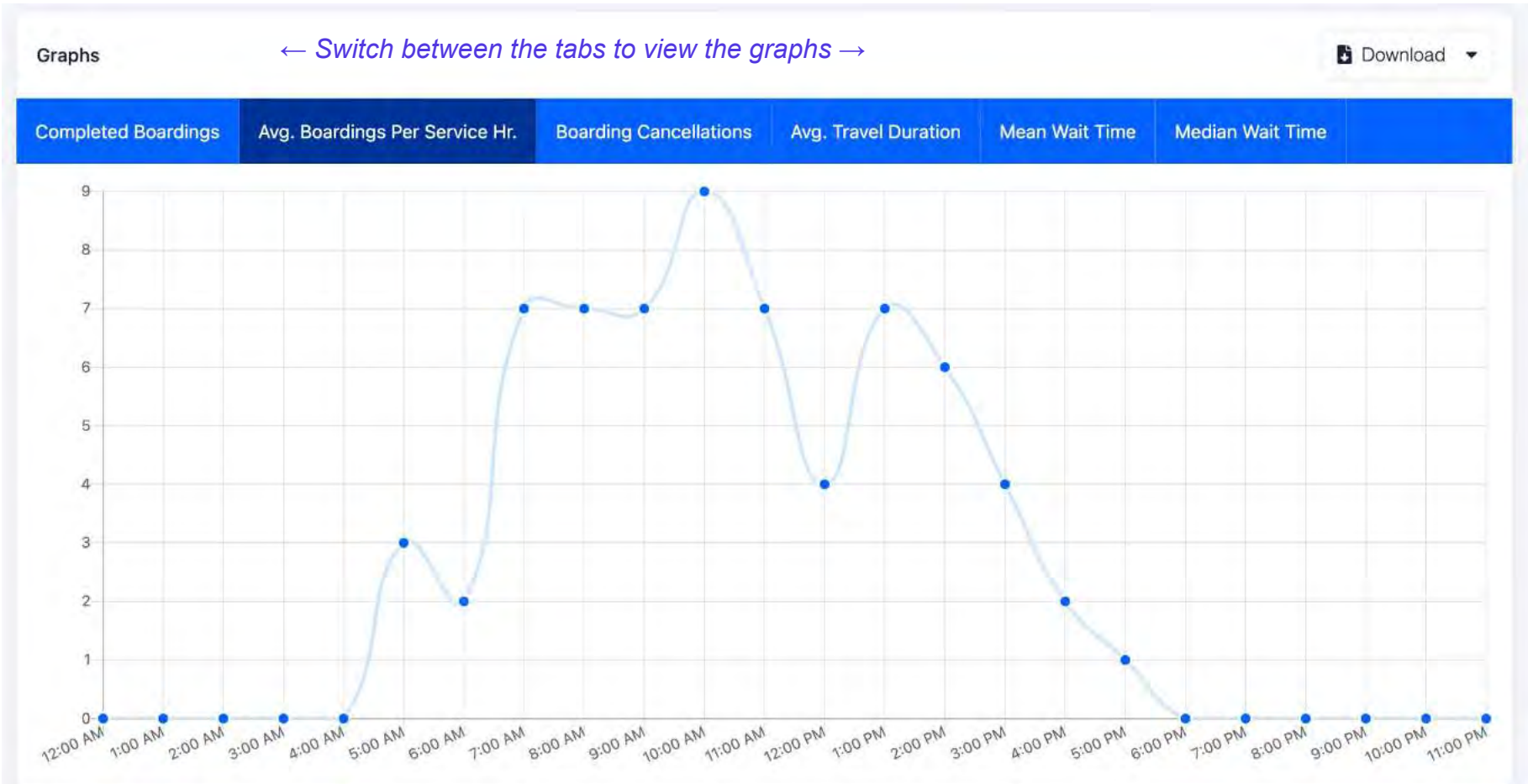
Here are the KPIs data you will see in the Ridership tab:

- **Completed Boardings:** The total number of passengers who completed trips. This can be different than the total number of trip requests (Total Requests), as there can be multiple passengers per trip.
- **Average Boardings Per Service Hour:** The mean number of Completed Boardings for each hour that service was available.
- **Boarding Cancellations:** The total number of passengers whose trips were canceled.
- **Cancellation Percentage:** The percentage of total cancellations out of total trips.
- **Cancellation Percentage (No Show):** The percentage of no-show cancellations out of total trips.
- **Total Requests:** Total number of trips that have reached a "final state". This includes Completed, Cancelled, and No Drivers Available trips. Trips that are In Progress or Processing are not included in this number.
- **Completed Requests:** The total number of completed trip requests.
- **No Drivers Available Requests:** The total number of trips that the system was not able to fulfill and went to the No Drivers Available Status.
- **Request Cancellations:** The total number of canceled trips.
- **Request Cancellations (No Show):** The total number of canceled trips due to a No-Show.
- **Avg. # of Requests per Rider:** The mean number of Completed Requests per rider.
- **Avg. Travel Duration:** The mean amount of time riders spend onboard a vehicle.
- **Avg. Travel Distance:** The mean distance riders traveled while onboard a vehicle.
- **Mean Wait Time:** The mean wait time of an individual rider during this time period. This only applies to the Next Available trips.
- **Median Wait Time:** The median wait time of an individual rider during this time period.
- **Bookings from Admin Panel:** Percentage of total rides that were booked through the Admin Panel.
- **Bookings from Rider App:** Percentage of total rides that were booked through the Rider App.
- **Flag Down Bookings:** Percentage of total rides that were booked through Spare Driver.
- **Avg. # Riders per Request:** The mean number of Completed Boardings per Completed Request. (There can be multiple riders per request).

2.2. How to View Ridership Data

2 View Visual Graphs

Right below the KPI table, the Graphs section lets you view a historical graphical interpretation of the following KPIs:



- **Completed Boardings:** An important metric to measure the relative increase/decrease of the demand and number of individual trips being made. This helps inform capacity, service hours, and expansion.
- **Average Boardings Per Service Hour:** A useful metric that shows the average amount of Completed Boardings per service hour. This is useful in seeing when demand is at its highest and lowest; allowing you to better recognize patterns with your service and schedule duties.
- **Boarding Cancellations:** An important metric to measure the relative increase/decrease of the number of trip cancellations. A high proportion of trip cancellations can point to numerous things, including high wait times, lack of capacity, difficulty in riders finding their ride, or other frictions that make the service less convenient or easy to use.
- **Average Travel Duration:** The average amount of minutes riders spend onboard the vehicle.
- **Mean Wait Time:** An important metric that can inform capacity and/or other technical issues/pain points. This is measured by the amount of time between when the rider wants a trip and when the trip gets fulfilled.
- **Median Wait Time:** An important metric that can inform capacity and/or other technical issues/pain points. This is measured by the amount of time between when the rider wants a trip and when the trip gets fulfilled.

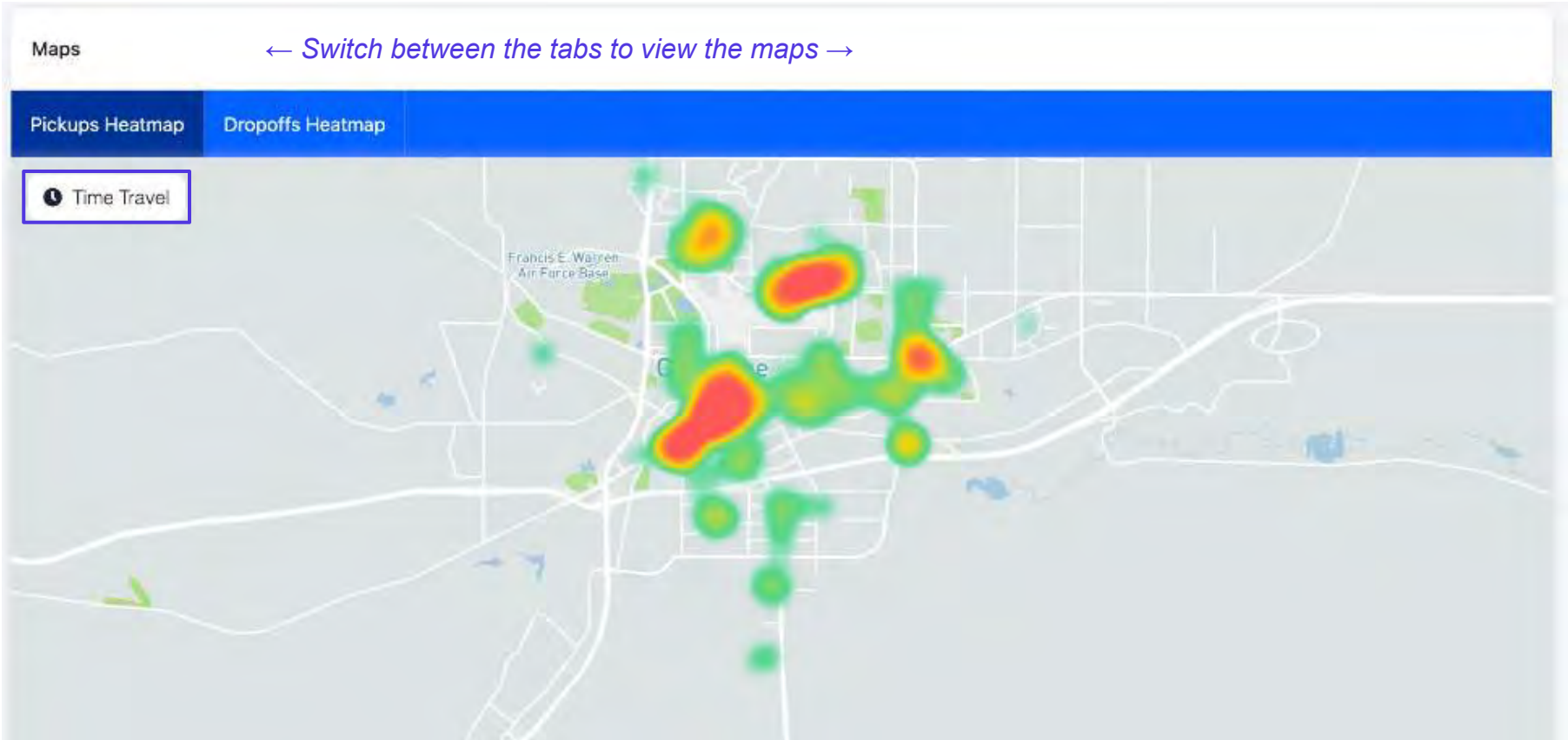
The graphs data will be reflective of the timeframe you have selected.

2.2. How to View Ridership Data

3 Explore Heat Maps

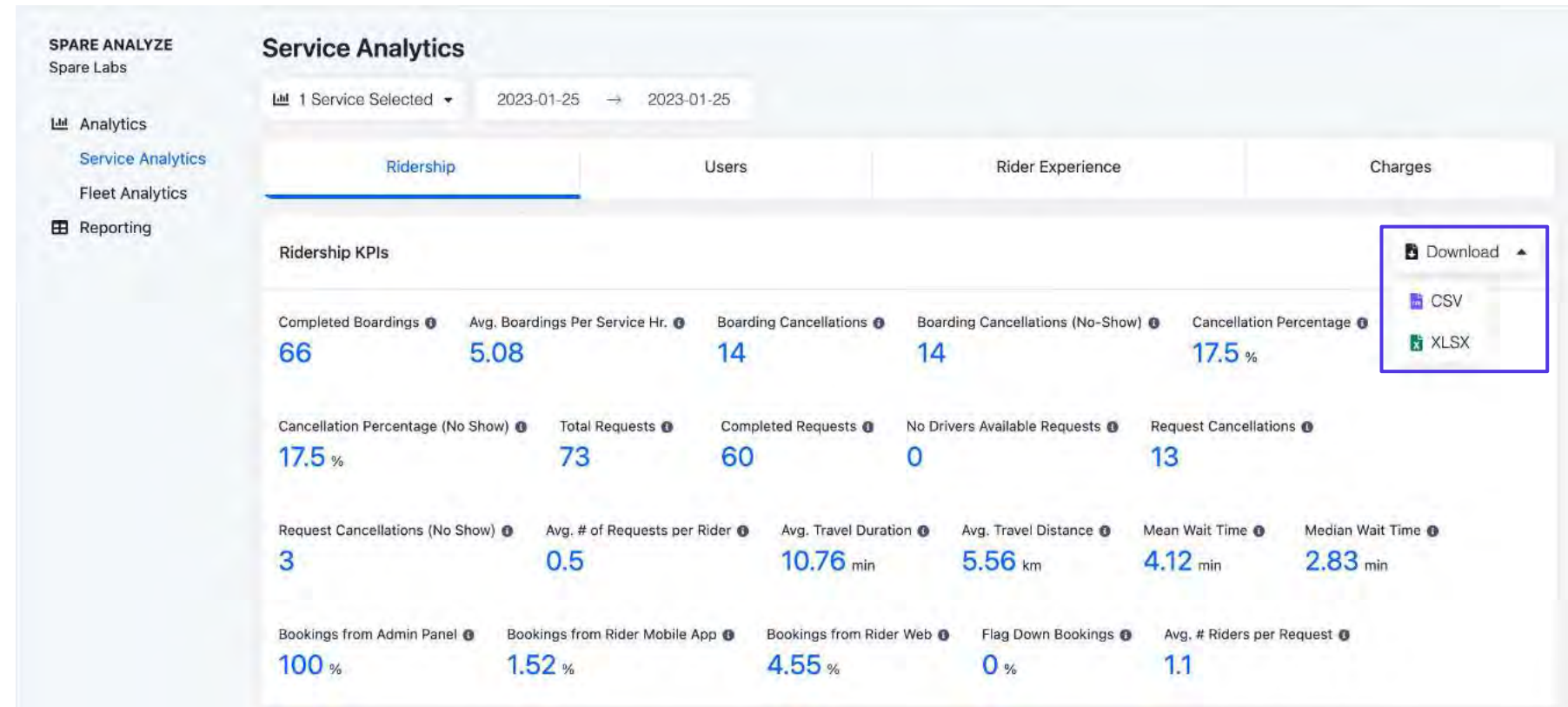
Below the Graphs, the Maps section lets you view heatmaps of both pickups and dropoffs for your selected services and time period, which are helpful to visualize the relative locations of demand.

Use **Time Travel**, the button on the top left, to scroll through time and see the heatmap within a 1 hour time window.



3 Export the Data

You can download CSV or XLSX reports with KPI data and/or Visual Graphs right from the Ridership tab. To do so, click the **Download** button and **select the file format**. The download will begin automatically.



2.3. How to View Users Data

1 Explore Ridership KPIs

Once you **select the service(s)[1]** and **the time range[2]** you would like the data to be displayed for, switch to the **Users tab[3]**.

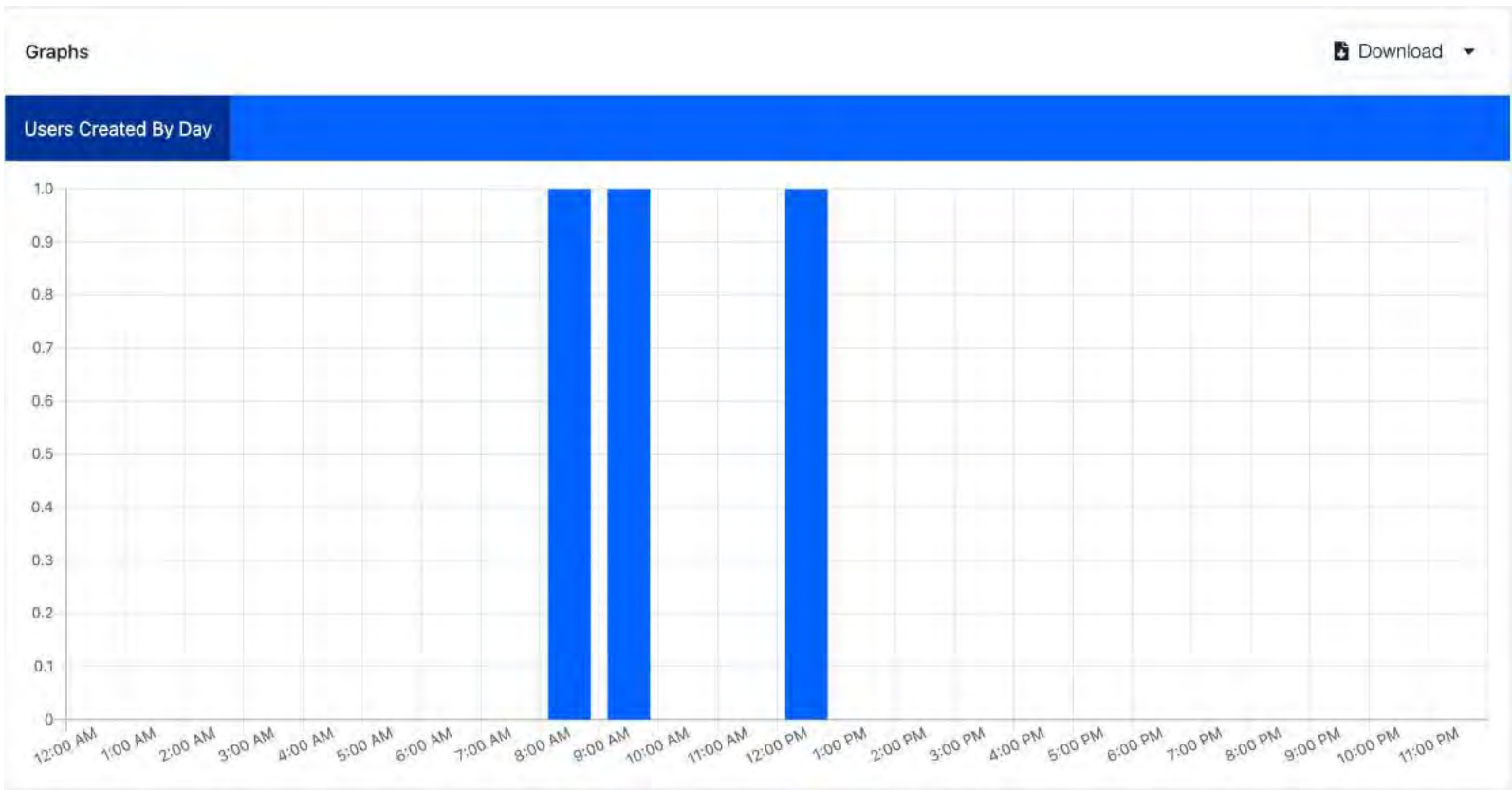


Here is the KPIs data you will see in the Users tab:

- **Users Created:** The number of users created over the given time period.
- **Users with 1st Trip:** The number of users who took their first trip over the given time period.
- **Active Users:** The number of users who took a trip over the given period.
- **Users (All Time):** The number of users ever created.
- **Recurring Users (All Time):** The number of users who have ever taken more than one trip.

2 View Visual Graphs

At the bottom half of the Users page, you can see a graph outlining the number of Users Created By Day. The graphs data will be reflective of the timeframe you have selected.



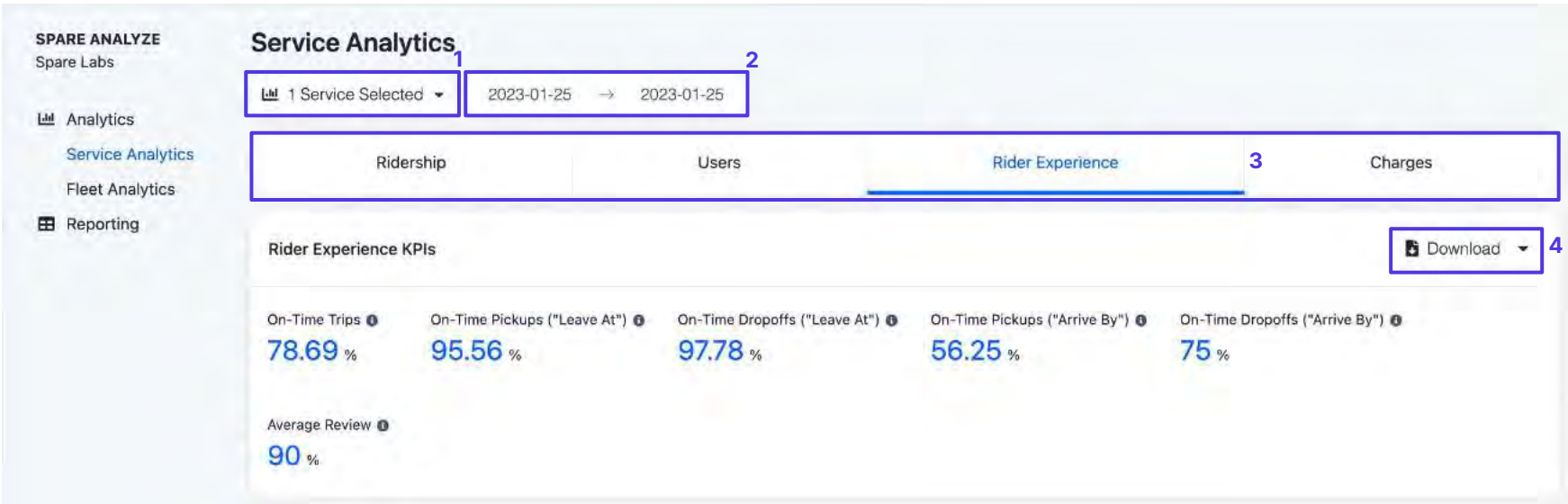
3 Export the Data

You can **download CSV or XLSX** reports with KPI data and/or Visual Graphs right from the Ridership tab. To do so, click on the **Download** button and select the file format. The download will begin automatically.

2.4. How to View Rider Experience Data

1 Explore Rider Experience KPIs

Once you **select the service(s)**[1] and the **time range**[2] you would like the data to be displayed for, switch to the **Rider Experience tab**[3]. **Download**[4] the KPIs table in the CSV/XLXS format if necessary.



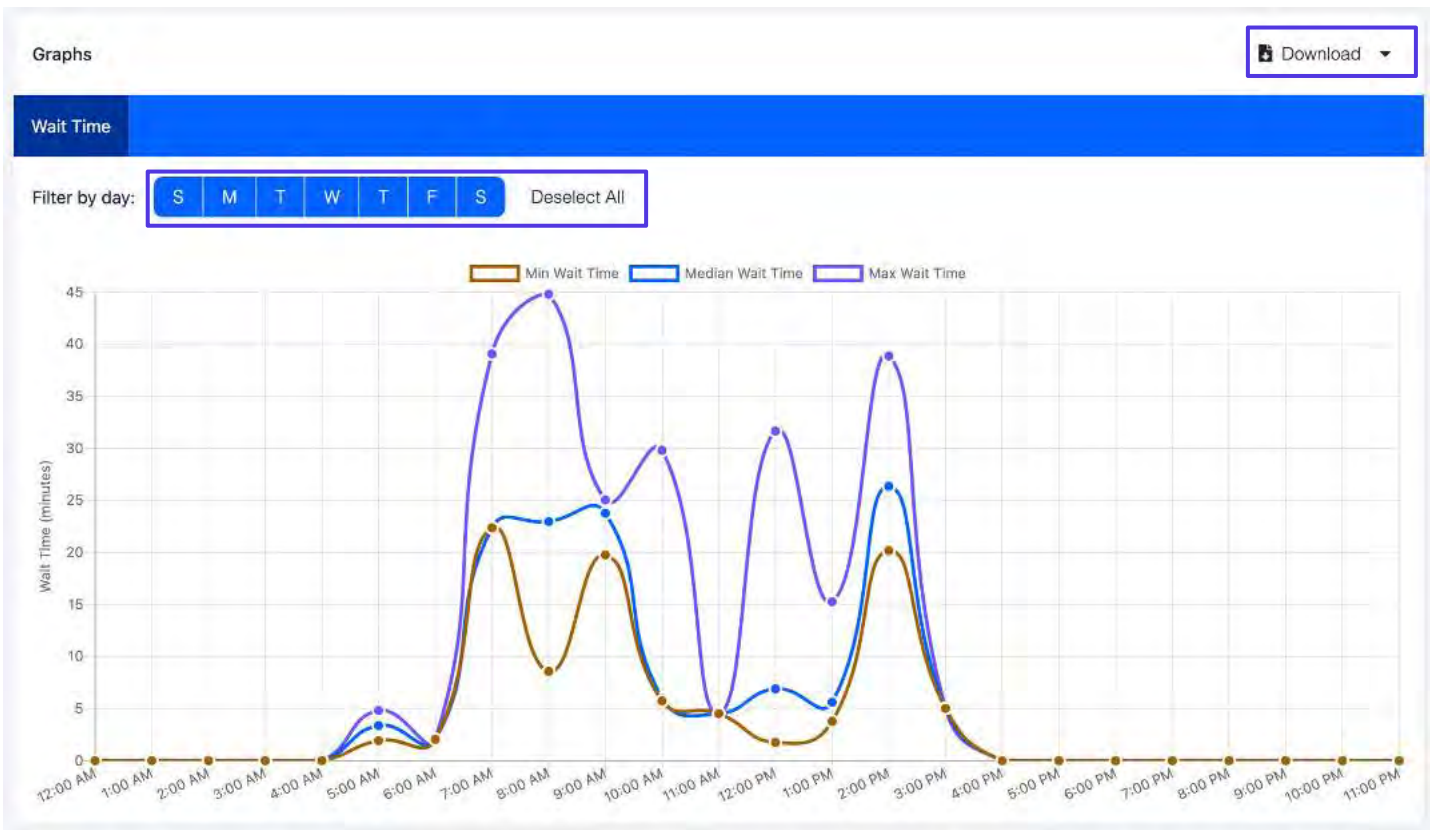
Here is the KPIs data you will see in the tab:

- **On-Time Trips:** Percentage of completed trips where both pickup and dropoff times were within the trip's flexibility margin.
- **On-Time Pickups ("Leave At"):** Percentage of completed "Leave At" trips where the actual pickup time was within the trip's flexibility margin.
- **On-Time Dropoffs ("Leave At"):** Percentage of completed "Leave At" trips where the actual dropoff time was within the trip's flexibility margin.
- **On-Time Pickups ("Arrive By"):** Percentage of completed "Arrive By" trips where the actual pickup time was within the trip's flexibility margin.
- **On-Time Dropoffs ("Arrive By"):** Percentage of completed "Arrive By" trips where the actual dropoff time was within the trip's flexibility margin.
- **Average Review:** Average ratings from riders who left a review at the end of their trip.

2 View Visual Graphs

At the bottom half of the Rider Experience page, you can see a graph outlining the Minimum Wait Time, Median Wait Time, and Maximum Wait Time of the selected services and timeframe.

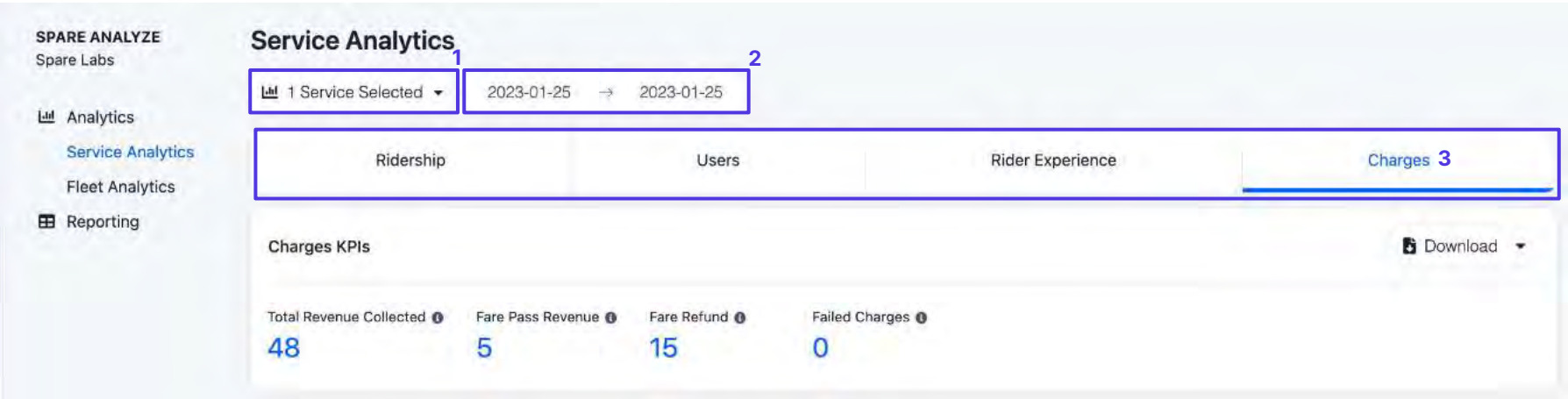
Filter the data by specific **days of the week** by selecting or deselecting them at the top of the graph. **Download** the graph in CSV/XLXS format if necessary.



2.5. How to View Charges Data

1 Explore Charges KPIs

Once you **select the service(s)**[1] and **the time range**[2] you would like the data to be displayed for, switch to **the Charges tab**[3].

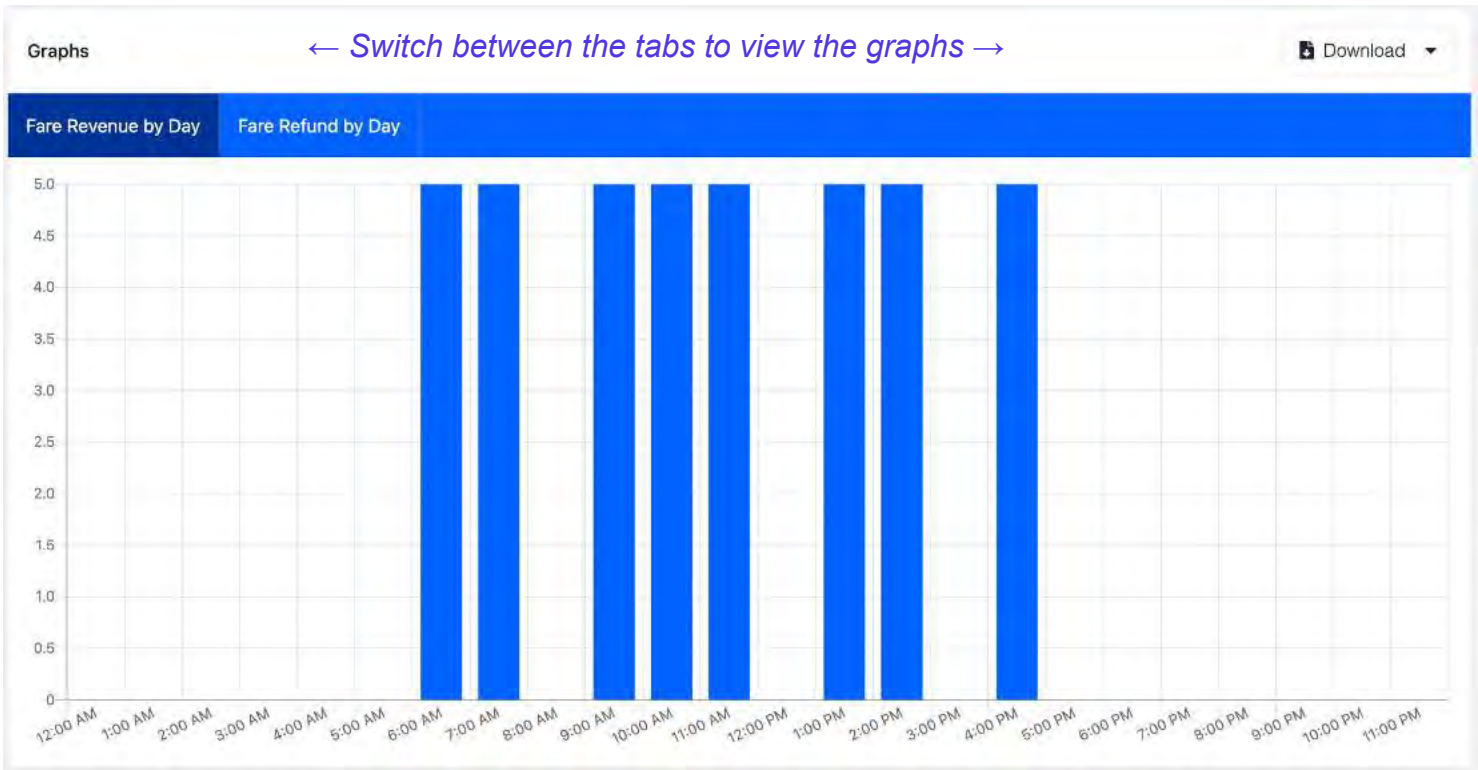


Here is the KPIs data you will see in the tab:

- **Fare Revenue:** Total amount of revenue from fares.
- **Fare Refund:** Total amount of refunded fare revenue.
- **Failed Charges:** Total amount of charges which failed.

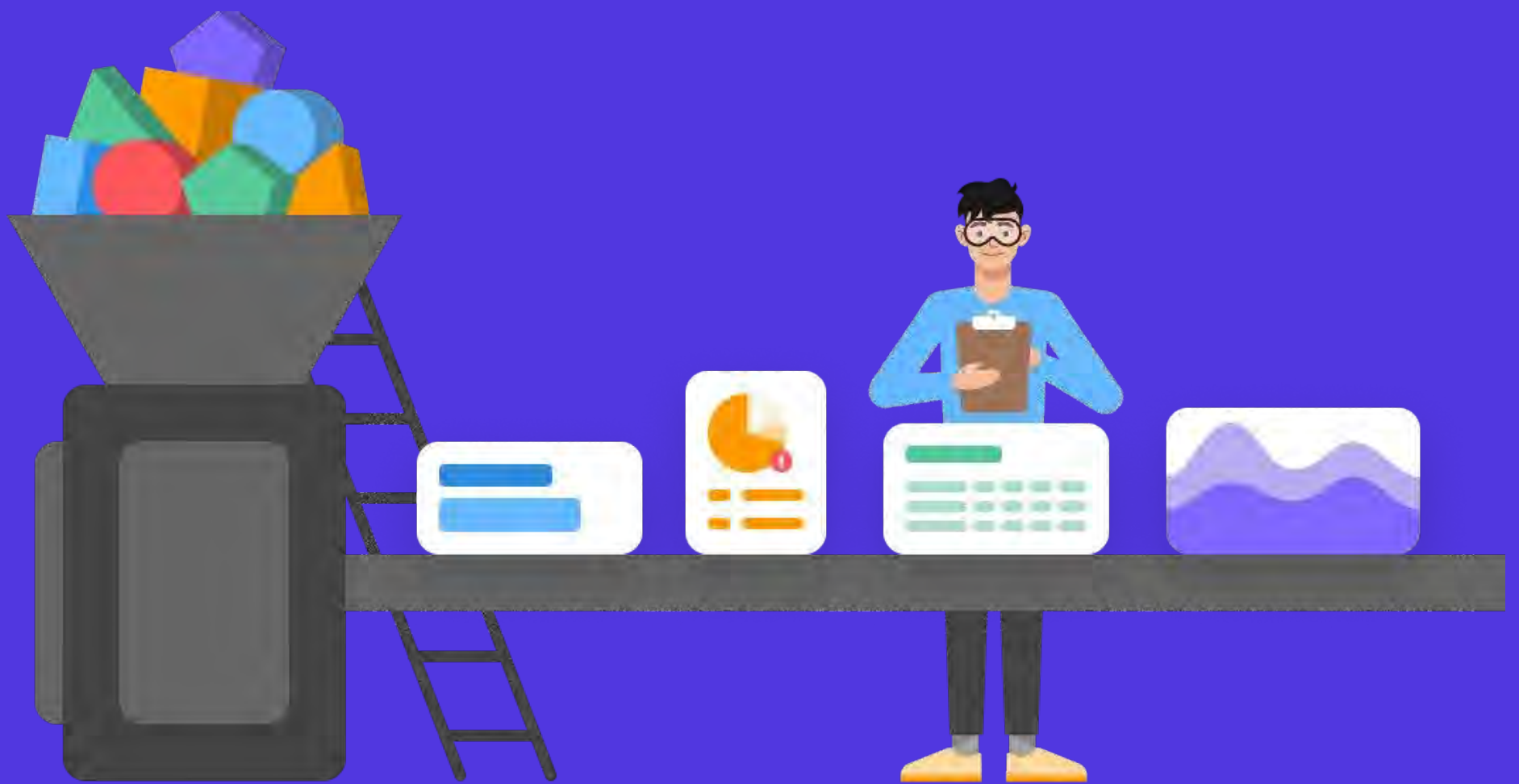
2 View Visual Graphs

At the bottom half of the Charges page, you can see a graph outlining the amount of Fare Revenue by Day and Fare Refund by Day. The graphs data will be reflective of the timeframe you have selected.



3 Export the Data

You can **download CSV or XLXS reports** with KPI data and/or Visual Graphs right from the Ridership tab. To do so, click on the Download button and select the file format. The download will begin automatically.



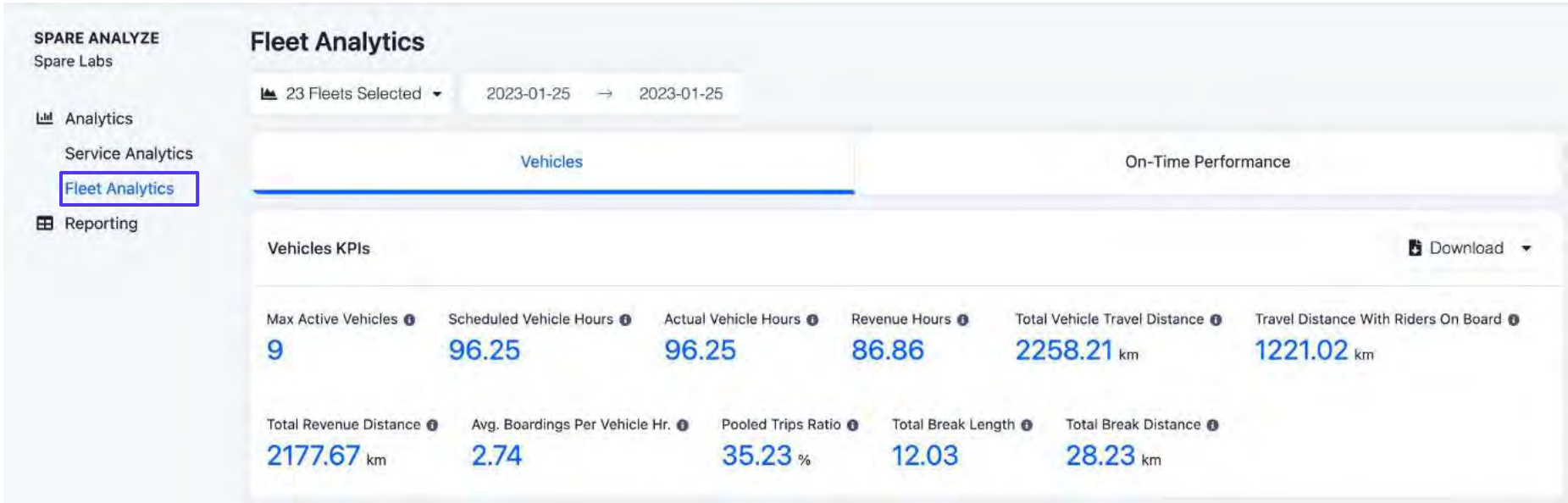
[3] Fleet Analytics

- Time frames and Reporting Periods
- Key Performance Indicators
- Visual Graphs

3.1. How to Access Fleet Data

1 Access Fleet Analytics

To do so, go to **Spare Analyze** and switch to the **Fleet Analytics** tab. You will see a **Fleet Data** dashboard.



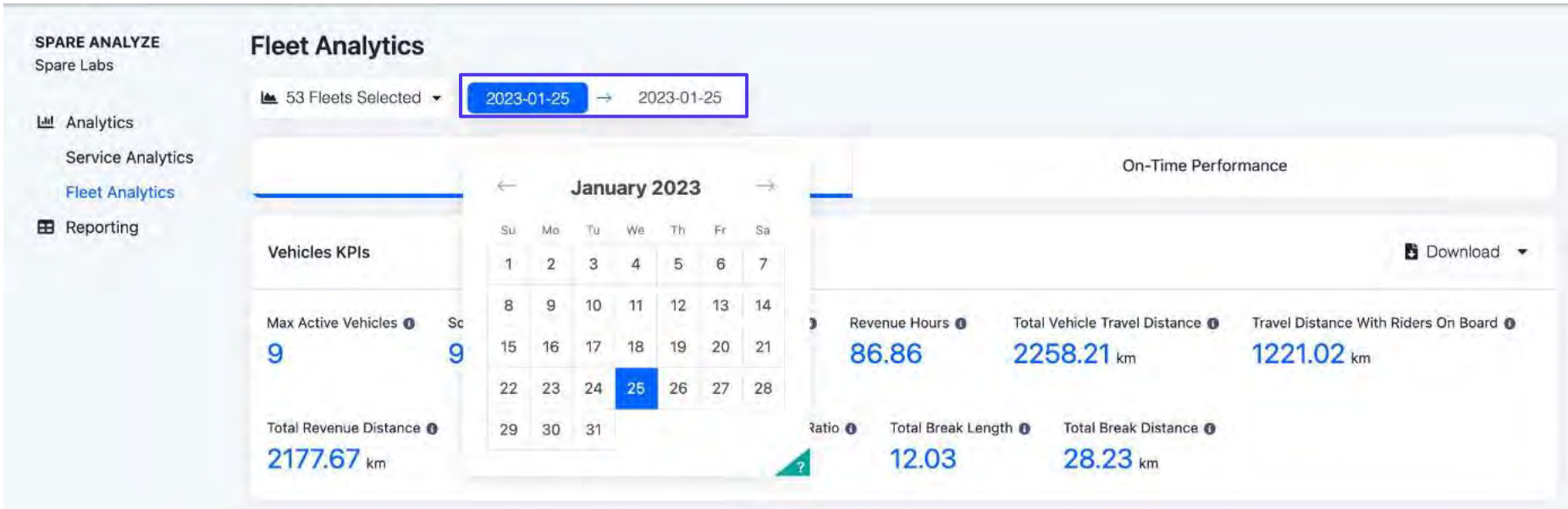
2 Select the Fleet(s)

To start working with the data, **select the fleet(s)** you would like to be analyzed. To do so, use the **toggle[1]** at the top of the screen. You can **deselect** all fleets by clicking the checkbox next to the **fleet search[2]**.



2 Set the Time Range

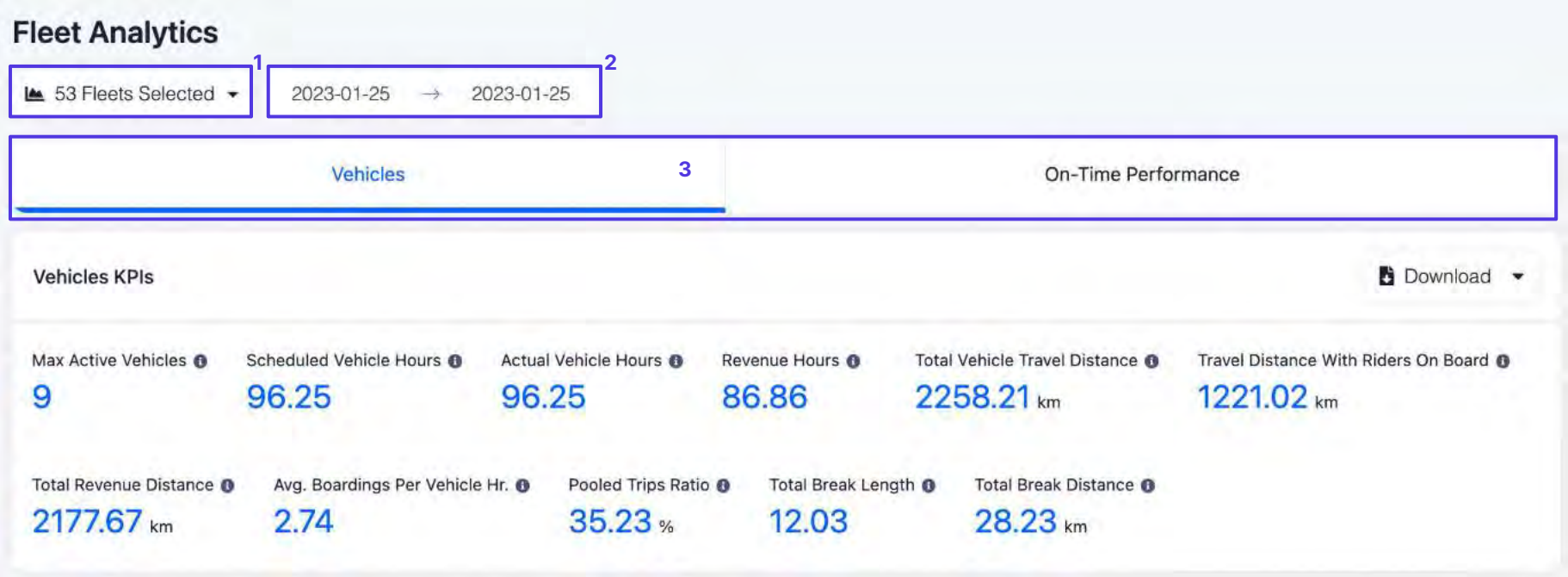
Now select the **time period**. To do so, use the **toggle[1]** at the top of the screen.



3.2. How to View Vehicles Data

1 Explore Vehicles KPIs

Once you **select the fleet(s)**[1] and **the time range**[2] you would like the data to be displayed for, you will see two tabs: **Vehicles** and **On-Time Performance**. Switch to the **Vehicles Tab**[3].



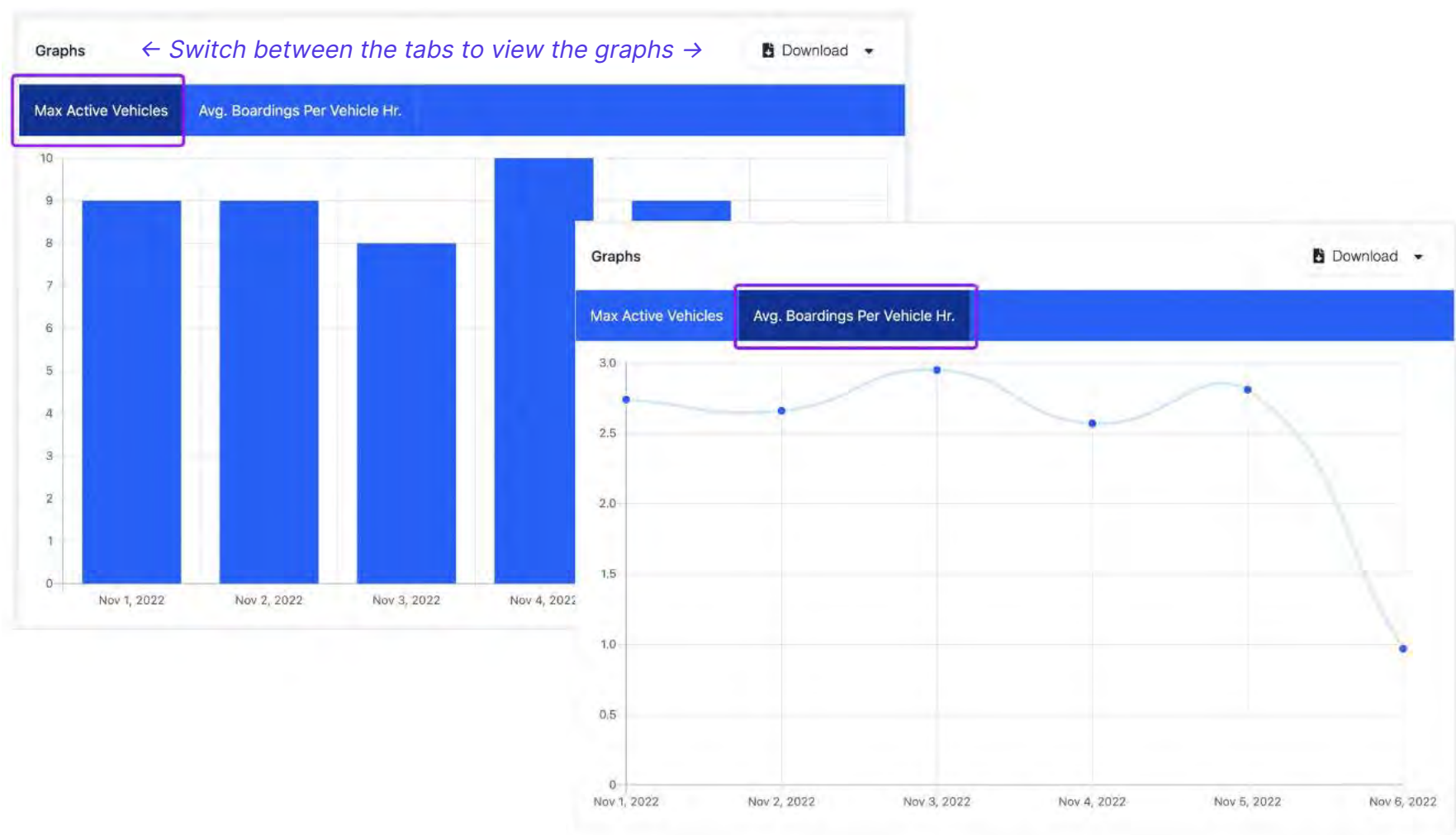
Here is the KPIs data you will see in the tab:

- **Max. Active Vehicles:** The highest number of duties simultaneously in progress during the selected time period.
- **Scheduled Service Hours:** Total number of scheduled duty hours for all operational vehicles.
- **Actual Vehicle Hours:** Total number of hours actually completed by all operational vehicles, including non-revenue time.
- **Revenue Hours:** Total number of hours actually completed by all operational vehicles, excluding non-revenue time.
- **Total Vehicle Travel Distance:** Total distance covered by all operational vehicles.
- **Travel Distance With Riders On Board:** Distance covered with riders on board for all operational vehicles.
- **Total Revenue Distance:** Distance covered between the first pickup and last dropoff for all operational vehicles.
- **Avg.Boardings Per Vehicle Hr.:**Mean number of boardings per hour driven by all operational vehicles.
- **Pooled Trips Ratio:** Percentage of trips where a passenger shared their ride with another passenger.
- **Total Break Length:** Total time spent on breaks by all operational vehicles.
- **Total Break Distance:** Total distance travelled on breaks by all operational vehicles.

3.2. How to View Vehicles Data

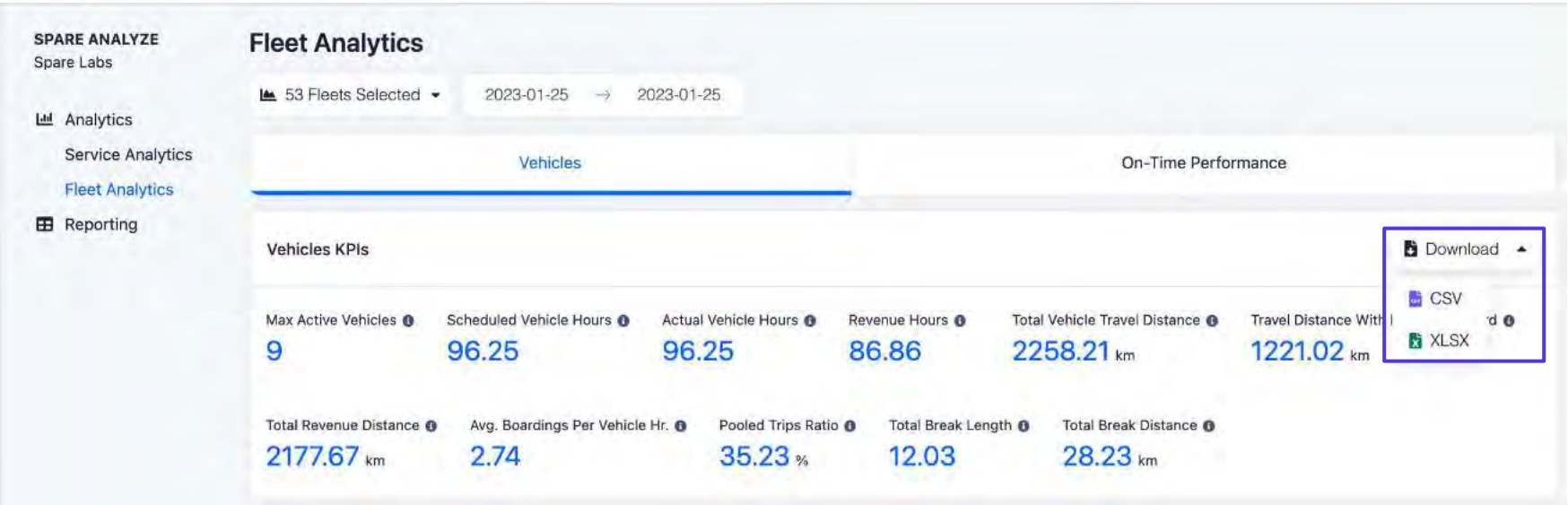
2 View Visual Graphs

At the bottom half of the Vehicles page, you can see a graph outlining Maximum Boarded Vehicles and Average Boardings per Vehicle per Hour. The graphs data will be reflective of the timeframe you have selected.



3 Export the Data

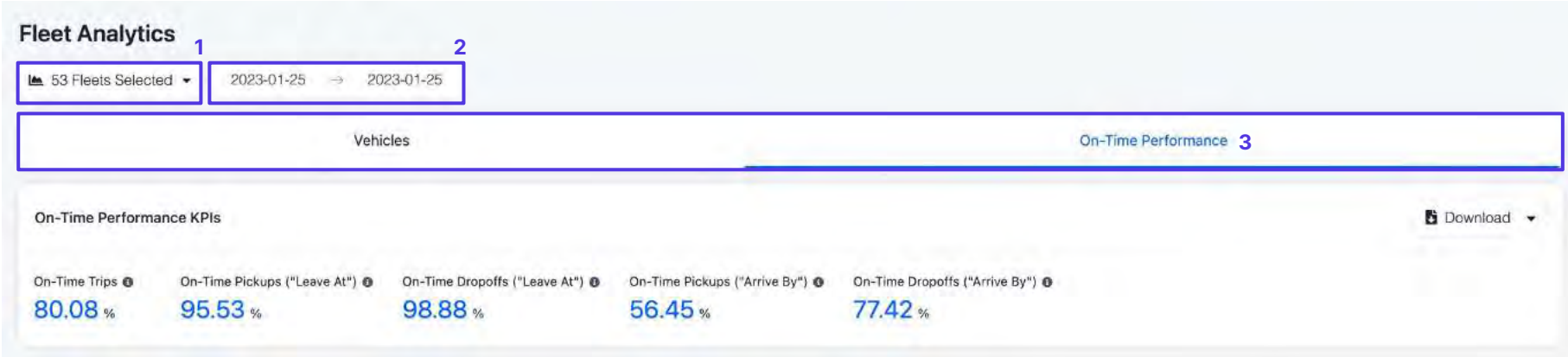
You can **download CSV or XLSX reports** with KPI data and/or Visual Graphs right from the Vehicles tab. To do so, click on the Download button and select the file format. The download will begin automatically.



3.3. How to View On-Time Performance Data

1 Explore Vehicles KPIs

Once you **select the fleet(s)[1]** and the time range you would like the data to be displayed for, you will see two tabs: **Vehicles** and **On-Time Performance**. Switch to the **On-Time Performance Tab[3]**.

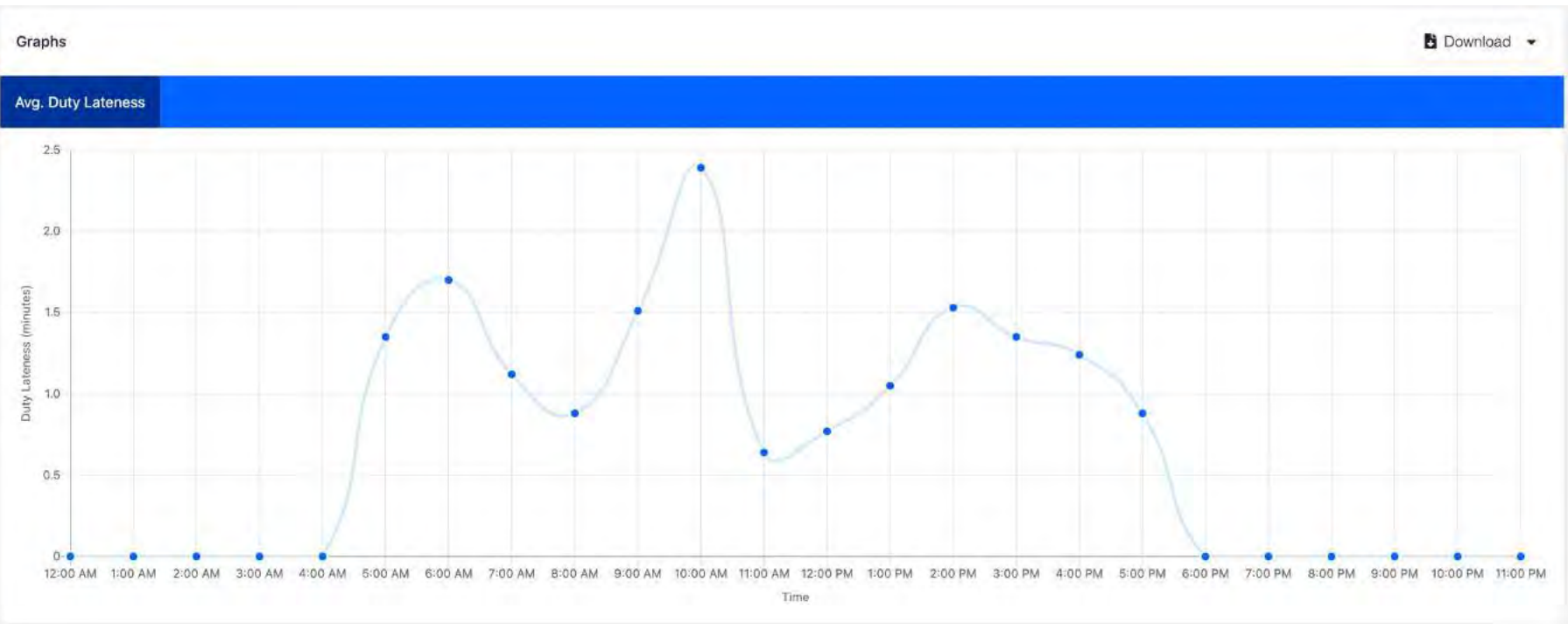


Here is the KPIs data you will see in the tab:

- **On-Time Trips:** Percentage of completed trips where both pickup and dropoff times were within the trip's flexibility margin.
- **On-Time Pickups ("Leave At"):** Percentage of completed "Leave At" trips where the actual pickup time was within the trip's flexibility margin.
- **On-Time Dropoffs ("Leave At"):** Percentage of completed "Leave At" trips where the actual dropoff time was within the trip's flexibility margin.
- **On-Time Pickups ("Arrive By"):** Percentage of completed "Arrive By" trips where the actual pickup time was within the trip's flexibility margin.
- **On-Time Dropoffs ("Arrive By"):** Percentage of completed "Arrive By" trips where the actual dropoff time was within the trip's flexibility margin.

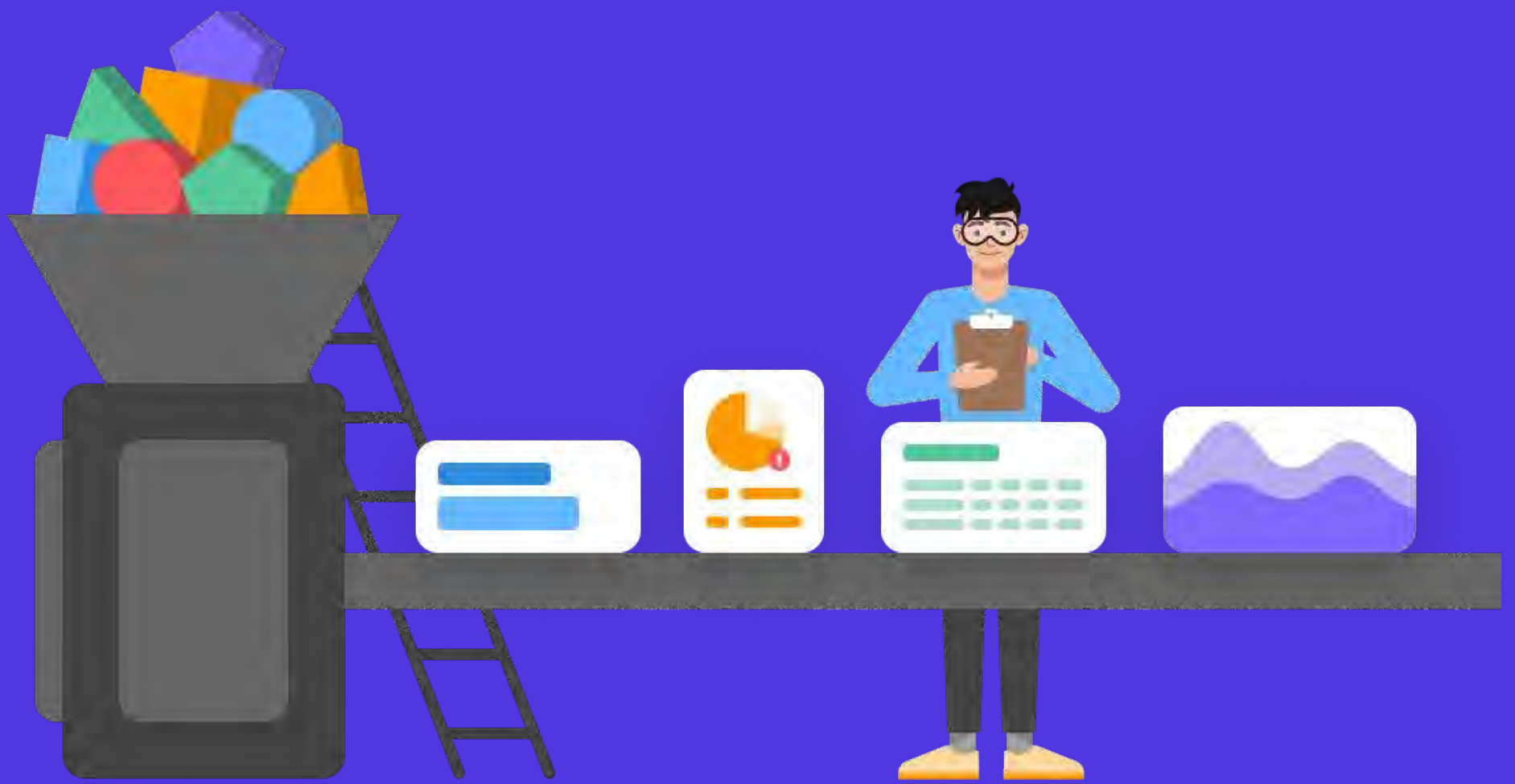
2 View the Visual Graph

At the bottom half of the On-Time Performance page, you can see a graph outlining **Average Duty Lateness**. The graph data will be reflective of the timeframe you have selected.



3 Export the Data

You can **download CSV or XLSX** reports with KPI data and/or Visual Graphs right from the On-Time Performance tab. To do so, click on the Download button and select the file format. The download will begin automatically.



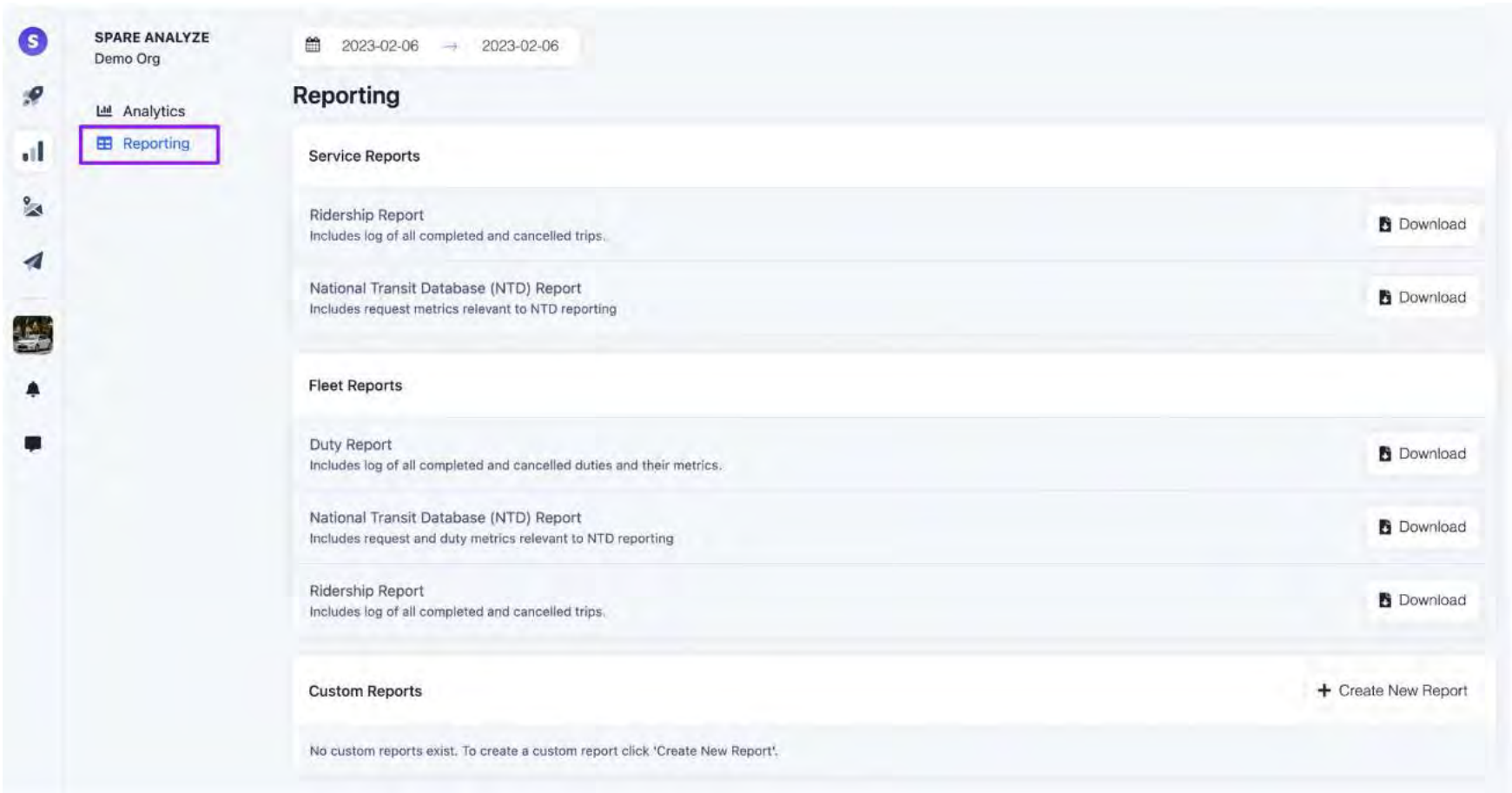
[4] Reporting

- Types of Reports: Service, Fleet, NTD
- Build Custom Reports on the Platform
- Get Automated Reports

4.1. How to Access and Download Reports

1 Access the Reporting Dashboard

To access Spare Reports, in **Spare Analyze**, go to the **Reporting** tab.



2 Select the Report Type

You will see there are 5 types of reports currently available that are related to two report groups: **Service Reports** and **Fleet Reports**.

Refer to the table below to learn about each of the 5 reports.

1. Service Reports	2. Fleet Reports
1.1. Ridership Report (Service): includes log of all completed and cancelled trips	2.1. Duty Report: includes Includes log of all completed and cancelled duties and their metrics.
1.2. NTD Report (Service): Includes request metrics relevant to NTD reporting	2.2. NTD Report(fleets): Includes request and duty metrics relevant to NTD reporting
	2.3. Ridership Report (Fleet): includes log of all completed and cancelled trips

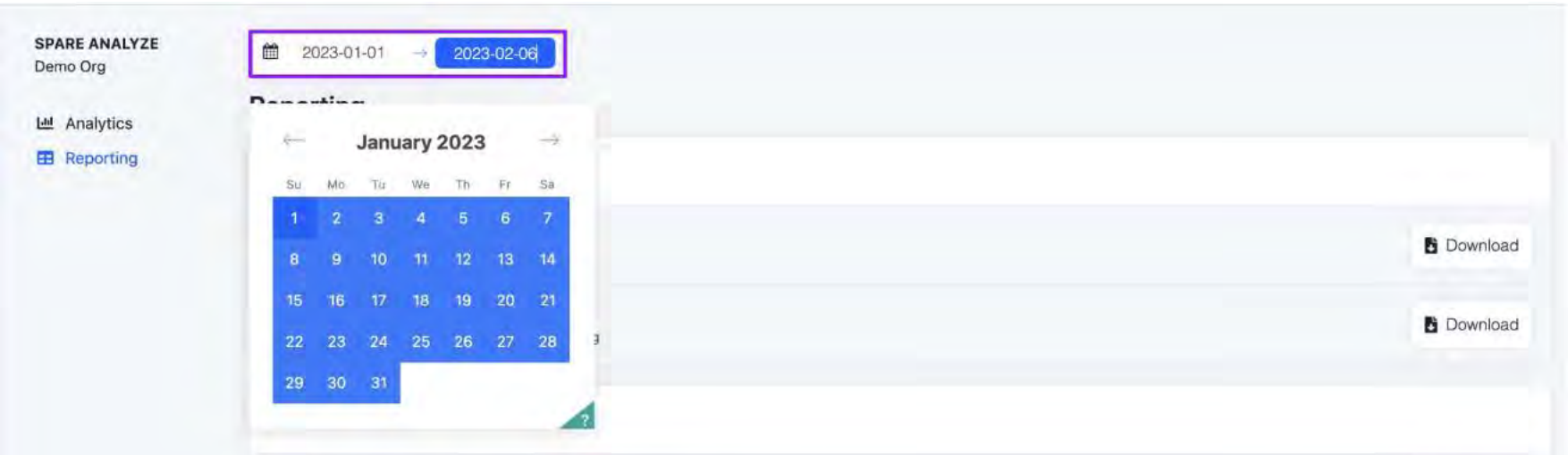


You can also build custom reports. To find out how to do it, go to the section 4.2 of this guide.

4.1. How to Access and Download Reports

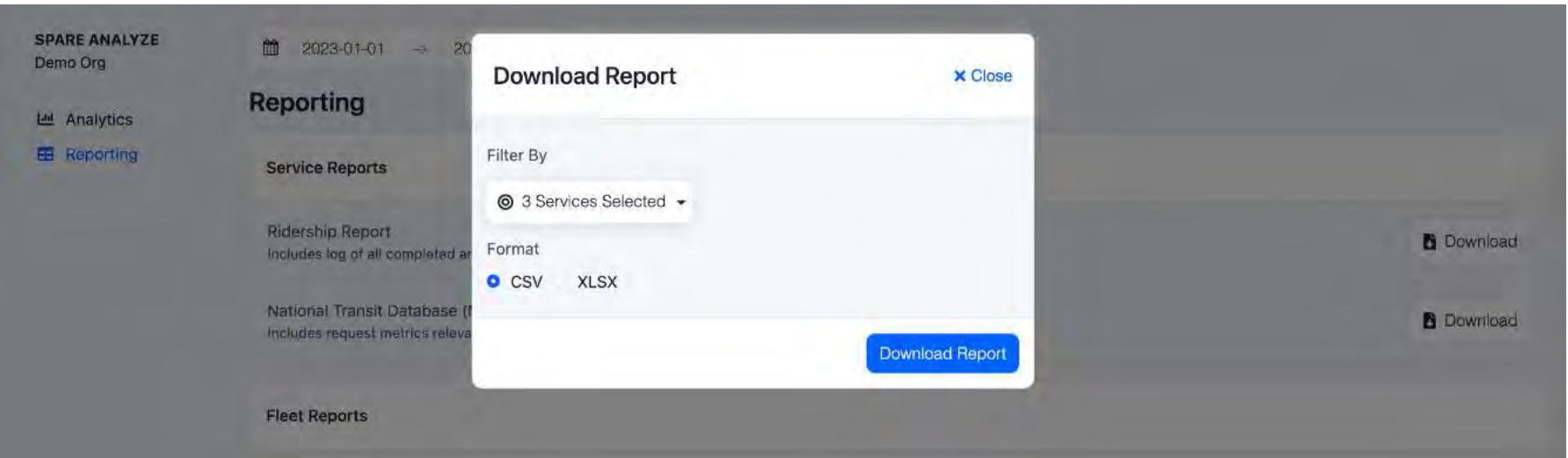
3 Set the Time Range

Use the toggle at the top of the screen to set the time range you'd like the report to be generated for.



4 Download a Pre-Built Report

Click **Download** next to the name of the report and **select fleet(s) or service(s)** you'd like to be included in the report. Use the dropdown menu to check/uncheck the fleet(s)/service(s).

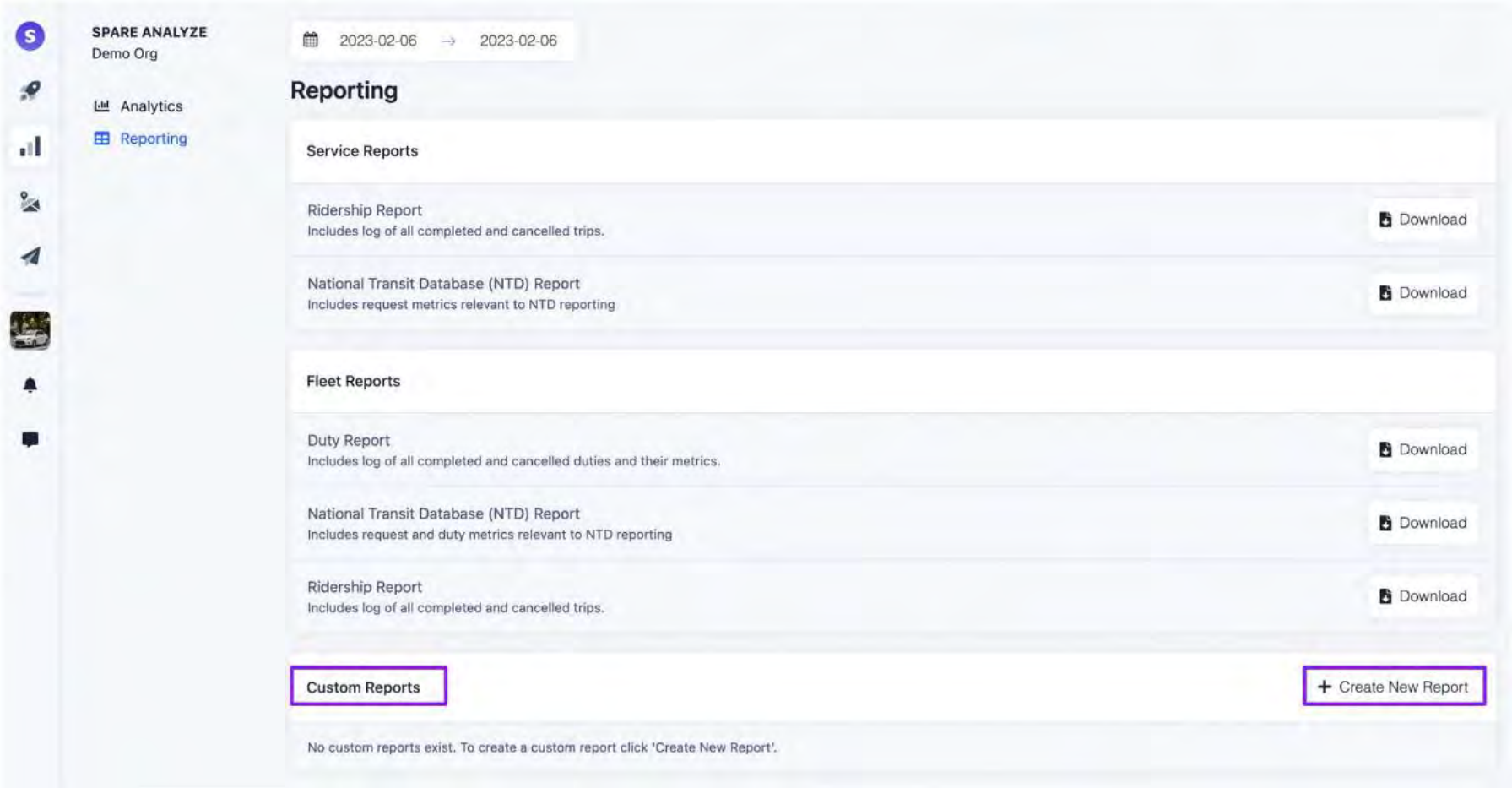


Finally, **select either a CSV or XLSX** file type and **click Download Report** - both will open in Excel and Google Sheets.

4.2. How to Build Custom Reports

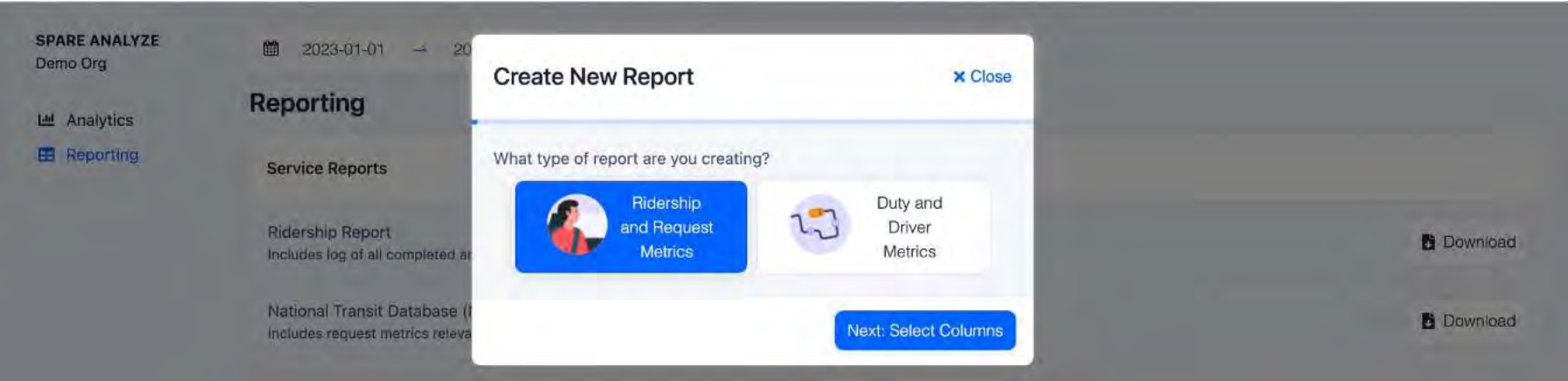
1 Create a New Report

Spare Reports are customizable! To build a custom report, click **+ Create New Report** in the **Custom Reports** section.

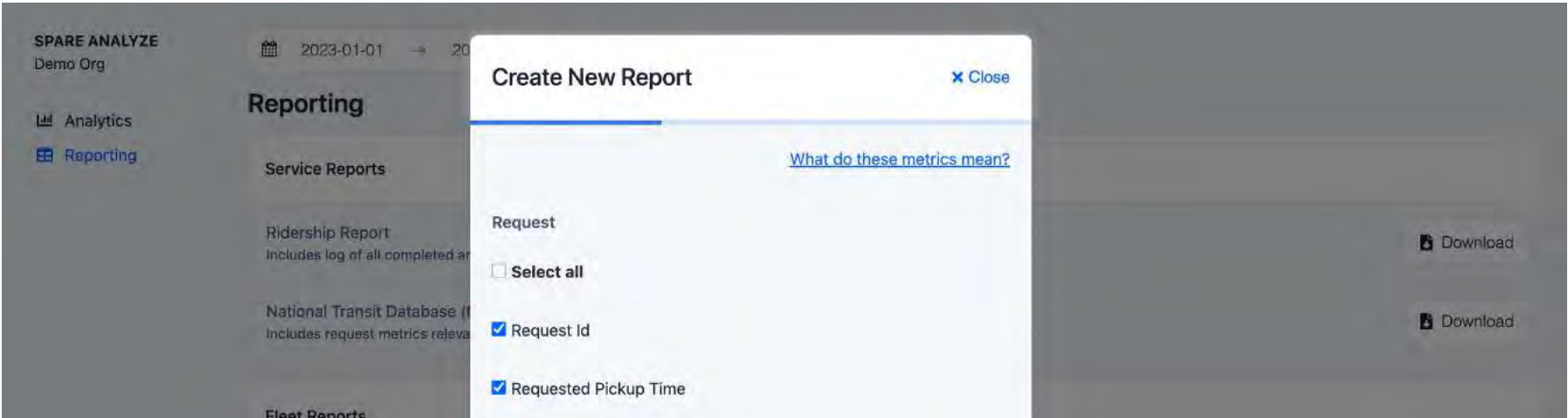


2 Select the Metrics

→ Choose what metrics you'd like to include: **Ridership Metrics** or **Duty Metrics**:



→ **Select the metrics** you need and scroll down to click **Next: Name and Save**

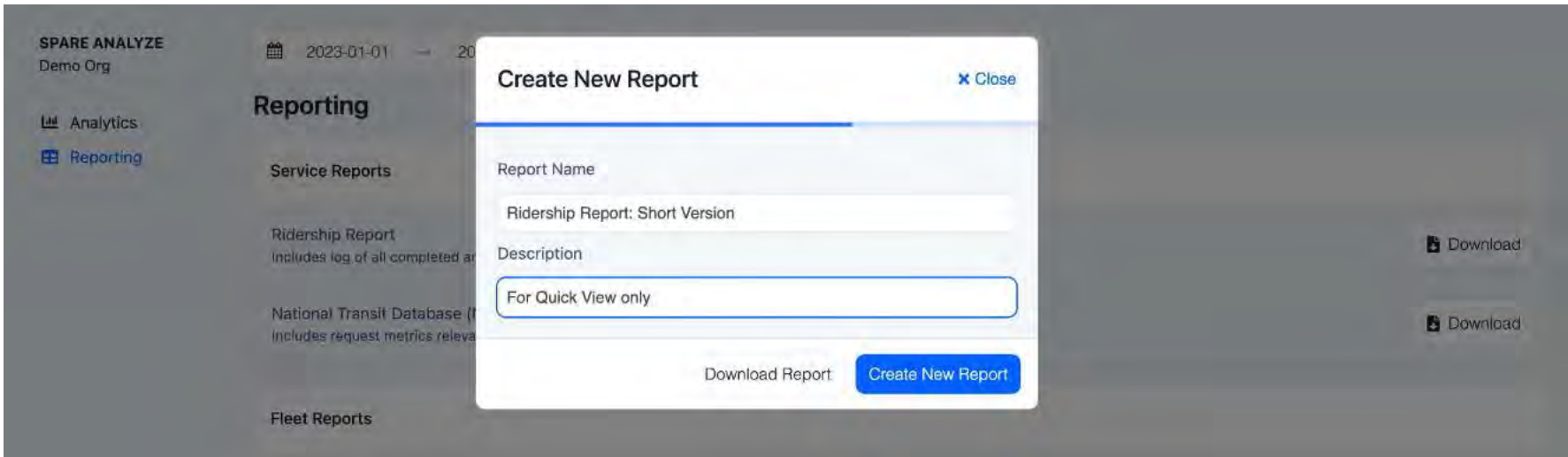


i To view metrics definitions, go to Section 5. Report Metrics Cheat Sheet of this guide.

4.2. How to Build Custom Reports

3 Add Description

Name the report and add a description.



4 Save or Download the Report

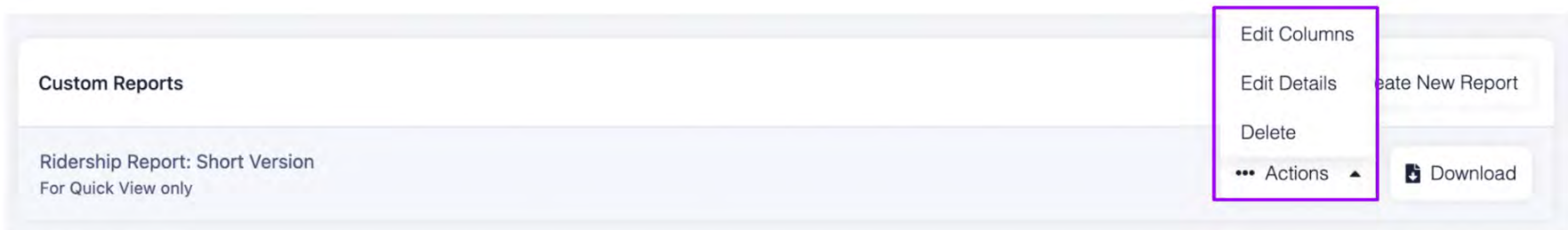
Decide if you want to download the report on your device or save the report on the platform.

→ The **"Create New Report"** option will save the report in the Custom Reports section and will allow you to edit and download the report later.

→ The **"Download Report"** option will generate the report in the CSV or XLSX file but will not create a record in the Custom Reports section.

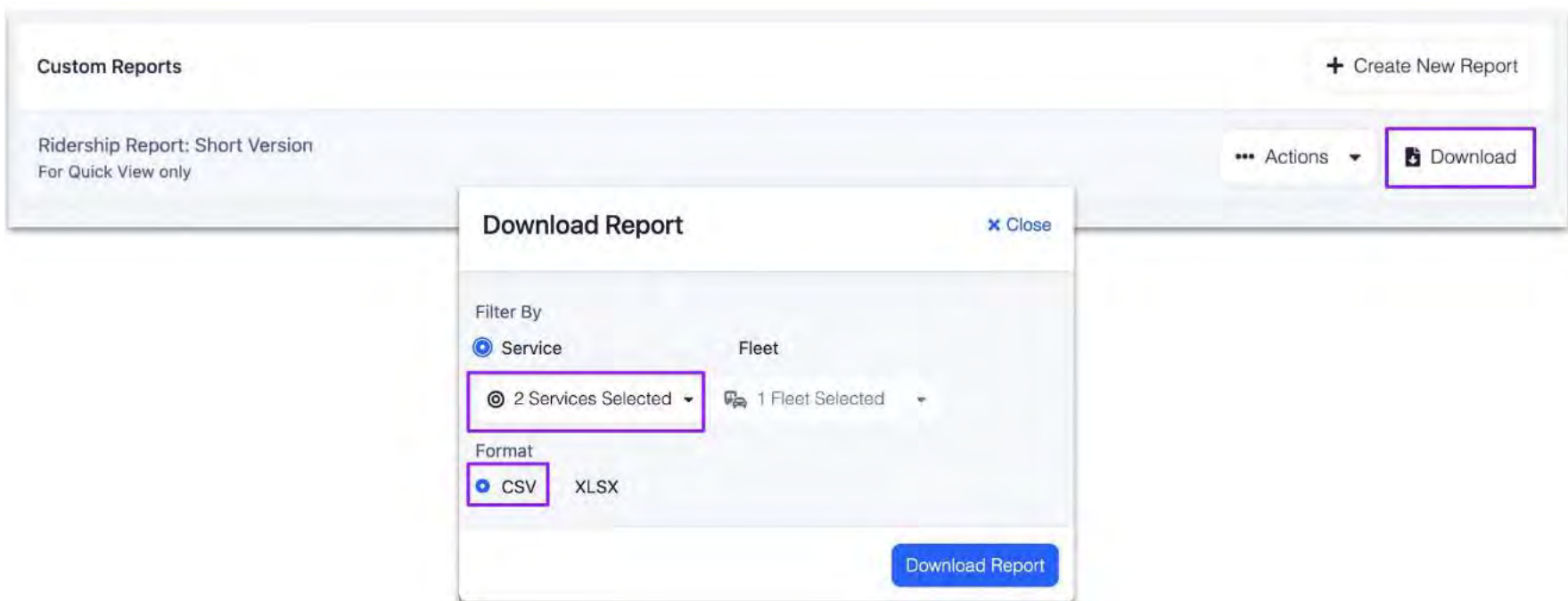
5 Edit the Report

To edit a custom report, click **Actions** next to the report name in the Custom Reports section. You can edit the report columns, name, and description or delete the report.



6 Download the Report

Click **Download**. A pop-up menu will appear. Narrow down your report to the specific **fleet(s)/service(s)** and select the file type: **CSV or XLXS**. Click **Download Report** to retrieve it on your device.



4.1. How to Access and Download Reports

1 Access the Reporting Dashboard

To access Spare Reports, in **Spare Analyze**, go to the **Reporting** tab.



2 Select the Report Type

You will see there are 5 types of reports currently available that are related to two report groups: **Service Reports** and **Fleet Reports**.

Refer to the table below to learn about each of the 5 reports.

1. Service Reports	2. Fleet Reports
1.1. Ridership Report (Service): includes log of all completed and cancelled trips	2.1. Duty Report: includes Includes log of all completed and cancelled duties and their metrics.
1.2. NTD Report (Service): Includes request metrics relevant to NTD reporting	2.2. NTD Report(fleets): Includes request and duty metrics relevant to NTD reporting
	2.3. Ridership Report (Fleet): includes log of all completed and cancelled trips



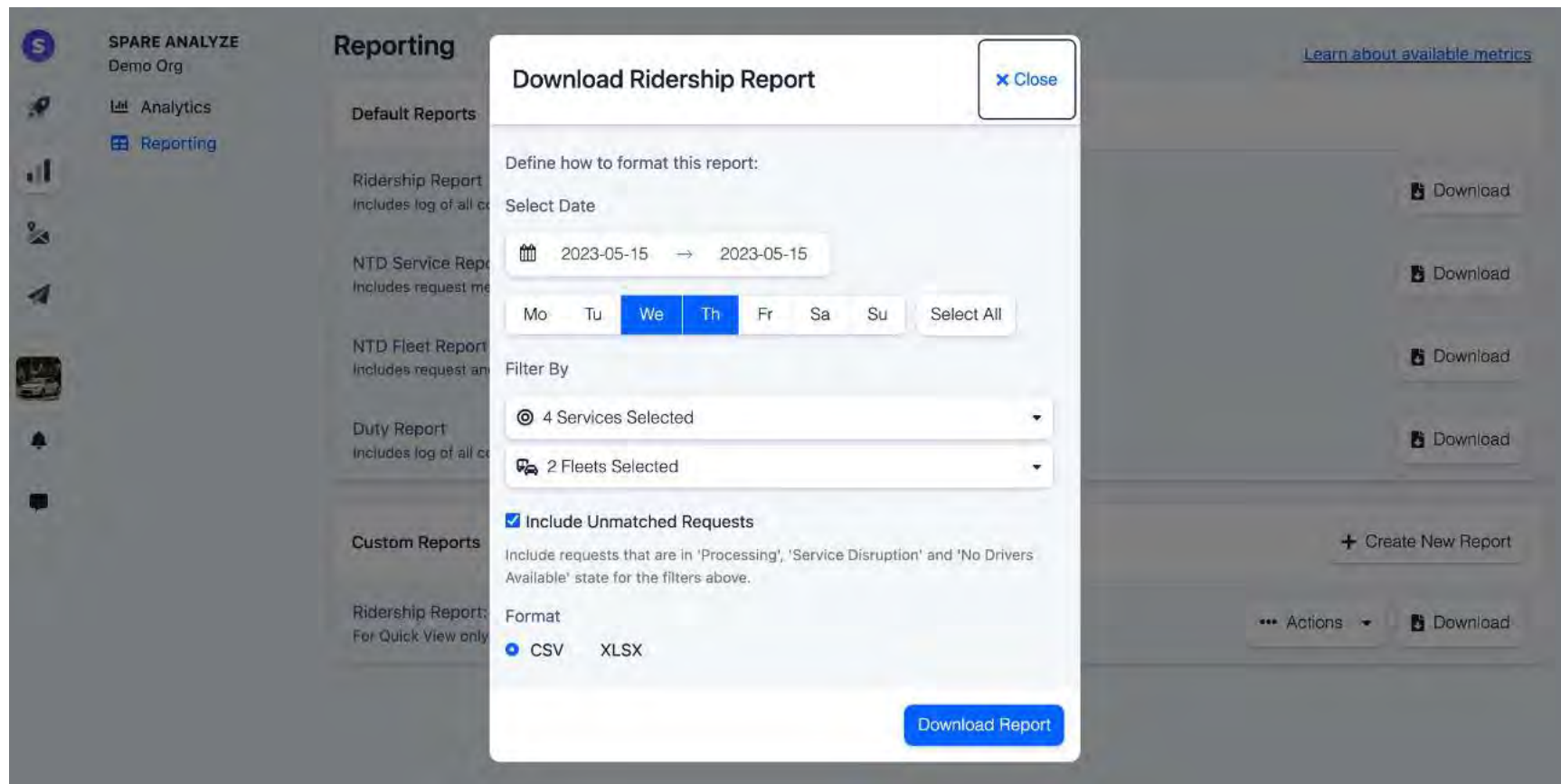
You can also build custom reports. To find out how to do it, go to the section 4.2 of this guide.

4.1. How to Access and Download Reports

3 Set the Parameters and Download the Report

Click “Download” and set the following parameters:

- Date range;
- Days of the week;
- Fleet(s) or service(s) to be included into the report;

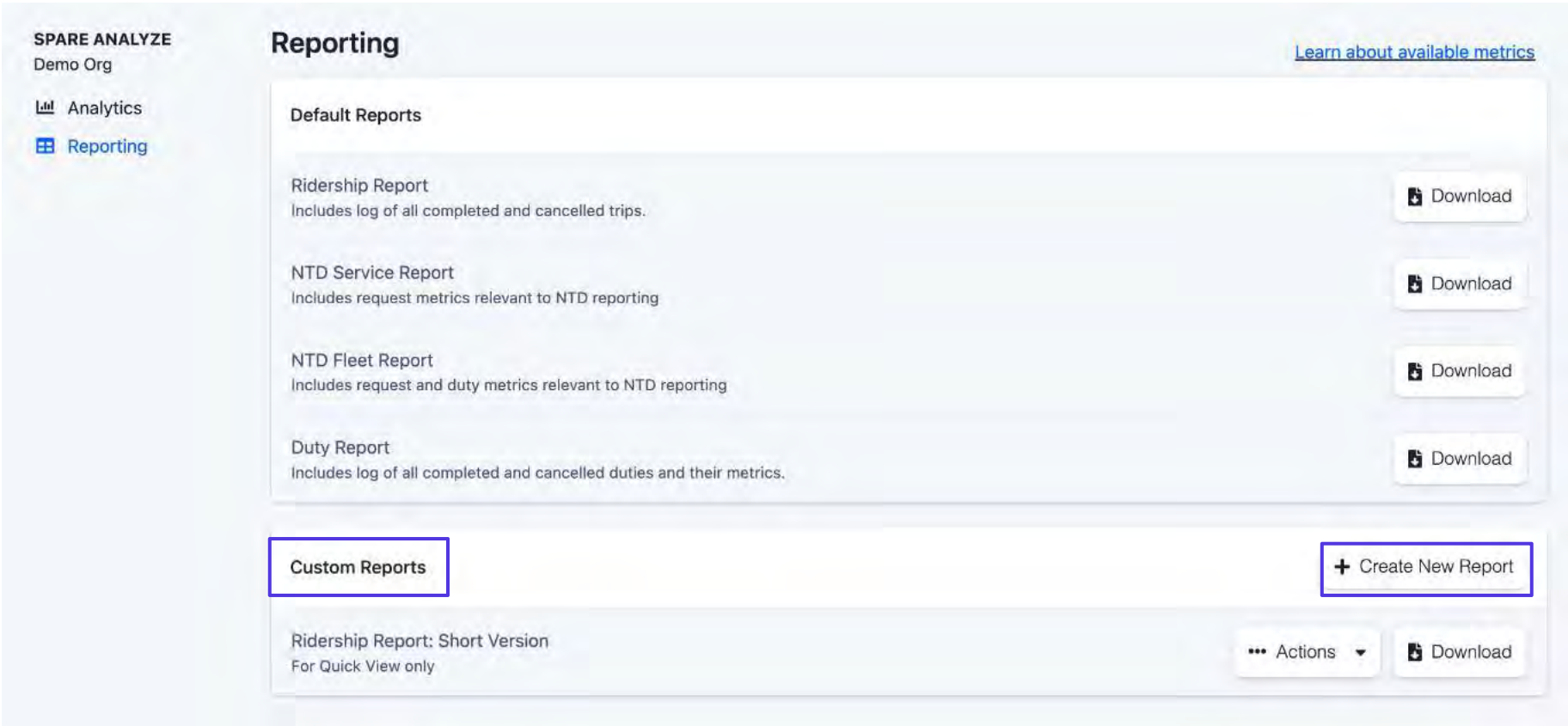


Finally, select either a **CSV** or **XLSX** file type and click **Download Report** - both will open in Excel and Google Sheets.

4.2. How to Build Custom Reports

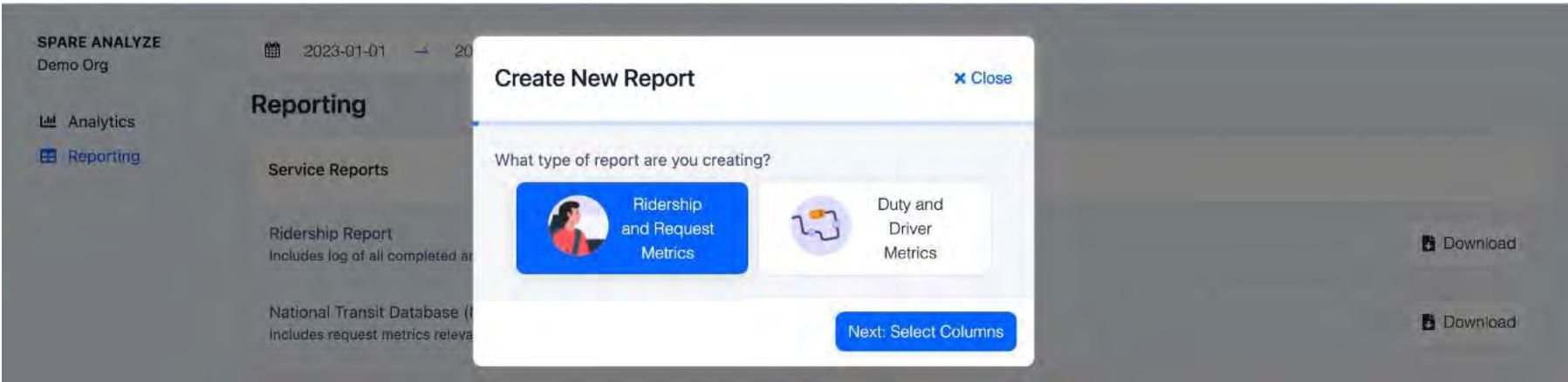
1 Create a New Report

Spare Reports are customizable! To build a custom report, click **+ Create New Report** in the **Custom Reports** section.

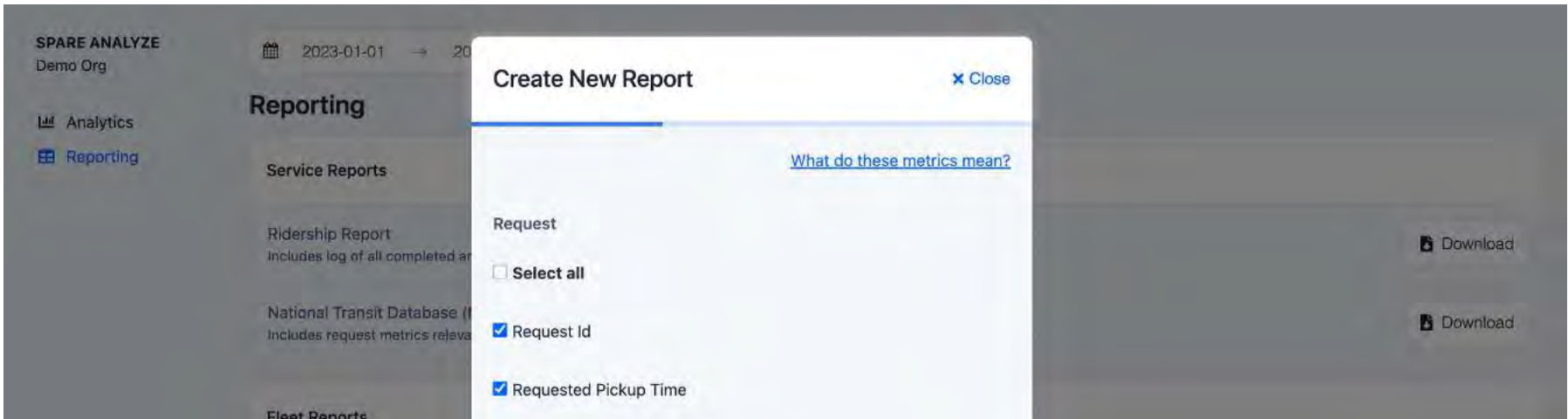


2 Select the Metrics

→ Choose what metrics you'd like to include: **Ridership Metrics** or **Duty Metrics**:



→ **Select the metrics** you need and scroll down to click **Next: Name and Save**

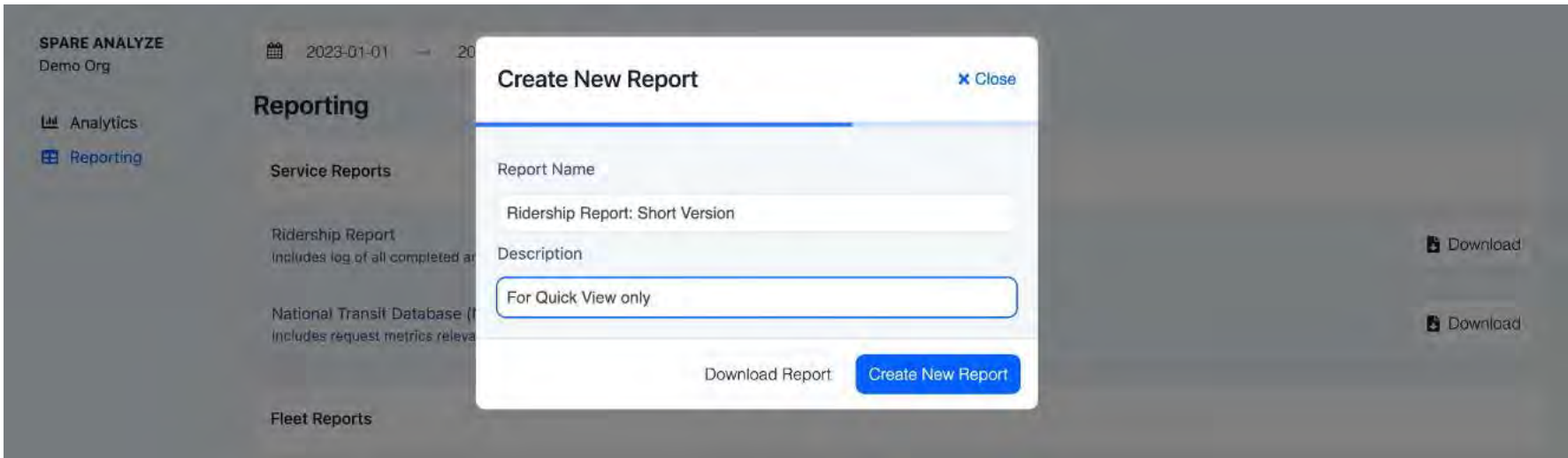


i To view metrics definitions, go to Section 5. Report Metrics Cheat Sheet of this guide.

4.2. How to Build Custom Reports

3 Add Description

Name the report and add a description.



4 Save or Download the Report

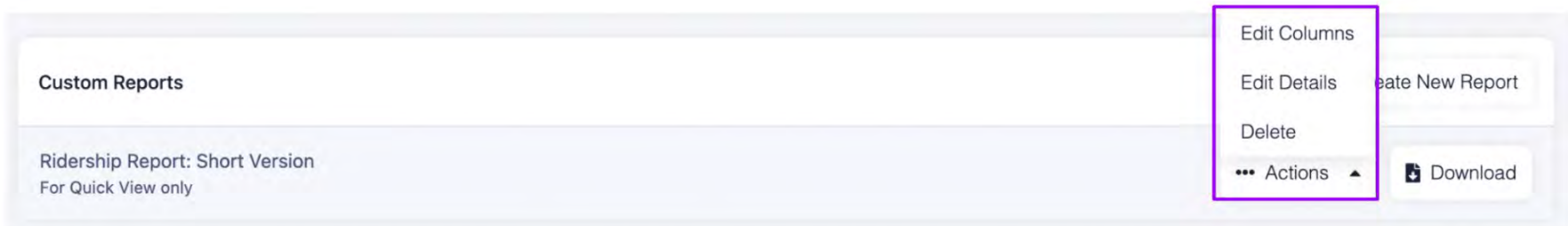
Decide if you want to download the report on your device or save the report on the platform.

→ The **"Create New Report" option** will save the report in the Custom Reports section and will allow you to edit and download the report later.

→ The **"Download Report" option** will generate the report in the CSV or XLSX file but will not create a record in the Custom Reports section.

5 Edit the Report

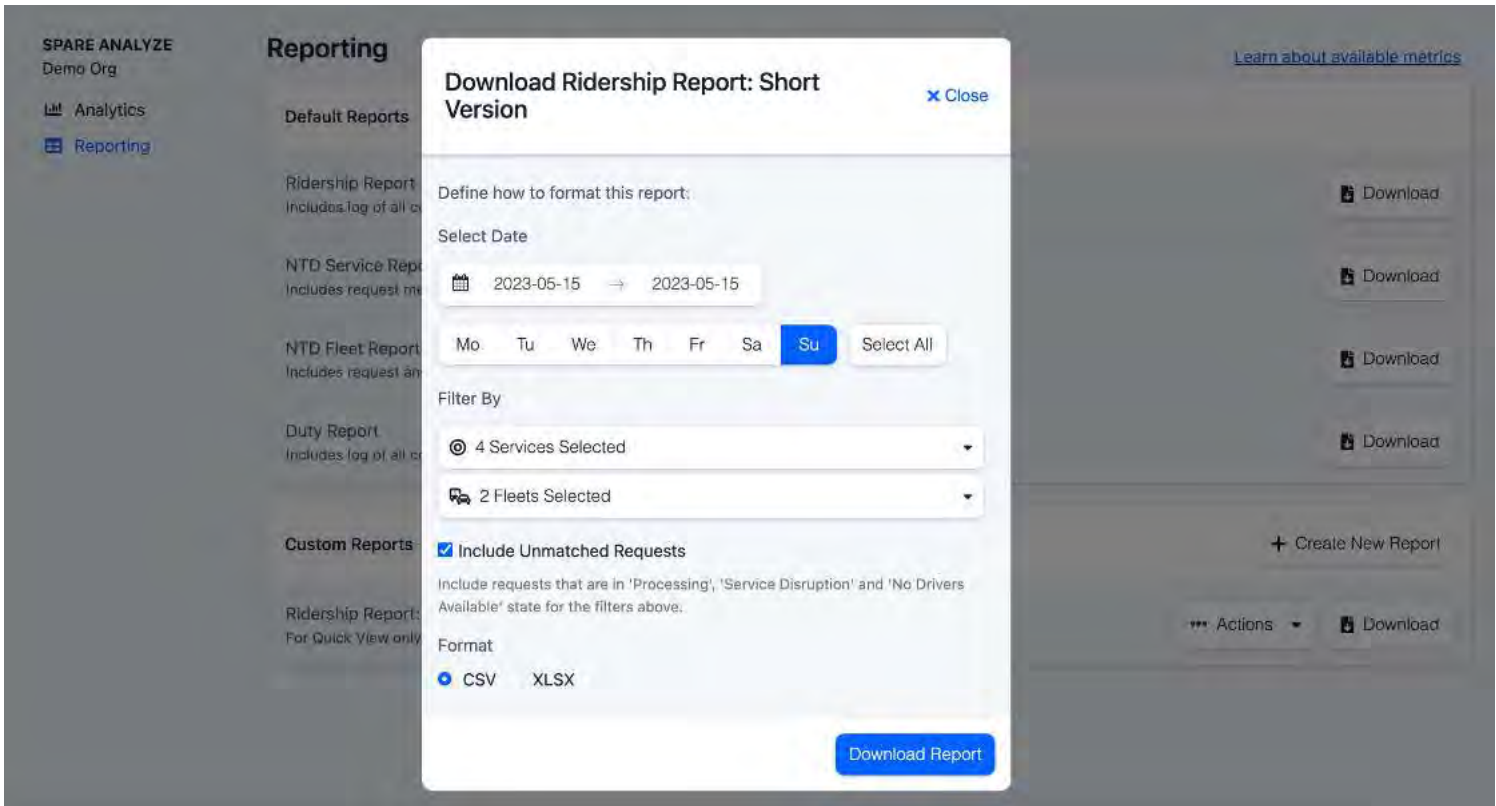
To edit a custom report, click **Actions** next to the report name in the Custom Reports section. You can edit the report columns, name, and description or delete the report.



6 Download the Report

Click **Download**. A pop-up menu will appear. Narrow down your report to the specific **date range**, **days of the week (if applicable)**, or **fleet(s)/service(s)**. **Select the file type: CSV or XLXS.**

Click **Download Report** to retrieve it on your device.



4.3. How to Set Up Automated Reports



You need to have either the **Admin** or **Access to Reporting** role in the organization to be able to set up the automated reports function. If you do not have either of these permission roles, please contact your account administrator.

1 Choose Frequency

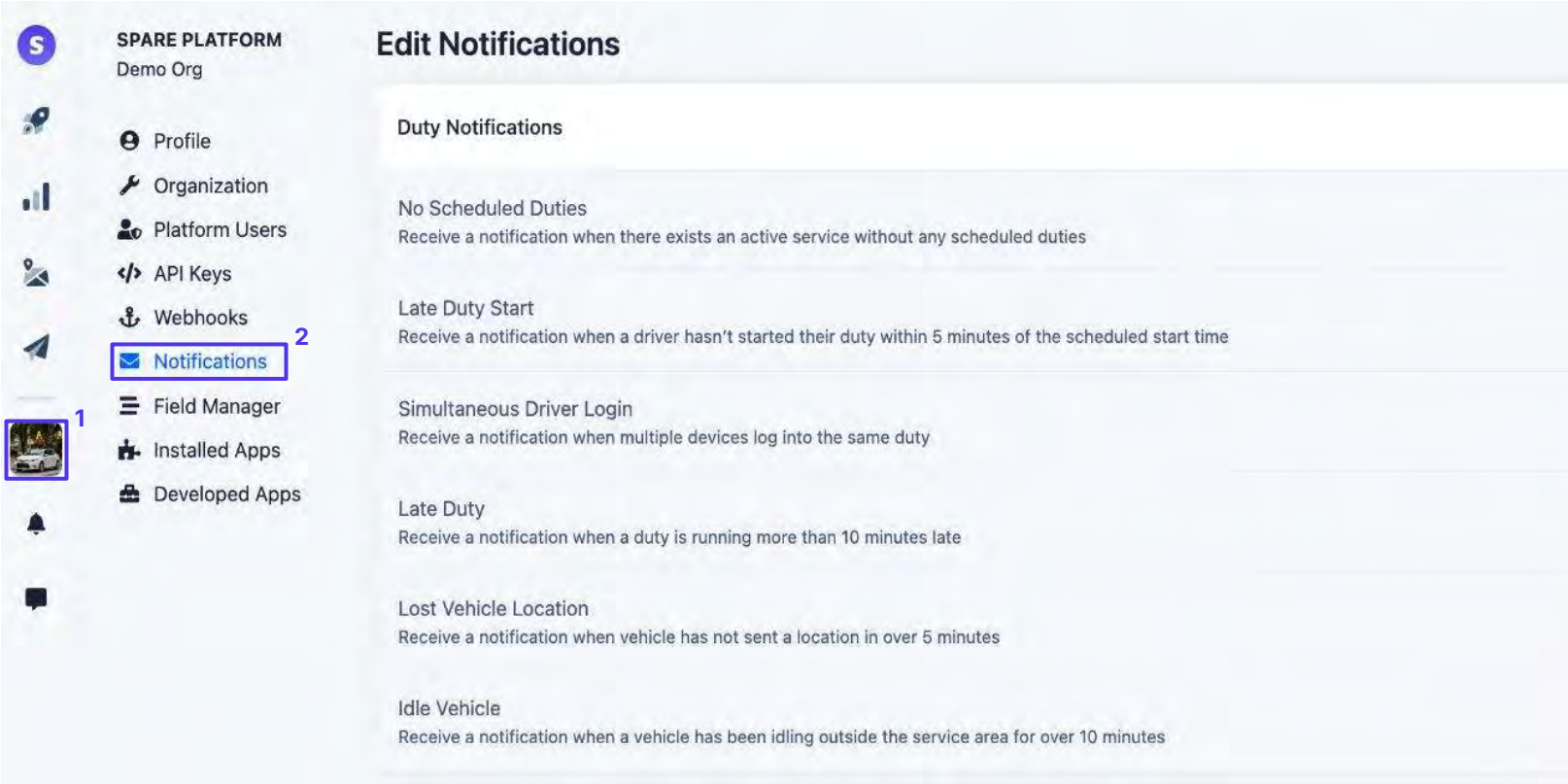
There are two types of automated reports currently available:

Spare Automated Weekly Report: ✓ Emailed every Tuesday, 8 a.m. local time; ✓ Range: Monday-Sunday, previous week; ✓ Contains: 9 Key Metrics	Spare Automated Daily Report: ✓ Emailed daily, for service days only;; ✓ Range: last 24 hours; ✓ Contains: 9 Key Metrics

2 Subscribe to Emails

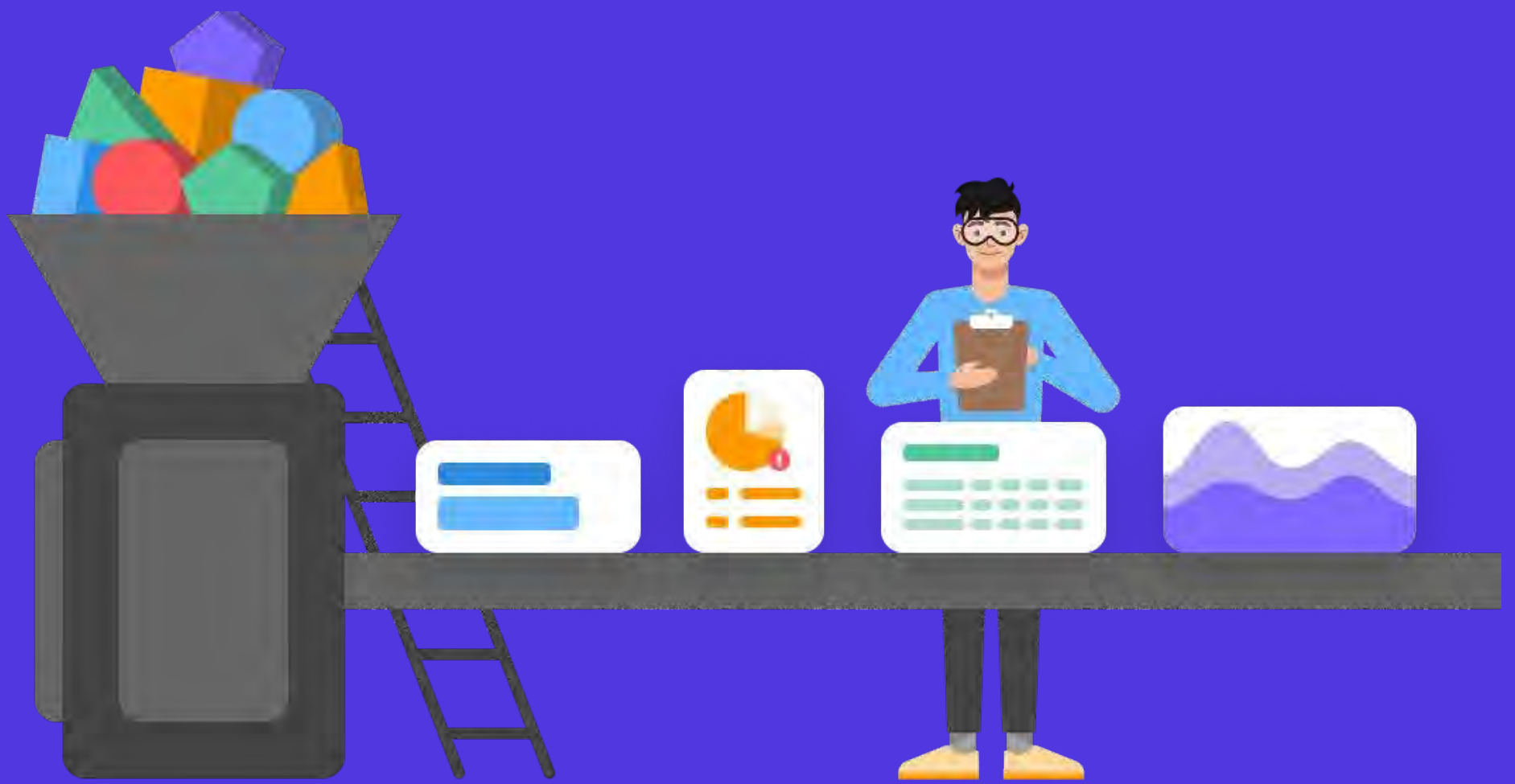
To receive reports via email:

1. Go to your **Organization icon**[1] and click **Settings**.
2. Jump into the **Notifications tab**[2] and **scroll down** to **Email Reports**[3].
3. Use the **dropdown menu**[4] to select the report you'd like to receive.



Scroll Down ↓





[5] Report Metrics Cheat Sheet

- Ridership Metrics
- NTD Metrics
- Duty Metrics

5.1. Ridership Metrics

Metric Name	Metric Definition
Request	
Request ID	The unique system-generated alpha-numeric code used to identify the trip request.
Requested Pickup Time	The requested pickup date and time from the rider.
Requested Pickup Address	The requested pickup address from the rider.
Requested Pickup Longitude	The longitudinal coordinate of the requested pickup location.
Requested Pickup Latitude	The latitudinal coordinate of the requested pickup location.
Requested Dropoff Time	The requested date and time of the dropoff from the rider.
Requested Dropoff Address	The requested dropoff address from the rider
Requested Dropoff Longitude	The longitudinal coordinate of the requested dropoff location.
Requested Dropoff Latitude	The latitudinal coordinate of the requested dropoff location.
Original Scheduled Pickup Time	The original pickup date and time that was communicated to the rider when the trip request was created.
Scheduled Pickup Time	The scheduled date and time of the trip request’s pickup. Gets updated in real time by Spare Engine.
Scheduled Pickup Address	The address where the vehicle will pick up the rider. This location can differ from the rider’s requested pickup address if the location falls within a stop zone. Spare Engine will determine a stop near the rider’s requested pickup address that they will be directed to walk to.
Scheduled Pickup Longitude	The longitudinal coordinate of the scheduled pickup location.
Scheduled Pickup Latitude	The latitudinal coordinate of the scheduled pickup location.
Scheduled Dropoff Time	The scheduled date and time of the dropoff at the scheduled dropoff address. Gets updated in real time by Spare Engine.
Scheduled Dropoff Address	The address where the vehicle will drop off the rider. This location can differ from the rider’s original trip request dropoff address if the location falls within a stop zone. Spare Engine will determine a stop near the rider’s requested destination and direct them to walk from the dropoff point to their final destination.
Scheduled Dropoff Longitude	The longitudinal coordinate of the scheduled dropoff location.
Scheduled Dropoff Latitude	The latitude coordinate of the scheduled dropoff location.
Pickup Walking Duration (seconds)	The estimated time required for the rider to walk from their requested pickup location to their scheduled pickup location.
Dropoff Walking Duration (seconds)	The estimated time required for the rider to walk from their scheduled dropoff location to their requested final destination.
Notes	Comments made within the “notes” section of a trip request booked from the Spare Admin Panel.
Status	The status of the trip request at report export. Statuses include: • Accepted: The trip request is scheduled to a driver’s manifest. • inProgress: The rider is on board and the trip is in progress” • Canceled: The trip request was canceled. • Completed: The driver has completed the trip. • driverArriving: The driver is pulling up to the pickup location. • noDriversAvailable: The system is unable to match a driver to the trip request.

5.1. Ridership Metrics

Metric Name	Metric Definition
Request	
Pickup Arriving At Time	The date and time when the rider receives a notification that their driver is about to arrive. Trip request changes to <i>Arriving</i> status. The vehicle should be approximately two minutes from the scheduled pickup location. Notification is triggered up to 4 minutes before the scheduled pickup time.
Pickup Completed At	The date and time when the driver confirms via the Spare Driver app that the pickup is completed. Trip request changes to <i>In Progress</i> status.
Request Cancelled At	The date and time when the trip request was canceled.
Dropoff Completed At	The date and time when the driver confirms via the Spare Driver app that the dropoff is completed. Trip request changes to Completed status.
In Vehicle Trip Distance	The actual distance traveled by the rider during the trip.
Trip Duration (minutes)	The actual duration traveled by the rider during the trip.
Trip Wait (minutes)	The time between the requested pickup time and the pickup completed time. This is only calculated for “leave soon as possible” trip requests.
Estimated Trip Distance (meters)	The estimated distance to be traveled by the vehicle between the specified pickup and dropoff location at the time of booking. Does not account for any potential detours due to pooling. Units are configured based on organization settings.
Estimated Trip Duration (minutes)	The estimated trip duration determined at the time of booking. Does not account for any potential detours due to pooling or any other factors on the day of the trip.
Equivalent Fixed Route Travel Time	* Available in Dispatch Package * The equivalent trip time is calculated using Google Directions API and is displayed in minutes and includes walking time and transfer time if applicable, as well as total in-vehicle travel time
Request Accepted Time	The time and date when the trip request was added to the driver’s manifest - currently in unix time. Note that if a request has been rematched to multiple duties, this will be the time at which it was added to the most recent duty.
Deadhead to Pickup	The total distance traveled from the driver’s last stop to the pickup location of the next trip when no other riders were on board.
Created By	The name of the user who originally created the trip request, whether a booking agent, a driver (via “flag down”), or the rider themselves. If the creator has left this organization or has deleted their account, this will be blank.
Created At Time	The date and time that the trip request was created.
Rider	
Rider ID	The unique system-generated alpha-numeric code used to identify the profile of the rider for whom this request was booked.
Rider Name	The name of the rider.
Number of Riders (Adult)	The number of adults indicated on the trip request.
Number of Riders (Infant)	The number of infants aged 0-3yr indicated on the trip request.
Number of Riders (Child)	The number of children aged 4-10yr indicated on the trip request.
Number of Riders (Youth)	The number of children aged 11-16yr indicated on the trip request.

5.1. Ridership Metrics

Metric Name	Metric Definition
Rider	
Number of Riders (Senior)	The number of seniors indicated on the trip request.
Number of Riders (Student)	The number of students indicated on the trip request.
Number of Riders (Disabled)	The number of riders with a disability indicated on the trip request.
Number of Riders (Veteran)	The number of veterans indicated on the trip request.
Number of Riders (Reduced)	The number of riders indicated as the reduced rider type on the trip request.
Number of Riders (Personal Care Attendant)	The number of personal care attendants that join the rider and are added to the total number of boardings recorded for each vehicle/duty.
Number of Riders (Other)	The number of riders indicated as ‘other’ on the trip request.
Accessibility Features	
Accessibility Stroller Count	The number of strollers indicated on the trip request.
Accessibility Wheelchair Count	The number of wheelchairs indicated on the trip request.
Accessibility Child Seat Baby Count	The number of child seats needed on the trip request for children aged 0-3yrs.
Accessibility Child Seat Young Count	The number of child seats needed on the trip request for children aged 4-10yrs.
Accessibility Service Animal Count	The number of service animals indicated on the trip request.
Number of Bikes	The number of bikes indicated on the trip request.
Number of Oversized Wheelchairs	The number of oversized wheelchairs indicated on the trip request.
Number of Lifts	The number of wheelchair lifts or ramps needed on the trip request.
Number of Walkers	The number of walkers indicated on the trip request.
Number of White Cane Seats	The number of white cane seats indicated on the trip request.
Number of Door to Door Stops	The number of actual door-to-door pickups and dropoffs the driver made.
Number of Stretchers	The number of emergency and transport stretchers needed on the trip request.
Number of Folding Wheelchairs	The number of folding wheelchairs indicated on the trip request.
Duty	
Duty ID	The unique system-generated alpha-numeric code used to identify the duty to which the trip request was matched (if it was matched).
Driver	
Driver Name	The name of the driver the trip request is assigned to.
Driver Location On Match Longitude	Longitude of the driver’s location when the trip request was matched to the driver, or empty if the trip request was matched before the duty started. Considers the trip request’s most recent match.
Driver Location On Match Latitude	Latitude of the driver’s location when the trip request was matched to the driver, or empty if the trip request was matched before the duty started. Considers the trip request’s most recent match.

5.1. Ridership Metrics

Metric Name	Metric Definition
Vehicle	
Vehicle License Plate	The license plate of the vehicle that the trip request is assigned to.
Vehicle Identifier	The identifier of the vehicle the trip request is assigned to.
Service	
Service Name	The name of the service the trip request is assigned to.
Fleet	
Fleet Name	The name of the fleet that the duty and trip request are assigned to.
Fleet Type	A fleet can be one of three types: Auto Accept, Accept / Reject, External.
Estimate	
Created Interface	The channel the trip request was created from: Admin Interface, Rider Web Interface, Rider Mobile app, Driver App.
Estimate Created At Time	Time of the most recent estimate obtained by the rider before booking a trip request.
Estimate Endpoint	Whether the trip request was booked as a “next available” “scheduled” (i.e. advanced booking) or flagdown
Zone	
Pickup Zone Name	The name of the selected zone where a rider’s pickup will occur.
Dropoff Zone Name	The name of the selected zone where a rider’s dropoff will occur.
Slot	
Pickup Completed Distance Deviation	Straight line distance between the scheduled pickup location and completed location.
Dropoff Completed Distance Deviation	Straight line distance between the scheduled dropoff location and completed location.
Request Cancellation	
Cancellation Cancelled By	If the trip request is canceled, the system will log (admin, rider, driver) who made the cancellation.
Cancellation Fault	The cancellation fault, this can be ‘riderFault’, ‘noFault’, or ‘driverFault’. The fault is logged when a cancellation is made.
Cancellation Reason	The cancellation reasoning indicated on the trip request (e.g. no show).
Cancellation Notes	Notes added to the cancellation by the reservationist or rider, depending on who cancelled the trip.
Fare	
Fare Cost	The total fare cost of the trip. Calculated before the trip request is matched, so does not take into account detour due to pooling. Currency configured on a per organization basis.
Fare Discount	The total discount applied to the rider’s fare, based on any promos or fare passes applied to this trip request.

5.1. Ridership Metrics

Metric Name	Metric Definition
Tip	
Tip	The tip amount provided by the rider (for services where tipping is enabled).
Tip Created Time	If the rider leaves a tip, the date and time that the tip was created.
Payment Method	
Payment Method ID	The unique system-generated alpha-numeric code given to the payment method attached to the trip request.
Payment Method Connected Account Type	The payment method chosen by the rider to pay for their trip.
Promotion	
Promo Names	If a promotion is applied to the rider’s trip request, the name of the promotion will be shown here.
Promo Discounts	If a promotion is applied to the trip request, the discounted amount given by the promotion will be shown here.
Review	
Rider Rating	The rating provided by the rider on the trip request. Standard is thumbs up equals 100% and thumbs done equals 0%.
Rider Review Tags	The tags selected by the rider when completing a review for their trip.
Rider Comment	The comment that the rider left for the trip request in the rider application.
Fare Pass	
Fare Pass Names	If a fare pass is applied to the rider’s trip request, the name of the fare pass will be shown here.
Fare Pass Discounts	If a fare pass is applied to the rider’s trip request, the discounted amount given by the fare pass will be shown here.
Request Recurrence	
Recurrence ID	The related recurring trip ID if the trip request was automatically generated by a recurring trip request.

5.2. National Transit Database (NTD) Metrics

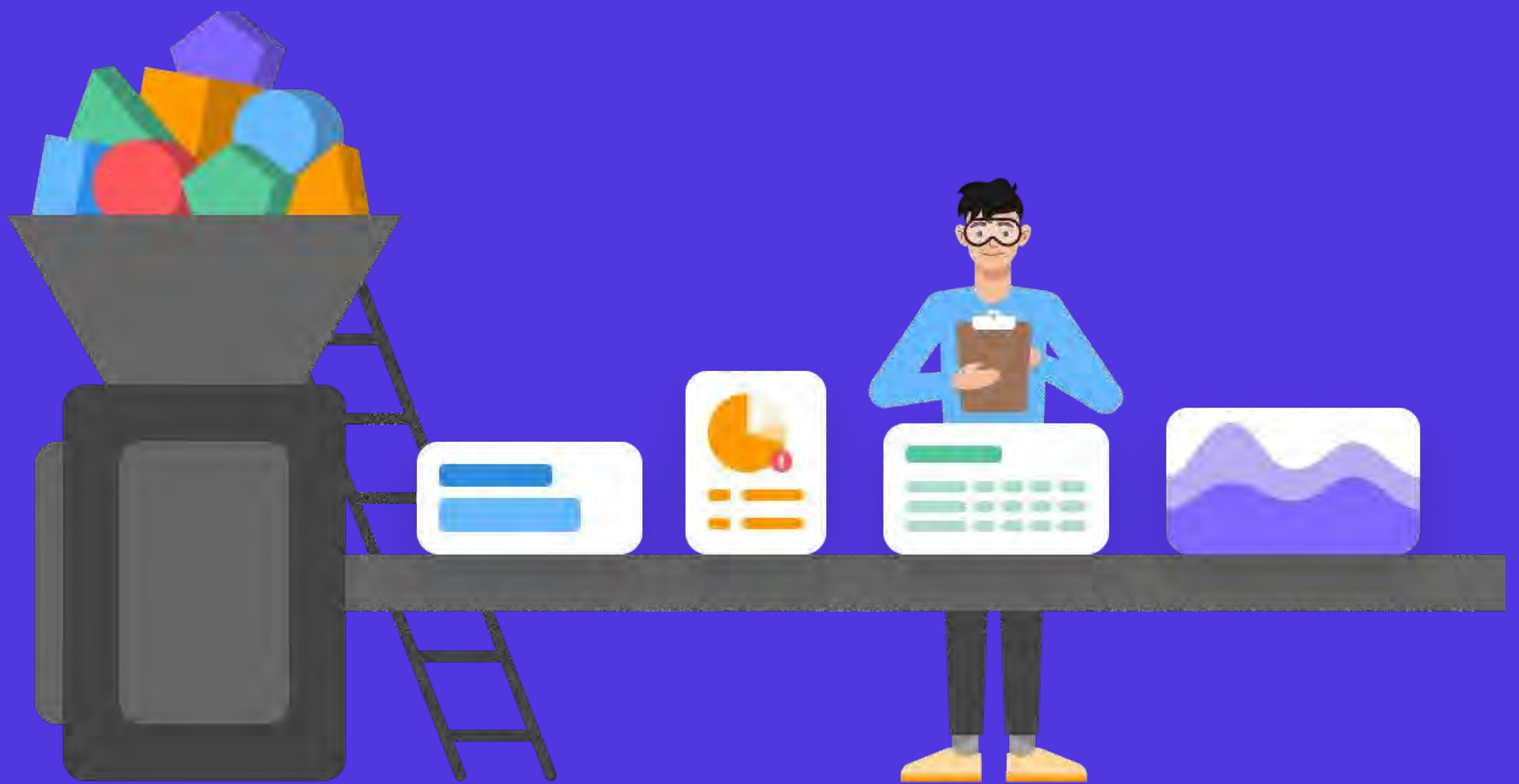
Metric Name	Metric Definition
Request	
Number of Completed Boardings	Total number of riders who successfully completed their trip
Number of Completed Requests	Total number of requests successfully completed
Number of Cancelled Requests	Total number of requests cancelled
Number of No Show Requests	Total number of requests whose rider was a 'No Show'
Duty	
Vehicle Hours	Total number of hours scheduled for all vehicles in the fleet.
Total Scheduled Vehicle Hours	Total number of hours scheduled for all vehicles in the fleet.
Total Actual Vehicle Hours	Total time recorded for all vehicles in the fleets. This takes into account when the duty was actually started, completed and cancelled.
Total Actual Vehicle Distance (km)	Total distances travelled as recorded by the Driver App for each vehicle in the fleets selected.
Revenue Hours	Total hours in revenue service based on the time of the first completed pickup to last completed dropoff.
Revenue Distance (km)	Total distance from the first completed pickup to the last completed dropoff. Same "vehicle locations between times polyline" approach as "Vehicle Distance"
Total Break Hours	The total hours of all breaks taken by all duties on this date
Total Break Distance (Meters)	The total distance driven during breaks taken by all duties on this date
Additional	
Date	The Date that this row corresponds to. Requests/duties are included in the aggregate metrics for this row if their <code>request.requestedPickupTs</code> was on this date. Only <code>Completed</code> and <code>Cancelled</code> requests are included

5.3. Duty Metrics

Metric Name	Metric Definition
Driver	
Driver Name	The name of the driver assigned to the duty.
Duty	
Duty ID	A unique system-generated alphanumeric code used to identify the driver profile.
Duty Created Time	The date and time when a driver's duty was created.
Duty Scheduled Start Time	The date and time that the duty is scheduled to begin.
Duty Scheduled End Time	The date and time that the driver duty is scheduled to end.
Duty Cancelled Time	The date and time the duty was cancelled.
Total Duration (hours)	The total duty duration, from duty actual start time to duty actual end time. If the duty was cancelled, the cancellation time is used as the actual end time.
Total Travel Distance (meters)	The total distance the vehicle traveled during the duty period.
First Seen in Service Area Time	The date and time the duty first entered the service area, as determined by the geographical zone boundaries of the service.
Last Seen in Service Area Time	The date and time a given duty is last in the service area, as determined by the geographical zone boundaries of the service.
Deadhead Travel Distance (meters)	The total distance traveled during the duty when there were no riders on board the vehicle.
Pause Duration While in Progress (minutes)	The total duration of the vehicle being paused while the duty is In-Progress.
Breaks	
Total Break Hours	Total time of all the actual breaks taken by the driver during this duty.
Total Scheduled Break Hours	Total time of all breaks scheduled for the driver during the duty.
Total Number of Breaks	Total number of breaks taken during this duty.
Total Break Distance (unit)	Distance travelled by the driver during their break.
Breaks	A list of the breaks that were assigned to this duty. For each break, includes scheduled time, actual start time, actual completion time and/or cancellation time if the break was cancelled.
Duty Status	The status of the duty at time of report download. The potential statuses are: Scheduled, Completed, Cancelled.
Vehicle	
Vehicle Identifier	A custom value used to internally identify each vehicle within an organization.
Vehicle License Plate	The license plate of the vehicle.

5.3. Duty Metrics

Metric Name	Metric Definition
Fleet	
Fleet Name	The fleet the duty is assigned to.
Fleet Type	The type of fleet the duty is assigned to. A fleet can fall under three categories: Auto Accept, Accept Reject, and External Fleet.
Slot	
Duty Actual Start Time	The date and time when the driver began their duty in the driver app.
Duty Actual Completed Time	The date and time the driver ended their duty in the driver app.
Boarding	
Total Boardings	The total number of riders who completed trips on the duty.
Rider Mobile App Bookings	The total number of bookings made through the Spare Rider mobile app
Rider Web Bookings	The total number of bookings made through the Spare Rider Web interface.
Driver App Bookings	The total number of bookings made through the Spare Driver mobile app (walk-ons).
Admin Panel Bookings	The total number of bookings made through the Spare Platform admin interface.



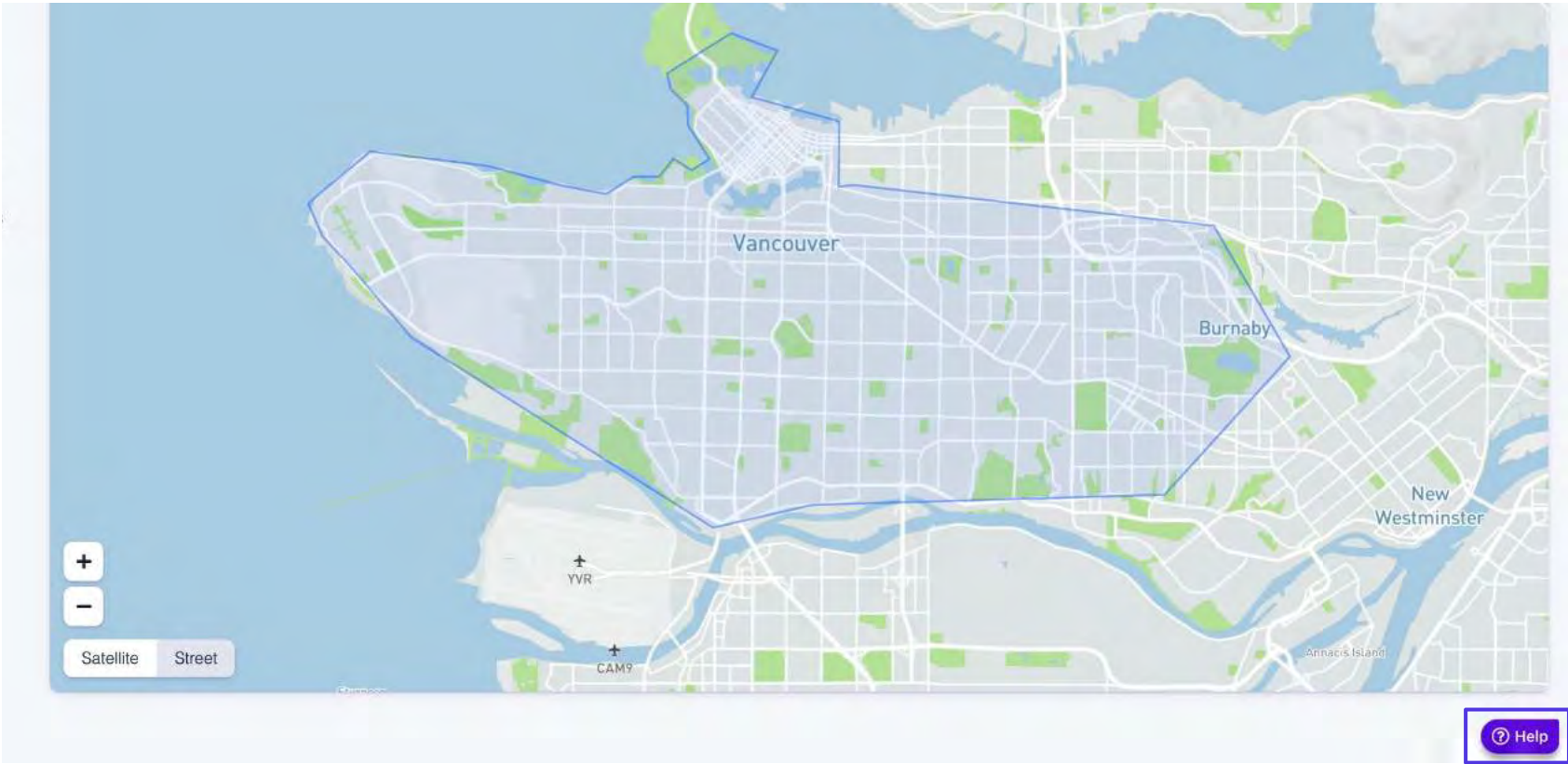
[6] Help & Troubleshooting

- Spare Help Centre
- Spare Tech Support

6.1. How to Reach out for Support

It is easy to **access Spare’s help resources**:

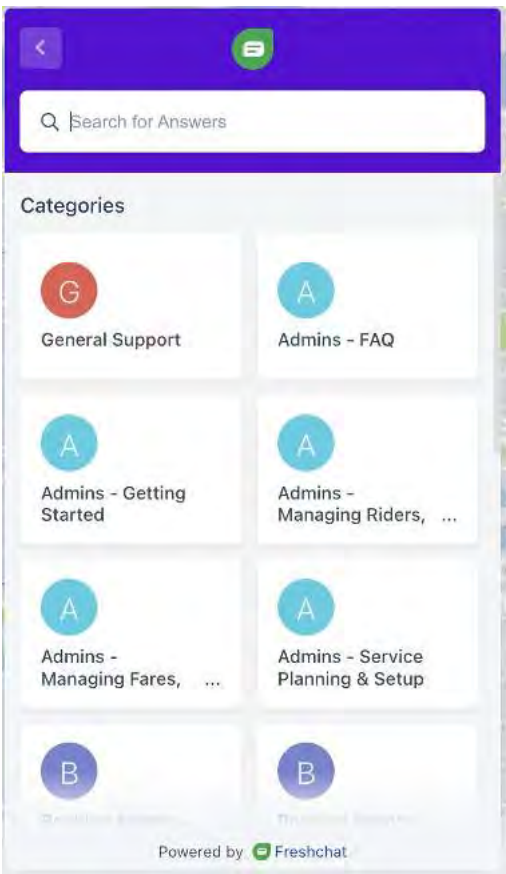
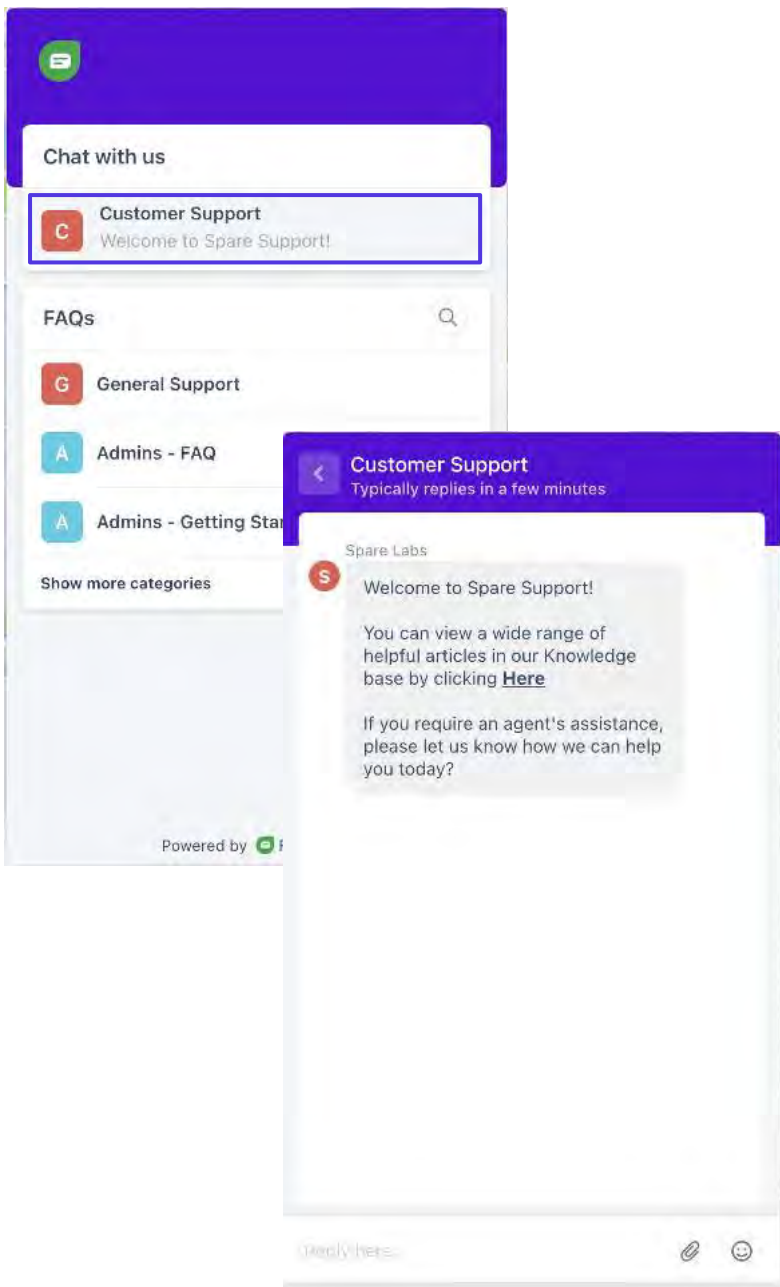
- 1 Click on the **Help widget** in the bottom right corner of the page. A **Help menu** will appear.



- 2 Click “**Customer Support**” to go into the live chat.

From there, you can **access Spare’s Knowledge Base** or **connect with a Tech Support representative**.

- 2 You can also access the **Knowledge Base articles** right from the main widget menu by browsing the **FAQ section**. Feel free to type in the key words in the search bar.

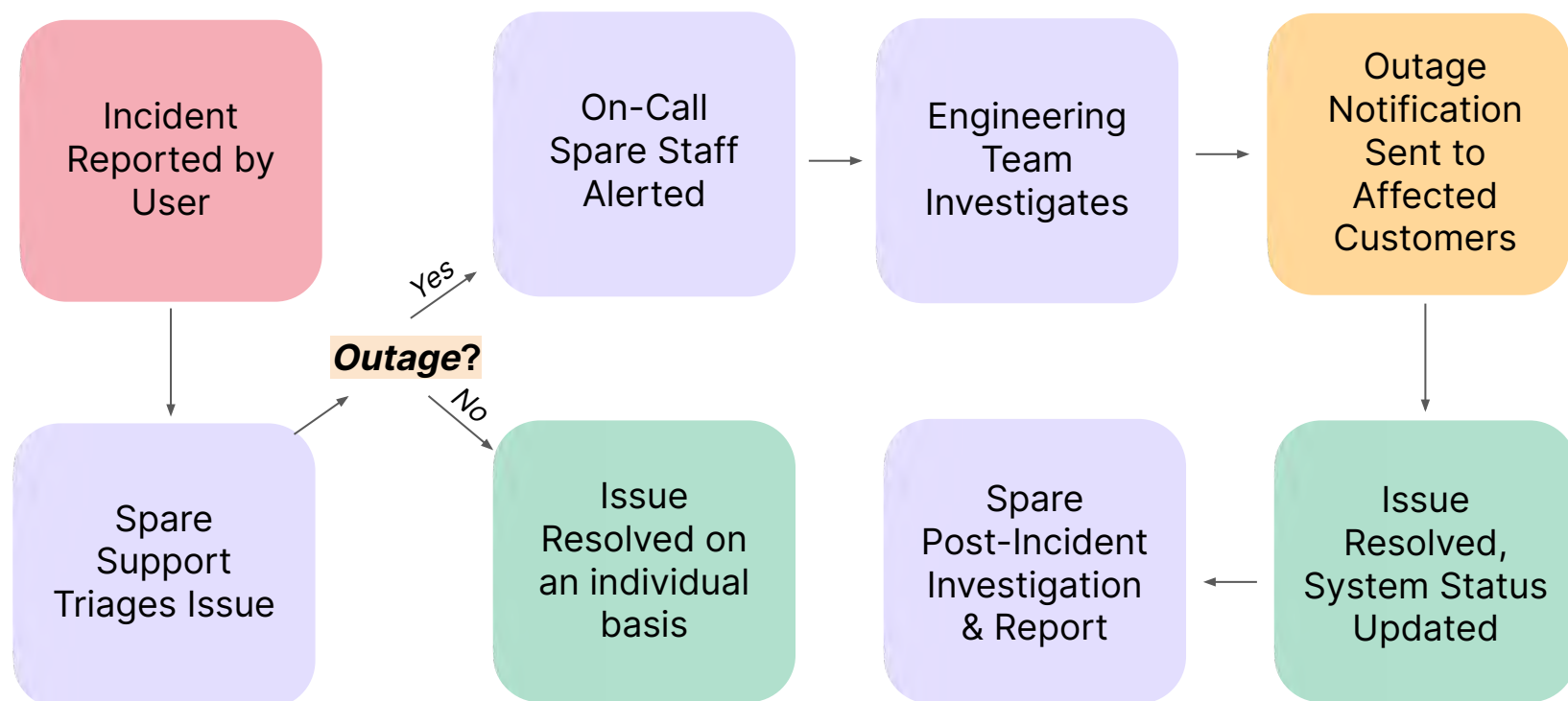




Spare Escalation Procedures

Visit sparelabs.com
815 W Hastings St Suite 810,
Vancouver, BC V6C 1B4
© Spare 2022

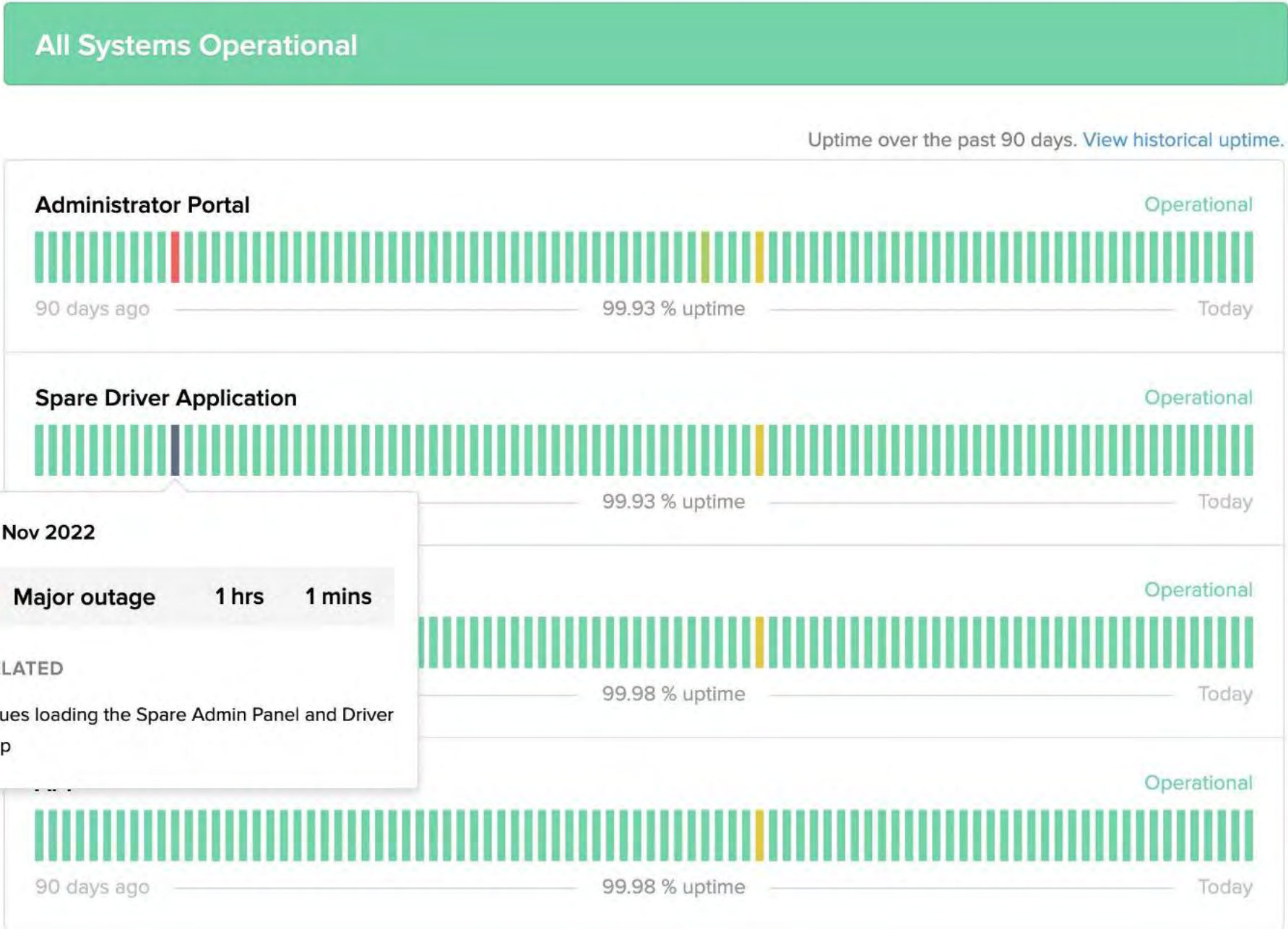
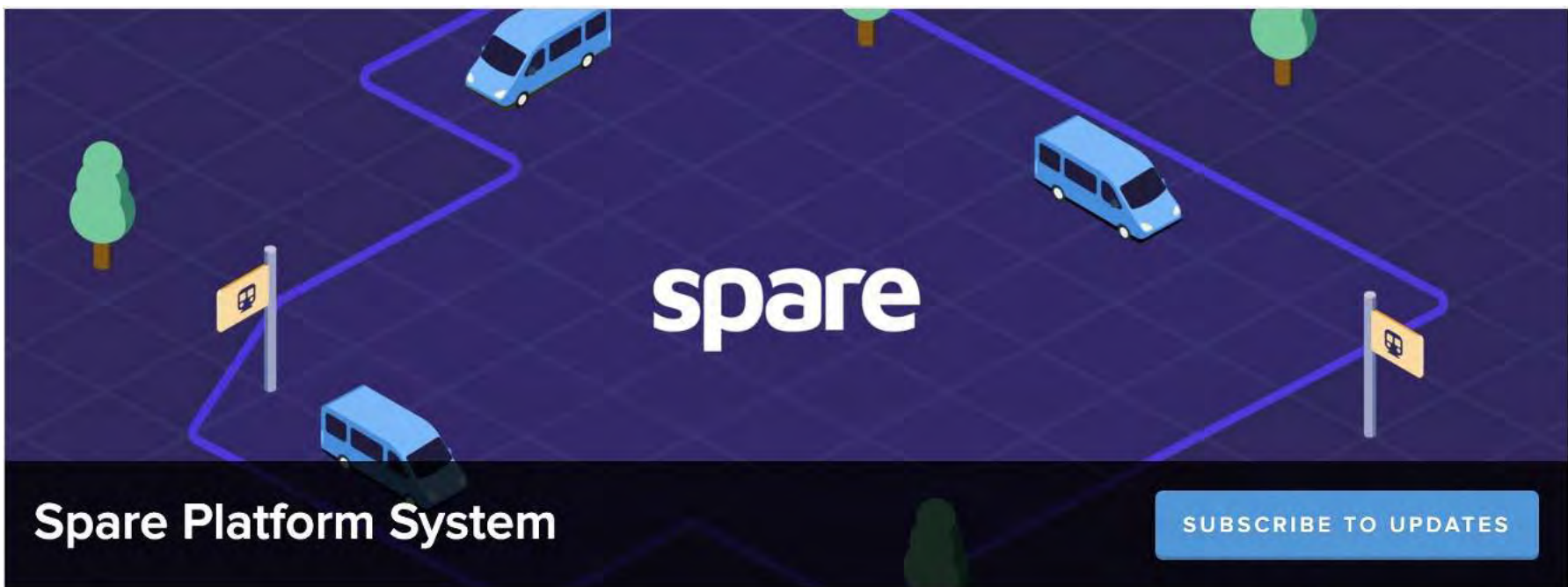
1. Internal Escalation Procedure



1. The user reaches out to Spare via live chat or email (support@sparelabs.com). They should outline the issue that they are experiencing and provide information such as links, screenshots, and other relevant information that can aid in diagnosis.
2. The Spare representative verifies the information presented to them, attempts to reproduce the issue, and then troubleshoots with the reporting user to try to resolve the issue.
3. If the issue being reported is something that is preventing the customer from booking new trips, editing or canceling existing trips, completing trips, creating or managing time-sensitive duties, or accessing the platform, then an outage can be triggered.
4. When an outage is triggered, an alert is sent to an on-call member of Spare's engineering team. On average, on-call alerts are acknowledged within 5 minutes.
5. The engineer assigned to the outage will triage the issue and begin investigating.
6. An internal communications channel is automatically created to provide a central location for outage communications.
7. If the issue is triaged and determined to be a true outage, an email communication is sent to customer outage contacts and the Spare system status page (<https://sparelabs.statuspage.io>) is updated with details.
8. Once the issue has been resolved, a follow-up email will be sent to customer outage contacts and the system status page will be updated.
9. The next business day, a post-mortem will be carried out by our engineering team to identify the root cause of the issue and what preventative measures Spare will take to prevent similar issues from recurring.

2. Spare's Status Page

- 1. Spare's [status page](#) is a reliable source for users to see the status and performance of our platforms (Admin Portal, Driver application, Rider application & API).
- 2. It includes live and historic data showing system uptime as well as any outage events, their descriptions, duration, as well as resolution and post-mortem details.



3. Administrator/Back-Office Escalation Procedure

1. If a back-office user encounters a problem that prevents them from carrying out their normal duties, the user should first:
 - a. Check that they are accessing platform.sparelabs.com from Google's Chrome browser (other browsers are not supported).
 - b. Force refresh the page by holding down (on Windows) the CTRL key and clicking the Refresh button in the top left or by holding down CTRL+F5.
 - c. Try quitting Chrome completely and reopening it.
 - d. Try closing other open programs (this will free up computer memory).
 - e. If the above steps do not resolve the issue, try restarting your computer.
2. If that does not resolve the issue, please contact a manager/administrator in your organization.

Please include:

Normal office hours phone/contact: _____

After-hours phone/contact: _____
3. If a manager or administrator cannot find a solution, contact Spare.

For non-urgent issues, email support@sparelabs.com or contact Spare via Freshdesk, the live chat feature that can be found in Spare Platform or at www.sparelabs.com. Both support@sparelabs.com and Freshdesk are monitored between the hours of 5 am - 11:30 pm PST, 7 days a week and have direct lines to Spare operations and engineering staff. You should receive a response within 10 minutes.

For emergency system disruptions, where a system issue is preventing the reception or delivery of passenger trips for multiple drivers or passengers and the issue needs to be **urgently** resolved to provide immediate rider trips, call our 24/7 response line:

+1 833-866-0771

Before calling, please gather details on the issue, including context and/or pictures and videos, and be prepared to explain the issue and provide information to Spare.

If calling at early or late hours of the day or night, please be advised that you may be waking someone up and that they may need some time to make their way to their computer to begin working on the issue.

4. Driver Escalation Procedure

1. If a driver encounters a problem that prevents them from carrying out their normal duties (i.e., the driver is being prevented from accepting or delivering trips), the driver should attempt to resolve the problem themselves using all the training they have received, the instructional video, and a [quick reference guide](#).
2. Check that the tablet is connected to cellular internet by looking in the top right of the screen to view the LTE label and signal strength.
3. Try quitting the app and reopening it.
4. Try restarting the tablet.
5. Check that the Spare Driver app is the up-to-date version by navigating to the updates section of the app store.
6. If you are running the latest version of the app or the issue still persists after an update, try uninstalling and reinstalling the application and sign in again.
7. If that does not resolve the issue, please contact a manager/administrator in your organization.
 - a. Please include:
 - i. Normal-hours phone/contact: _____
 - ii. After-hours phone/contact: _____
8. If a manager or administrator cannot find a solution, contact Spare.

For non-urgent issues, email support@sparelabs.com or contact Spare via Freshdesk, the live chat feature that can be found in Spare Platform or at www.sparelabs.com. Both support@sparelabs.com and Freshdesk are monitored between the hours of 5 am - 11:30 pm PST, 7 days a week and have direct lines to Spare operations and engineering staff. You should receive a response within 10 minutes.

For emergency system disruptions, where a system issue is preventing the reception or delivery of passenger trips for multiple drivers or passengers and the issue needs to be **urgently** resolved to provide immediate rider trips, call our 24/7 response line:

+1 833-866-0771

Before calling, please gather details on the issue, including context and/or pictures and videos, and be prepared to explain the issue and provide information to Spare.

If calling at early or late hours of the day or night, please be advised that you may be waking someone up and that they may need some time to make their way to their computer to begin working on the issue.

9. If the problem is determined to be a hardware or network issue, Spare will work with your organization to try to find an interim fix - however, please note that Spare's ability to resolve issues related to hardware and/or network issues is limited.

5. Rider Escalation Procedure

1. If multiple rider/end-users encounter problems that prevent them from booking a trip or otherwise utilizing the service, the customer service agent or other person communicating with the rider/end-user should:
 - a. Ask the rider to quit and then reopen the app
 - b. Check to make sure that the rider is connected to the internet
 - c. Check that the rider is using the latest version of the rider app and, if not, ask them to update to the latest version
 - i. If using the Spare Rider app, the version number can be found at the bottom of the account page that is accessed by clicking on the menu button in the top left of the app. The version number can then be compared to the latest version found in the App Store or Google Play Store.
 - ii. If using a proprietary rider app, please check with your organization.
 - d. Ask the passenger to restart their phone and retry.
2. If that does not resolve the issue, please contact a manager/administrator in your organization.

Please include:

Normal-hours phone/contact: _____

After-hours phone/contact: _____
3. If a manager or administrator cannot find a solution, contact Spare.

For issues with the rider app, email support@sparelabs.com or contact Spare via Freshdesk, the live chat feature that can be found in Spare Platform or at www.sparelabs.com. Both support@sparelabs.com and Freshdesk are monitored between the hours of 5 am - 11:30 pm PST, 7 days a week and have direct lines to Spare operations and engineering staff. You should receive a response within 10 minutes.

General Support Service Level Agreement

- Unlimited support via Spare Platform chat and email (support@sparelabs.com)
- Guaranteed response within:
 - 2 hours for inquiries received from 5am-5pm PST on weekdays, (excluding Canadian holidays)
 - 48 hours for inquiries received on weekends (excluding Canadian holidays)
 - 48 hours for inquiries received on Canadian holidays

Critical Incident Support Service Level Agreement

- 24/7, 365 automated monitoring of Spare Platform core functionalities with automated on-call personnel alerts
- 24/7, 365 on-call support and engineering personnel
- 24/7, 365 emergency support phone number
- Support via Spare Platform chat and email (support@sparelabs.com)
- Guaranteed response within:
 - 30 mins for P1 Urgent Severity Issues
 - 120 mins for P2 High Severity Issues

P1 Urgent Severity: A critical system failure in the operational functionality of Spare Platform and/or an error that causes Spare Platform to be severely impacted as to be unusable and/or use of Spare Platform core functionalities are impossible with no workaround available.

P2 High Severity: System errors that highly impact Spare Platform core functionalities as to make them significantly degraded in a widespread manner where a short-term workaround may be available.

Appendix C - Standard Master Agreement

Spare Master "Software as a Service" Agreement

Last Modified: May 2, 2023

THIS SPARE MASTER "SOFTWARE AS A SERVICE" AGREEMENT ("Agreement") is made and entered into between SPARE LABS INC ("Spare") with a place of business at Suite 810, 815 W Hastings St, Vancouver, BC V6C 1B4, Canada, and customer stated in the applicable Order Form ("Customer") (individually a "Party"; collectively, the "Parties").

By agreeing to an Order Form referencing this Agreement or by accessing or using the Services offered by Spare, the Customer is confirming that the Customer has read, understood and accepted this Agreement. This Agreement can be updated from time to time in accordance with Section 2.5 below. Customer is responsible for regularly reviewing the most current version of this Agreement, which is published at: sparelabs.com/msa. When the Spare changes this Agreement, Spare will update the "Last Modified" date above.

RECITALS

1. WHEREAS, Spare is in the business of providing software as a service with respect to certain business application software and related services; and
2. WHEREAS, Customer desires to utilize such applications on a "software as a service" basis, and both Parties desire that Spare provide the services required and desire that all of the rights, duties, and obligations of the Parties be governed in accordance with the terms of this Agreement.

NOW, THEREFORE, based on the foregoing facts and in consideration of the mutual covenants and conditions contained in this Agreement, Spare and Customer hereby agree as follows:

1. DEFINITIONS

Defined terms used in this Agreement shall have the meanings given in this Agreement, including in any applicable Order Form.

"Fees" means the fees specified in the applicable Order Form, including without limitation any Subscription Fees;

“Open Fleet Provider” means a third party transportation network company (“TNC”) such as Lyft whose TNC services can be accessed through the Spare Services on express approval by Customer;

“Open Fleet Service” means Spare’s “Open Fleet” service where the services provided by Open Fleet Providers can be accessed through the Spare Platform, as described in greater detail at sparelabs.com;

“Order Form” means a written document executed by the parties that specifies the Service, subscription period, Fees and any other additional commercial terms agreed by the parties;

“Services” means the subscription(s) pursuant to one or more Order Form(s) to the Spare’s transportation software as a service offering described in greater detail at sparelabs.com;

“Subscription Fees” means the fees payable for subscription to the Services as specified in the applicable Order Form but excluding any trip or usage fees such as those payable to or in respect of Open Fleet Providers through the Services.

“Term” has the meaning given to in section 6.1.

2. SAAS SERVICES AND SUPPORT

2.1 Spare shall provide the Services and such other functions and responsibilities specified in this Agreement and any applicable Order Form, as they may be supplemented, enhanced, modified or replaced, and all updates thereto, during the Term pursuant to the terms of this Agreement.

2.2 Order Forms are binding on the parties only when executed by each party. Customer’s right to use the Services during the Term shall be in accordance with any additional conditions, restrictions or parameters specified in the Order Form(s) executed by the Parties. Services specified under an Order Form shall be provided during the term of that Order Form.

2.3 Subject to the terms of this Agreement, Spare will use commercially reasonable efforts to provide Customer the Services in accordance with the Service Level Terms attached hereto as Exhibit A. As part of the registration process, Customer will identify an administrative user name and password for the Spare account. Spare reserves the right to refuse registration of, or cancel passwords it deems inappropriate.

2.4 Subject to the terms hereof, Spare will provide Customer with reasonable technical support in accordance with the terms set forth in Exhibit B.

2.5 Amendment. Spare may change any part of this Agreement (including any terms or documents incorporated by reference in this Agreement) at any time by posting the revised terms on sparelabs.com/msa. It is important for Customer to review this Agreement before using Services and from time to time, though the Spare will notify the Customer of any changes that, in Spare's sole discretion, materially impact this Agreement. The updated Agreement will be effective as of the time of posting, or on such later date as may be specified in the updated Agreement, and Customer's continued use of the Services after any such changes are effective will constitute Customer's consent to such changes.

2.7 Open Fleet. In the event that Customer opts to subscribe for or otherwise use the Open Fleet (as indicated in the applicable Order Form or as expressly elected by Customer through the Service), Customer agrees to be bound by the Spare Open Fleet Terms attached at Exhibit C.

3. RESTRICTIONS AND RESPONSIBILITIES

3.1 Customer will not, directly or indirectly: reverse engineer, decompile, disassemble or otherwise attempt to discover the source code, object code or underlying structure, ideas, know-how or algorithms relevant to the Services or any software, documentation or data related to the Services ("Software"); modify, translate, or create derivative works based on the Services or any Software (except to the extent expressly permitted by Spare or authorized within the Services); use the Services or any Software for timesharing or service bureau purposes or otherwise for the benefit of a third-party; or remove any proprietary notices or labels. With respect to any Software that is distributed or provided to Customer for use on Customer premises or devices, Spare hereby grants Customer a non-exclusive, non-transferable, non-sublicensable license to use such Software during the Term only in connection with the Services.

3.2 Customer represents, covenants, and warrants that Customer will use the Services only in compliance with all applicable laws and regulations. Customer hereby agrees to indemnify and hold harmless Spare against any damages, losses, liabilities, settlements and expenses (including without limitation costs and attorneys' fees) in connection with any claim or action that arises from an alleged violation of the foregoing or otherwise from Customer's use of Services. Although Spare has no obligation to monitor Customer's use of the Services, Spare may do so and may prohibit any use of the Services it believes may be (or alleged to be) in violation of the foregoing.

3.3 Customer Responsibilities. The successful operation of the Service is dependent on Customer use of proper procedures and systems and input of correct data. Customer agrees that it shall have the sole responsibility for inputting, protecting and backing up their original data used in connection with the Service. The Customer is responsible for providing Spare with the necessary information to appropriately

integrate with the system and deliver all portions of the contract. Customer is solely responsible for the accuracy and adequacy of the information and data that it furnishes to Spare for use with the Service, and Spare is not responsible for reductions in Service quality due to Customer action or inaction.

3.4 Customer shall be responsible for obtaining and maintaining any equipment and ancillary services needed to connect to, access or otherwise use the Services, including, without limitation, modems, hardware, servers, software, operating systems, networking, web servers and the like (collectively, "Equipment"). Customer shall also be responsible for maintaining the security of the Equipment, Customer account, passwords (including but not limited to administrative and user passwords) and files, and for all uses of Customer account or the Equipment with or without Customer's knowledge or consent.

3.5 Customer shall comply with all applicable local, state, provincial, federal and foreign laws in using the Service.

3.6 Customer is solely responsible for (i) providing terms of service and privacy policy in respect of use of the Service by Customer's end users (which shall be an agreement solely between Customer and such end user); and (ii) obtaining the requisite permission, consent or other lawful basis from or in respect of end users for the use, storage and processing of their personal information by Spare through the provision of the Services, as required by applicable law.

4. CONFIDENTIALITY; PROPRIETARY RIGHTS

4.1 Each party (the "Receiving Party") understands that the other party (the "Disclosing Party") has disclosed or may disclose business, technical or financial information relating to the Disclosing Party's business (hereinafter referred to as "Proprietary Information" of the Disclosing Party). Proprietary Information of Spare includes non-public information regarding features, functionality and performance of the Service. Proprietary Information of Customer includes non-public data provided by Customer to Spare to enable the provision of the Services ("Customer Data"). The Receiving Party agrees: (i) to take reasonable precautions to protect such Proprietary Information, and (ii) not to use (except in performance of the Services or as otherwise permitted herein) or divulge to any third person any such Proprietary Information. The Disclosing Party agrees that the foregoing shall not apply with respect to any information after five (5) years following the disclosure thereof or any information that the Receiving Party can document (a) is or becomes generally available to the public, or (b) was in its possession or known by it prior to receipt from the Disclosing Party, or (c) was rightfully disclosed to it without restriction by a third party, or (d) was independently developed without use of any Proprietary Information of the Disclosing Party or (e) is required to be disclosed by law.

4.2 As between Spare and Customer, Customer shall own all right, title and interest in and to the Customer Data. Customer Data shall include all data entered by end users through the Service at Customer's request, but shall hold a non-exclusive right to all "registration" information of such end users such as user name, account name, telephone number and email address and ("Registration Information"). Spare reserves, owns and retains all right, title and interest in and to (a) the Services and Software, all improvements, enhancements or modifications thereto, (b) any software, applications, inventions or other technology developed in connection with Implementation Services or support, and (c) all intellectual property rights related to any of the foregoing; and (d) its database of all Registration Information and user password information. No rights are granted to Customer hereunder other than as expressly set forth herein.

4.3 Notwithstanding anything to the contrary, Spare shall have the right collect and analyze data and other information relating to the provision, use and performance of various aspects of the Services and related systems and technologies including, without limitation, aggregated or anonymized information derived from Customer Data ("Learning Data"). Spare shall hold all right, title and interest to Learning Data and, without limiting such ownership, will be free (during and after the term hereof) to (i) use such information and data to improve and enhance the Services and for other development, diagnostic and corrective purposes in connection with the Services and other Spare offerings, and (ii) disclose such data solely in aggregate or other de-identified form in connection with its business (including without limitation for marketing and sales purposes). No rights or licenses are granted except as expressly set forth herein.

5. FEES

5.1 Customer will pay Spare the then applicable fees described in any applicable Order Form for the Services with the terms therein (the "Fees"). If Customer's use of the Services exceeds the Service Capacity set forth on the Order Form or otherwise requires the payment of additional fees (per the terms of this Agreement), Customer shall be billed for such usage and Customer agrees to pay the additional fees in the manner provided herein. Spare reserves the right to change the Fees or applicable charges and to institute new charges and Fees at the end of the Term or then-current renewal term, upon thirty (30) days prior notice to Customer (which may be sent by email). If Customer believes that Spare has billed Customer incorrectly, Customer must contact Spare no later than 60 days after the closing date on the first billing statement in which the error or problem appeared, in order to receive an adjustment or credit. Inquiries should be directed to Spare's customer support department. All Fees are non-refundable once paid.

5.2 Spare may choose to bill through an invoice, in which case, full payment for invoices issued in any given month must be received by Spare thirty (30) days after the mailing date of the invoice. Unpaid amounts are subject to a finance charge of 1.5% per month on any outstanding balance, or the maximum

permitted by law, whichever is lower, plus all expenses of collection and may result in immediate termination of Service.

5.3 Taxes. Unless otherwise stated, Spare's fees do not include any direct or indirect local, state, provincial, federal or foreign taxes, levies, duties or similar governmental assessments of any nature, including value-added, goods and services, harmonized, use or withholding taxes (collectively, "Taxes"). Customer is responsible for paying all Taxes associated with its purchases hereunder, excluding taxes based on Spare's net income or property. If Spare has the legal obligation to pay or collect Taxes for which Customer is responsible under this section, the appropriate amount shall be invoiced to and paid by Customer, unless Customer provides Spare with a valid tax exemption certificate authorized by the appropriate taxing authority.

5.4 Spare will be billed according to payment schedules set out in any applicable Order Form.

5.5 CPI Increase. The Fees shall be increased on each anniversary of the first day of the Term (the "CPI Adjustment Date") by an amount equal to the greater of a) 5% or b) the increase, if any, in the CPI (as defined below) in effect for December of the immediately preceding calendar year (the "Most Recent Calendar Year") over the CPI in effect for December of the calendar year immediately preceding the Most Recent Calendar Year. The term "CPI" shall mean the Consumer Price Index for All Urban Consumers (CPI-U) for the U.S. City Average for All Items (1984=100) published by the United States Department of Labor, Bureau of Labor Statistics.

6. TERM AND TERMINATION

6.1 Subject to earlier termination as provided below, this Agreement will commence on the date you agree to an Order Form, and will continue in effect for the term described in such Order Form (the "Term"). Except as expressly stated otherwise in the applicable Order Form, each Order Form will automatically renew for subsequent one-year renewal periods unless the Customer or Spare gives written notice of non-renewal at least sixty (60) days prior to the end of the then-current term. Notwithstanding the foregoing, in no event shall the term of this Agreement or any Order Form exceed the term agreed to in writing between Spare and Customer.

6.2 In addition to any other remedies it may have, either party may also terminate this Agreement upon thirty (30) days' notice (or without notice in the case of nonpayment), if the other party materially breaches any of the terms or conditions of this Agreement. Customer will pay in full for the Services up to and including the last day on which the Services are provided. All sections of this Agreement which by their nature should survive termination will survive termination, including, without limitation, accrued rights to payment, confidentiality obligations, warranty disclaimers, and limitations of liability.

7. WARRANTY AND DISCLAIMER

7.1 Spare shall use reasonable efforts consistent with prevailing industry standards to maintain the Services in a manner which minimizes errors and interruptions in the Services and shall perform the Implementation Services in a professional and workmanlike manner. Services may be temporarily unavailable for scheduled maintenance or for unscheduled emergency maintenance, either by Spare or by third-party providers, or because of other causes beyond Spare's reasonable control, but Spare shall use reasonable efforts to provide advance notice in writing or by e-mail of any scheduled service disruption. HOWEVER, SPARE DOES NOT WARRANT THAT THE SERVICES WILL BE UNINTERRUPTED OR ERROR FREE; NOR DOES IT MAKE ANY WARRANTY AS TO THE RESULTS THAT MAY BE OBTAINED FROM USE OF THE SERVICES. EXCEPT AS EXPRESSLY SET FORTH IN THIS SECTION, THE SERVICES AND IMPLEMENTATION SERVICES ARE PROVIDED "AS IS" AND SPARE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT.

8. INDEMNITY

8.1 Spare shall hold Customer harmless from liability to third parties resulting from infringement by the Service of any United States patent or any copyright or misappropriation of any trade secret, provided Spare is promptly notified of any and all threats, claims and proceedings related thereto and given reasonable assistance and the opportunity to assume sole control over defense and settlement; Spare will not be responsible for any settlement it does not approve in writing. The foregoing obligations do not apply with respect to portions or components of the Service (i) not supplied by Spare, (ii) made in whole or in part in accordance with Customer specifications, (iii) that are modified after delivery by Spare, (iv) combined with other products, processes or materials where the alleged infringement relates to such combination, (v) where Customer continues allegedly infringing activity after being notified thereof or after being informed of modifications that would have avoided the alleged infringement, or (vi) where Customer's use of the Service is not strictly in accordance with this Agreement. If, due to a claim of infringement, the Services are held by a court of competent jurisdiction to be or are believed by Spare to be infringing, Spare may, at its option and expense (a) replace or modify the Service to be non-infringing provided that such modification or replacement contains substantially similar features and functionality, (b) obtain for Customer a license to continue using the Service, or (c) if neither of the foregoing is commercially practicable, terminate this Agreement and Customer's rights hereunder and provide Customer a refund of any prepaid, unused fees for the Service.

9. LIMITATION OF LIABILITY

9.1 NOTWITHSTANDING ANYTHING TO THE CONTRARY, EXCEPT FOR BODILY INJURY OF A PERSON, SPARE AND ITS SUPPLIERS (INCLUDING BUT NOT LIMITED TO ALL EQUIPMENT AND TECHNOLOGY SUPPLIERS), OFFICERS, AFFILIATES, REPRESENTATIVES, CONTRACTORS AND EMPLOYEES SHALL NOT

BE RESPONSIBLE OR LIABLE WITH RESPECT TO ANY SUBJECT MATTER OF THIS AGREEMENT OR TERMS AND CONDITIONS RELATED THERETO UNDER ANY CONTRACT, NEGLIGENCE, STRICT LIABILITY OR OTHER THEORY: (A) FOR ERROR OR INTERRUPTION OF USE OR FOR LOSS OR INACCURACY OR CORRUPTION OF DATA OR COST OF PROCUREMENT OF SUBSTITUTE GOODS, SERVICES OR TECHNOLOGY OR LOSS OF BUSINESS; (B) FOR ANY INDIRECT, EXEMPLARY, INCIDENTAL, SPECIAL OR CONSEQUENTIAL DAMAGES; (C) FOR ANY MATTER BEYOND SPARE'S REASONABLE CONTROL; OR (D) FOR ANY AMOUNTS THAT, TOGETHER WITH AMOUNTS ASSOCIATED WITH ALL OTHER CLAIMS, EXCEED THE SUBSCRIPTION FEES PAID BY CUSTOMER TO SPARE FOR THE SERVICES UNDER THIS AGREEMENT IN THE 12 MONTHS PRIOR TO THE ACT THAT GAVE RISE TO THE LIABILITY, IN EACH CASE, WHETHER OR NOT SPARE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

10. MISCELLANEOUS

10.1 If any provision of this Agreement is found to be unenforceable or invalid, that provision will be limited or eliminated to the minimum extent necessary so that this Agreement will otherwise remain in full force and effect and enforceable. This Agreement is not assignable, transferable or sublicensable by Customer except with Spare's prior written consent. Spare may transfer and assign any of its rights and obligations under this Agreement without consent. Notwithstanding the foregoing, It is understood and agreed by Customer and Spare that, subject to Spare's agreement, where Customer is a governmental, municipal or other form of publicly-funded entity then any entity reasonably associated with Customer ("Associated Entity") may purchase the services specified herein in accordance with the terms and conditions of this agreement, with the exception of the pricing provided. It is also understood and agreed that each such Associated Entity will establish its own contract with Spare, be invoiced therefrom and make its own payments to Spare in accordance with the terms of the contract established between the Associated Entity and Spare . It is also hereby mutually understood and agreed that Customer is not a legally bound party to any contractual agreement made between Spare and any entity other than Customer. This Agreement is the complete and exclusive statement of the mutual understanding of the parties and supersedes and cancels all previous written and oral agreements, communications and other understandings relating to the subject matter of this Agreement, and that all waivers and modifications must be in a writing signed by both parties, except as otherwise provided herein. No agency, partnership, joint venture, or employment is created as a result of this Agreement and Customer does not have any authority of any kind to bind Spare in any respect whatsoever. In any action or proceeding to enforce rights under this Agreement, the prevailing party will be entitled to recover costs and attorneys' fees. All notices under this Agreement will be in writing and will be deemed to have been duly given when received, if personally delivered; when receipt is electronically confirmed, if transmitted by facsimile or e-mail; the day after it is sent, if sent for next day delivery by recognized overnight delivery service; and upon receipt, if sent by certified or registered mail, return receipt requested. This Agreement shall be governed by the laws of the Province of British Columbia, Canada without regard to its conflict of laws provisions.

Customer otherwise agrees to reasonably cooperate with Spare to serve as a reference account upon request.

10.2 This agreement is available to any other public agency (i.e., city, district, public authority, public agency, municipality and other political sub-division or public corporation). Customer shall incur no financial responsibility in connection with contracts executed with other parties under the authority of this provision or in making payments to the firms or contractor teams.

EXHIBIT A

Service Level Terms

General Service Level Terms and Downtime Management:

The Services shall be available 99.9%, measured monthly, excluding scheduled maintenance. If Customer requests maintenance during these hours, any uptime or downtime calculation will exclude periods affected by such maintenance. Further, any downtime resulting from outages of third party connections or utilities or other reasons beyond Spare's control will also be excluded from any such calculation. Customer's sole and exclusive remedy, and Spare's entire liability, in connection with Service availability shall be that for each period of downtime lasting longer than one hour, Spare will credit Customer 0.3% of annual Service fees for each period of 30 or more consecutive minutes of downtime; provided that no more than one such credit will accrue per day. Downtime shall begin to accrue as soon as Customer (with notice to Spare) recognizes that downtime is taking place, and continues until the availability of the Services is restored. In order to receive downtime credit, Customer must notify Spare in writing within 24 hours from the time of downtime, and failure to provide such notice will forfeit the right to receive downtime credit. Such credits may not be redeemed for cash and shall not be cumulative beyond a total of credits for one (1) week of Service Fees in any one (1) calendar month in any event. Spare will only apply a credit to the month in which the incident occurred. Spare's blocking of data communications or other Service in accordance with its policies shall not be deemed to be a failure of Spare to provide adequate service levels under this Agreement.

Incident Management:

If any service issue should arise throughout the duration of service, all issue shall be marked and prioritized as follows:

1. Fatal (Complete degradation -- 30 Minute response time during Support Hours (see Exhibit B)). All users and critical functions affected.
2. Severe (significant degradation -- 90 Minutes response time during Support Hours (see Exhibit B)). Large percentage of users or critical functions affected.

3. Medium (limited degradation -- 3 hour response time during Support Hours (see Exhibit B)). Limited number of users or non-critical functions affected. Business processes can continue.
4. Minor (small degradation -- 4 hour response time during Support Hours (see Exhibit B)). One user affected. Business processes can continue.

EXHIBIT B

Support Terms

Spare will provide support to Customer via electronic mail, chat, and over phone on a twenty-four (24) hour, seven (7) days a week basis ("Support Hours").

Customer may initiate a helpdesk ticket during Support Hours by emailing support@sparelabs.com.

Spare will use commercially reasonable efforts to respond to all helpdesk tickets within one business day.

EXHIBIT C

Open Fleets Terms

See following page for Open Fleets terms.

Additional terms specific to provision of Open Fleet Provider integration through Spare Open Fleets:
In providing and using Open Fleet Providers through Spare Open Fleets, the following additional provisions shall apply:

- (a) Spare obligations: Spare shall only enable an Open Fleet Provider integration with Customer's account within the Spare Platform where such integration has been expressly approved in writing by Customer ("Approved Open Fleet Provider").
- (b) Customer Obligations.
 - (i) Unless otherwise agreed in writing between the Parties, Customer represents and warrants that it (i) either has a direct agreement in place with each Approved Open Fleet Provider that permits that the Open Fleet Provider integration with Customer's account within the Spare Platform and use as part of the Services that does not require any further agreement be entered into by Spare; or (ii) that it has agreed to be bound by the applicable Approved Fleet Providers Terms as set out in sub-section (c) below.
 - (ii) Customer covenants and agrees to immediately inform Spare in the event that any such agreement with an Approved Open Fleet Provider lapses, in which event Spare shall immediately terminate the integration within the Customer's account within the Spare Platform in respect of such Open Fleet Provider.
 - (iii) For each Approved Open Fleet Provider whose integration Customer has approved in writing, Customer shall include such notification and/or require any user of the Service to accept or acknowledge such additional terms of use, privacy policy or similar, in each case as may be required by such Open Fleet Provider and applicable law.

(c) Approved Open Fleet Provider Terms

Where subsection (b)(i) above does not apply and the Approved Open Fleet Provider is:

- (i) Uber Inc. ("Uber", which expression shall include any subsidiaries or affiliates of Uber Inc.), then Customer agrees to be bound by the standard Uber for Business terms and conditions (the "U4B Online Terms"), available via <https://www.uber.com/legal/business/dashboard/en/> (as may be updated from time to time), in the US, or the applicable global equivalent;
- (ii) Lyft ("Lyft", which expression shall include any subsidiaries or affiliates of Lyft Inc.), then Customer agrees to be bound by the Lyft-specific terms set out in appendix []; or
- (iii) Any other Approved Open Fleet Provider, such Approved Open Fleet Provider-specific terms as may be notified to Customer at the time of express approval of such Open Fleet Provider by Customer.

Appendix D - Other Supporting Materials

Identity and Access Management (IAM)

The following is a description of Spare's IAM protocols and how we make them available for application integration/consumption:

Spare uses WorkOS integrate with an external identity provider using SAML. This allows agencies to utilize and manage their own authentication protocols and have control over password policy etc.

1. Configure your Identity Provider (IdP):

Set up your preferred Identity Provider (e.g., Okta, OneLogin, Azure AD, ADFS) and configure it to work with SAML.

- Obtain the necessary metadata from your IdP, such as the Entity ID and SSO (Single Sign-On) URL.

2. Set up your Service Provider (SP) with workOS:

- Sign up for a workOS account and create a new project.
- Install the workOS SDK in your application's backend.

3. Configure workOS settings:

- In your workOS project, navigate to the "Authentication" section and select "SAML."
- Provide the metadata from your IdP to workOS.
- Configure other settings, such as the SAML Audience (SP Entity ID) and SAML ACS (Assertion Consumer Service) URL.

4. Implement the SAML flow in your application:

- When a user tries to access a protected resource, redirect them to the workOS /sso/saml endpoint with the appropriate parameters, such as the desired redirect URL after authentication.
- workOS will initiate the SAML flow and redirect the user to your IdP's SSO URL.
- The IdP will authenticate the user and generate a SAML response containing the user's identity information.
- The IdP will redirect the user back to the SAML ACS URL provided by workOS.

- workOS will validate the SAML response and generate a JWT (JSON Web Token) containing the user's identity.
- Retrieve the JWT in your application backend and validate it.
- If the JWT is valid, log the user in and grant access to the requested resource.

5. Handle user logout:

- When a user logs out of your application, redirect them to the workOS /sso/saml/logout endpoint.
- workOS will initiate the SAML logout flow and redirect the user to the IdP's logout URL.
- The IdP will handle the logout process and redirect the user back to your application's specified logout URL.

6. Optional: Customize the authentication experience:

- workOS provides options to customize the SAML login page, such as adding your application's logo and custom CSS styles.

Commingling for A More Efficient Service

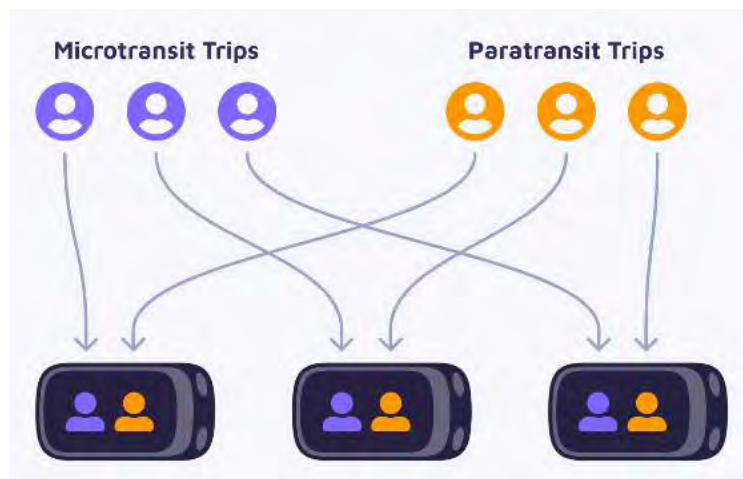
Depending on the individual DROs, Spare proposes leveraging our advanced, shared-ride commingling feature to generate added value and resources to re-invest into the DROs' existing transit system.

Commingling, in the most general sense, is the ability to combine different types of transit services (on-demand, paratransit, NEMT, etc.) into a single cohesive one. Commingling includes the ability to combine different passenger types into a single vehicle and the ability to use the same vehicle for different types of services. It can

enable significant **cost savings for agencies by maximizing resources and service availability**.

Commingling can also help promote social inclusion by virtue of breaking down former silos and creating a mosaic of riders, enabling riders of different backgrounds to share similar rides.

Many agencies are now combining on-demand and paratransit rides. Across our partner network, transit agencies leverage Spare's commingling and pooling algorithm to **drive operational efficiencies and increase vehicle productivity**.



Many agencies opt to take a phased approach to commingling, opting to start with separated services and transitioning to a more commingled approach when passenger demand or operational conditions justify it. Thanks to the flexibility of Spare Platform and with the support of our Partner Success team, **the DROs can choose what works best** for their community and deploy commingling at any time.

Spare has extensive experience in powering commingled transit services and non-commingled paratransit and on-demand operations, as well as services that started separately and later became commingled services.

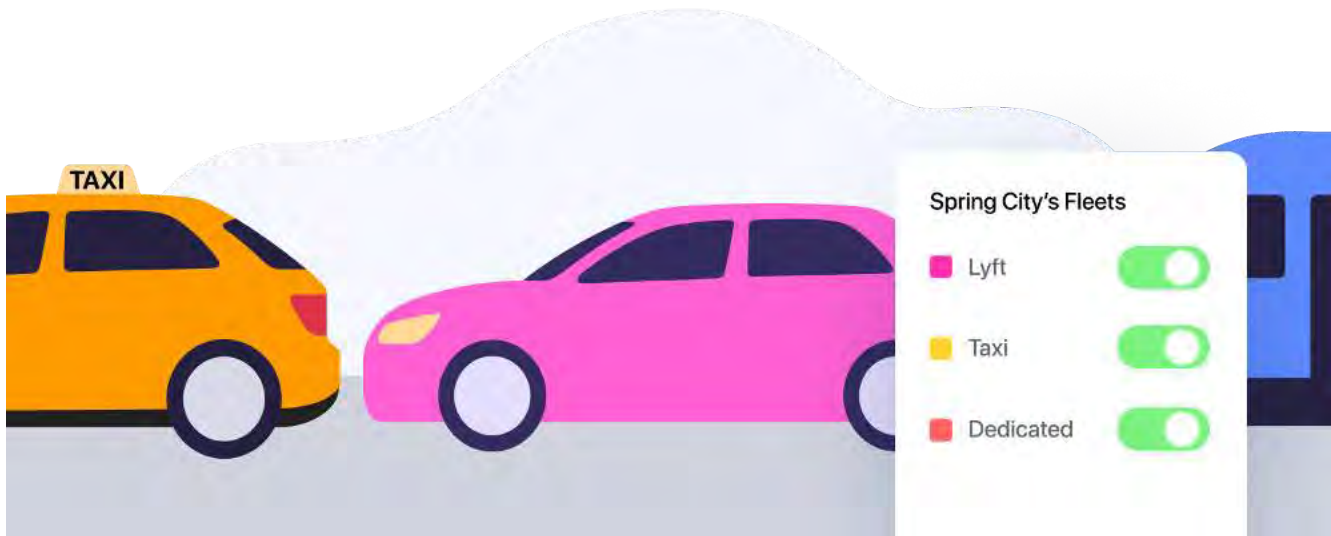
Spare's algorithm takes into account parameters such as empty vehicle seats, locations, timing of schedules, and wait times to decide when to commingle trips. The algorithm uses an advanced proprietary algorithm to analyze thousands of possible matches for every trip request and creates the most efficient manifest possible for every single duty. It does so by keeping in mind the constraints determined by the various services that are running in parallel. For example, it knows not to move a paratransit ride beyond the flexibility parameters and only accept new on-demand same day requests if they can be executed without delaying paratransit rides. To make the process even more responsive, the algorithm works even after trips have been matched to make adjustments on the fly as the day progresses and unforeseen events occur, such as breakdown and delays.

Where it works. Spare launched a commingled service with Citibus in Lubbock, Texas. Layering two zones together in Spare Platform, the Citibus Access (ADA paratransit) service and Citibus On-Demand (general microtransit) service co-exists to serve the residents of Lubbock. Through fleet sharing, Spare provided operational savings of up to 30% in Lubbock by avoiding the need to operate a larger, overall fleet.

Including Non-Dedicated Service Providers for An Elastic Vehicle Supply

Powered by our API, Spare's trip brokering module called **Spare Open Fleets** is, to our knowledge, the only technology in the industry that natively integrates dedicated public transit fleets with local taxis, TNCs, and other local transport providers in a single cloud-based software platform with full reporting and live vehicle capabilities. This makes Spare uniquely positioned to deliver on a future state of the DROs' transit program, if a mixed fleet supply is desired for the transit system.

Spare built Open Fleets to leverage non-dedicated service providers (NDSPs) to augment vehicle supply and fulfill an unmet need in trip delivery. We also built this innovative module to reduce manual, cumbersome, and technologically outdated workflows. For example, there was no effective software solution to automate the reservations, scheduling, and dispatching process from an agency to NDSPs, nor an effective way to track, manage, and bill NDSPs. There was also no automated way to intelligently select the most cost effective fleet that meets the requirements of an individual trip.



Spare Open Fleets enables transit agencies to seamlessly mix NDSPs onto their vehicle fleet and have all of the same abilities and privileges as their dedicated multi-fleet operators within one centralized software platform, all while ensuring trip minimums and other contractual requirements. **By doing this, agencies increase cost savings, improve on-time performance (OTP), and reduce wait times for riders.** All of this comes together to improve overall service quality for both the agency and its riders. Our Open Fleets module allows a seamless integration of transit service which will also allow multimodal connectivity with active transportation, taxis, and transportation network companies, and car-share services.

To-date, **80% of all bookable vehicles in North America are available on Spare through Open Fleets.** We would be happy to discuss the details of this powerful innovation further, including non-dedicated trip visibility, streamlining the rider opt-in process, and optimizing trip distribution between dedicated and non-dedicated providers.

Spare has several agency partners in North America that incorporate NDSPs into their Spare-powered transit offering. Below we highlight some of them with key operational statistics, demonstrating the value that Spare can bring:

Collin County Transit Mobility on Demand, Texas

Collin County Transit received immediate benefits of Open Fleets with their cost per trip decreasing by 47% from going from only using dedicated service providers (DSPs) to using a combination of DSPs and NDSPs powered by Spare Open Fleets. Today, in partnership with Dallas Area Rapid Transit and three operators (Irving Holdings, Echo [dedicated], and Lyft [non-dedicated]), and a third party call center (Telelink), Spare provides and manages an end-to-end, modern turnkey transportation service for those with disabilities and low incomes in Collin County.

Ridership for the service has grown from under 150 boardings per week at launch to over 800 boarding per week today. The share of trips going to dedicated providers has decreased from 100% at launch (without Lyft) to 30% today (with the remaining 70% going to Lyft). With the introduction of Lyft and the optimization of the service, Spare has reduced the average cost per trip from over \$72 at launch to less than \$38 today. This is an example of the power of Open Fleets leveraged in a community where mixed fleet supply is highly effective. Spare uses a bespoke approach with each partner to understand where and when a mixed fleet transportation model makes the most sense to apply.

PSTA Access Paratransit, Florida

In Pinellas County, Florida Spare, Uzurv, and Lyft offer a mixed fleet supply for PSTA's demand response paratransit program, where more than 40% of its nearly 1-million residents are reported to have a disability. Launched in December 2021, Open Fleets has brokered **more than 20% of trips** to NDSPs and with each month that passes the rate increases as riders switch from traditional paratransit to the mobility on demand service that includes NDSPs. In 2022, PSTA saw an increase of more than 25%.

Platform integration features include:

1. **Integrated Dispatch:** Assigned trips are auto-dispatched to the Uzurv technology platform by Spare. For accepted trips, Uzurv driver and vehicle info is visible in Spare, including the driver's name, the vehicle color, make, model, year, plate state, and tag number.
2. **Real-Time Ride Status:** Real-time vehicle tracking is available in Spare with GPS and timestamp on each status change, including driver en route, pick-up arrived, in progress, drop-off arrived, and completed trip.
3. **Transparent Reporting:** All Uzurv ride execution data is seamlessly available via Spare reporting.

Optional Call Centre: Telelink

Spare's award-winning call center partner Telelink is available to take overflow calls throughout the day when the queue gets too long. Telelink utilizes a shared customer service representative model. This allows for maximum flexibility for DROs' call centers for their services, as these services **are only used when needed and charged by the minute**.

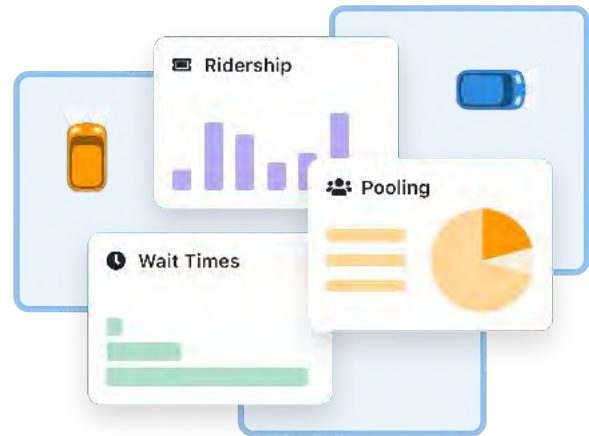
There is full access call center reporting, recorded phone calls, and digital scripting system. Call recordings are stored within the third party software for 12 months. Our partners have found that having an overflow call center is valuable in managing ridership growth in not overwhelming dispatch with additional calls.

Cheyenne Transit Program (CTP) replaced Paraplan's paratransit software with Spare has seen a 50% reduction in time spent on calls when reserving trips due primarily to the intuitive nature of the system for the reservationists.



Planning and Service Design Support with Spare Realize

Spare offers not only full training to the DROs staff, but also testing environments to simulate rides, announcements, new features, and more. One tool that may be particularly useful for these simulations and what-if scenarios in the sandbox environments is Spare's transit duty planning tool that helps users visualize where they are over- or under-providing vehicle supply across different parts of a day. By changing vehicle shifts and capacities accordingly, the DROs' planning team can easily understand the implications of their decision-making on overall run structure.



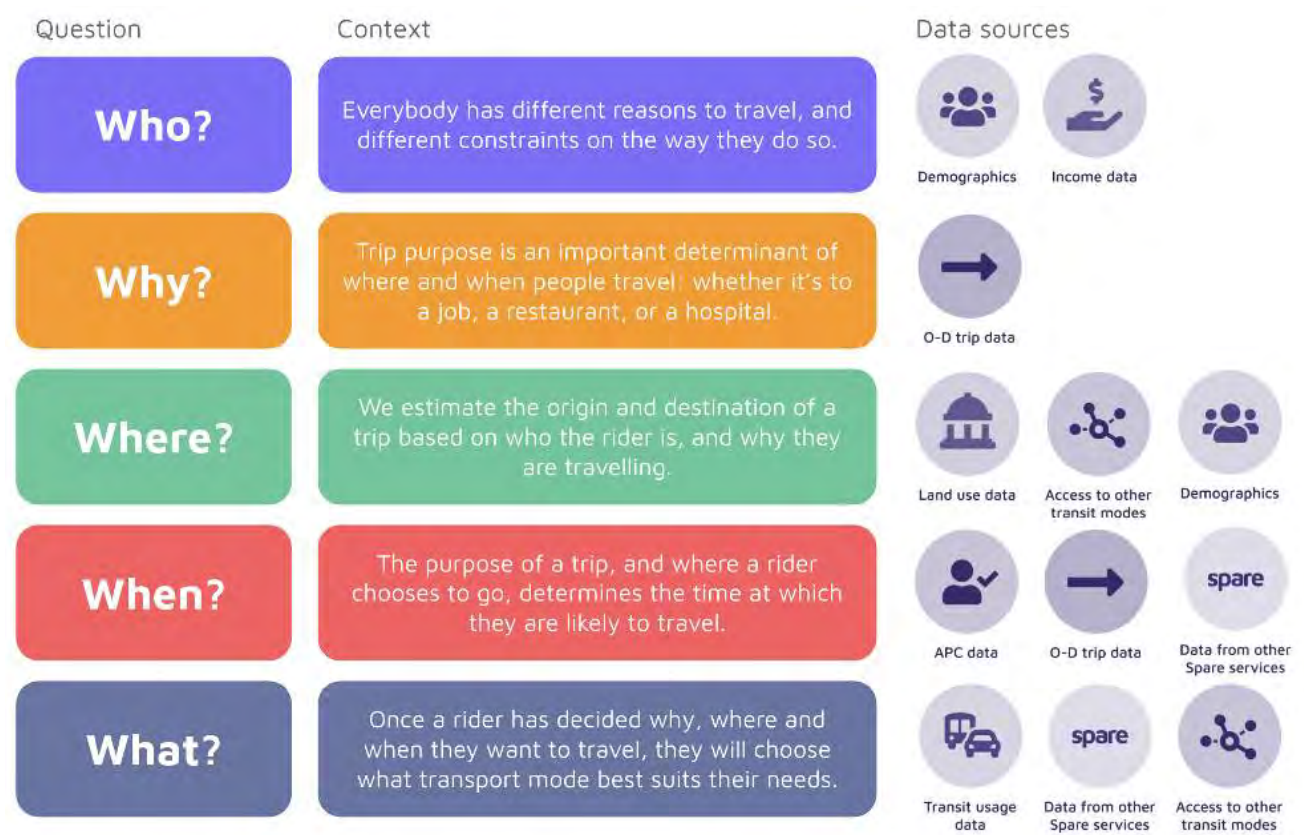
Spare Realize is a transportation network simulation tool that can be used to run quick and informative transit simulations during the planning and operational stages of a transportation service. It is a fundamentally new way of planning and optimizing transportation networks that provides users with **detailed data-driven simulations**.

Spare Realize functions using a demand model that uses back-end statistical and machine learning models, which in turn output demand estimates. The framework analyzes where an on-request system should operate, whom it is likely to serve and therefore impact, during which times it should operate, and its potential costs and returns. Spare approaches simulations through these steps:

1. Estimate trip volume using existing ridership data for lines of interest
2. Estimate trip distribution
3. Determine trip types (e.g. commuter, recreational, medical)
4. Distribute trips spatially (i.e. trip origin and destination)
5. Distribute trips temporally (i.e. trip start time and end time)
6. Realize predicts likely origin-destination pairs and routes them through its routing algorithm to run iterative simulations
7. Aggregate simulation results and present them to the user

Whenever we use Spare Realize to plan for a new service deployment, we are careful to work through the '5 Ws' that we feel should be addressed to maximize its success. Each of these Ws (*figure to the right*) is associated with some key data sources that we rely on to visualize and understand the local transportation context, as well as to drive our demand and supply models. The data sources range from publicly available socio-economic datasets, such as census and jobs data, to travel surveys and academic literature, all the way through to 'on-request potential' and 'paratransit potential' data layers, which leverage machine learning techniques to identify potential hotspots of demand from Spare's own operational data in other parts of the world.

Spare’s Data Science and Consulting team have completed **15 transit simulation studies** for customers such as TransLink in Metro Vancouver, McKinney in Texas, SMART in Detroit, RTC in Quebec City, Evansville/Toyota Mobility Foundation in Evansville, IN, and more to offer powerful and informative insights of the potential performance of an on-request service.



Appendix E - Remaining Attachments

roles

Transit Software Solution

54-12008772-CM

June 16, 2023

SECURITY EVALUATION FORM (SEF)

Version 1.6

Prepared for

North Carolina Department of Information Technology - Transportation



Executive Summary

The State of North Carolina Statewide Information Security Manual (SISM) was established by the State CIO under authority N.C.G.S § 143B-1375, 143B-1376, and 143B-1378 to identify and implement information technology security controls. The policies, guidelines, and standards established by the SISM apply to all [Information Environments](#) that store, process, transmit, and/or can impact the security of NCDOT/DMV data.

STATUTORY LAW

https://www.ncleg.gov/EnactedLegislation/Statutes/PDF/BySection/Chapter_143B/GS_143B-1375.pdf

f

https://www.ncleg.gov/EnactedLegislation/Statutes/PDF/BySection/Chapter_143B/GS_143B-1376.pdf

f

https://www.ncleg.gov/EnactedLegislation/Statutes/PDF/BySection/Chapter_143B/GS_143B-1378.pdf

f

POLICIES, GUIDELINES AND STANDARDS

<https://it.nc.gov/resources/cybersecurity-and-risk-management/esrmo-initiatives/statewide-information-security/>

<https://it.nc.gov/documents/statewide-data-classification-and-handling-policy>

<https://archives.ncdcr.gov/government/state-government-agencies/functional-schedule>

GLOSSARY OF INFORMATION TECHNOLOGY TERMS

<https://it.nc.gov/documents/statewide-glossary-information-technology-terms>

<https://csrc.nist.gov/glossary>

PURPOSE

The Security Evaluation Form (SEF) and its underlying assessment activities serve to provide NCDOT with an understanding of the third-party contractor's [security capabilities](#) relevant to the third-party contractor's access to NCDOT's [information resources](#). The SEF is unlike a full [security assessment](#) in that the SEF typically does not require third-parties to submit technical evidence (e.g., screenshots, logs, packet captures, security scans, configuration exports, test results, etc.) to validate their stated security capabilities. This is important to understand because the third-party's overall security capabilities are typically conceptual from NCDOT's perspective and cannot be fully assessed and verified in a manner consistent with the Statewide Information Security Manual (SISM). For this reason, the outcome of this security evaluation is largely dependent on the third-party contractor's ability to understand the security requirements established by NCDOT and provide meaningful and comprehensive responses to the questions in the SEF and throughout the assessment process.

SECURITY CONTROLS AND CAPABILITIES

The third-party contractor's responses throughout the security evaluation are used to assess the third-party contractor's overall security capabilities. Security capabilities are defined and evaluated by bringing together specific sets of security controls derived from the appropriately tailored baselines that together produce the required capabilities. The SISM establishes the security controls and capabilities that must be satisfied before [information systems](#) are permitted access to NCDOT's data.

APPROACH AND USE OF THIS DOCUMENT

The security evaluation begins when the third-party contractor returns their completed SEF and supporting documentation to NCDOT for review. In addition to the third-party contractor's responses to the security questions, they may be asked to provide copies of their applicable security program documents including policies, standards, procedures, plans, dataflows, network architecture diagrams, third-party risk assessment reports, etc.

OUTCOMES

Submission of this report by the third-party does not guarantee a state-ready designation, nor does it guarantee that the North Carolina Department of Transportation (NCDOT) will procure services from the third-party.

Third-Party's System Information

Third-Party Name:
System/Service Name:
Service Model: (e.g. IaaS, PaaS, SaaS)
FIPS PUB 199 System Security Level: (Moderate)
Fully Operational as of: Enter the date the system became fully operational.
Number of Customers (State/Others): Enter # of customers / # of other customers
Deployment Model: Is the service a Public Cloud, Government-Only Cloud, Federal Government-Only Cloud, or Other? If other, please describe.
System Functionality: Briefly describe the functionality of the system and service being provided.

Information Security Questionnaire

1. The [Statewide Information Security Manual \(SISM\)](#) was established by the State CIO under authority N.C.G.S. § 143B-1375, 143B-1376, and 143B-1378. The policies and standards defined in the SISM apply to all systems and services that store, process, transmit, and/or could impact the security of NCDOT Data. It is important to understand a SOC 2 Type II (or equivalent) only indicates the third-party contractor's policies, standards, and procedures were assessed as being compliant with generic industry accepted practices. A SOC 2 Type II (or equivalent) does not certify the third-party contractor's services as being compliant with the NCDOT's information security policies, guidelines, and standards (e.g., account lockout thresholds, employment background checks (local/State/Federal), minimum password requirements, data classification, change management, etc.).

2. The term **Personally Identifiable Information (PII)** refers to information that can be used to distinguish or trace an individual's identity, alone or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as name, date and place of birth, employer, home and work addresses, email address, phone number, mother's maiden name, etc.

The third-party contractor's services will process **Restricted** and/or **Highly Restricted** NCDOT data that could be used to distinguish or trace an individual's identity.

3. Describe the third-party contractor's methodology for acknowledging and maintaining compliance with NCDOT's information security policies, guidelines, and standards.
- i. Is the third-party contractor's methodology documented in a policy document?
 - ii. Does the methodology extend to all third parties supporting the third-party contractor's services? Please explain in detail.

To acknowledge and maintain compliance with NCDOT's Statewide Information Security Manual (SISM), Spare follow the following methodology:

1. Manual Familiarization: Start by thoroughly reading and understanding NCDOT's Statewide Information Security Manual (SISM). Familiarize yourself with the policies, guidelines, and standards outlined in the manual. Pay close attention to the specific requirements, objectives, and best practices it provides.

2. Gap Analysis: Perform a comprehensive gap analysis to identify any gaps between our organization's current information security practices and the requirements specified in the SISM. This analysis will help Spare understand areas that need improvement or further attention to align with the manual's guidelines.

3. Compliance Assessment: Conduct regular assessments or audits to evaluate your organization's compliance with the SISM. Review your current practices, procedures, and controls against the requirements and benchmarks defined in the manual. Identify any deviations or non-compliance issues that need to be addressed.

4. Risk Assessment: Perform a risk assessment to identify potential threats and vulnerabilities in

your information systems, considering the context of the SISM. Assess the impact and likelihood of these risks, and prioritize them based on their potential impact on NCDOT's security objectives as defined in the manual.

5. Security Controls Implementation: Develop and implement appropriate security controls based on the identified gaps and risk assessment results. Ensure that these controls align with the requirements specified in the SISM. Implement technical, administrative, and physical measures to safeguard information and systems accordingly.

6. Training and Awareness: Provide training and awareness programs to educate employees about the SISM's policies, guidelines, and standards. Ensure that all staff members understand their roles and responsibilities in maintaining compliance and are aware of the potential risks associated with information security. Highlight the importance of adhering to the established controls outlined in the manual.

7. Incident Management: Establish an incident management process aligned with the SISM to handle security incidents and breaches effectively. Develop response procedures, escalation protocols, and reporting mechanisms that are in line with the manual's requirements. Ensure timely detection, containment, and resolution of security incidents, and report them as per the guidelines defined in the SISM.

8. Continuous Monitoring and Review: Regularly monitor and review your information security controls to ensure their ongoing effectiveness and compliance with the SISM. Conduct periodic internal audits, vulnerability assessments, and penetration tests to identify any new risks or areas of non-compliance. Monitor changes or updates to the SISM and adjust your practices accordingly.

9. Documentation and Reporting: Maintain comprehensive documentation of your organization's information security policies, procedures, controls, and compliance efforts as per the SISM's requirements. Keep records of security incidents, risk assessments, audits, and remediation actions taken. Generate reports to provide updates on compliance status to NCDOT and other relevant stakeholders in accordance

	with the manual's guidelines. 10. Periodic Review and Improvement: Conduct periodic reviews of your compliance program to identify areas for improvement and make necessary adjustments based on the SISM's guidelines. Stay updated with any changes or updates to the SISM and adapt your practices accordingly to ensure continued compliance. The methodology extends to all third party contractors and will be documented if Spare is contracted by NCDOT.
4. The System Security Plan (SSP) provides a summary of the security requirements of the information system(s) and describes the controls for meeting those requirements and defined responsibilities and expected behavior of all individuals who access the system. The SSP also contains or references other key security-related documents for the information system such as a risk assessment, Corrective Actions Plan (CAP), accreditation documentation, privacy threshold and impact assessment, contingency plan, configuration management plan, security configuration checklists and system interconnection agreements as appropriate. i. Provide a System Security Plan (SSP) that addresses all applicable aspects of the third-party contractor's proposed services and solution. Linked below is a copy of the State's SSP template. https://it.nc.gov/documents/system-security-plan-template	Spare System Security Plan Overview This Information Security Policy is intended to protect Spare's employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly. Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, web browsing, and file transfers, are the property of Spare. These systems are to be used for business purposes in serving the interests of the company, and of our clients and customers in the course of normal operations. Effective security is a team effort involving the participation and support of every Spare employee or contractor who deals with information and/or information systems. It is the responsibility of every team member to read and understand this policy, and to conduct their activities accordingly. Purpose The purpose of this policy is to communicate our information security policies and outline the acceptable use and protection of Spare's information and assets. These rules are in place to protect customers, employees, and Spare. Inappropriate use exposes Spare to risks including virus attacks, compromise of network systems and services, and legal and compliance issues. The Spare "Information Security Policy" comprises this policy and all Spare policies referenced and/or linked within this document.

	Scope This policy applies to the use of information, electronic and computing devices, and network resources to conduct Spare business or interact with internal networks and business systems, whether owned or leased by Spare, the employee, or a third party. All employees, contractors, consultants, temporary, and other workers at Spare and its subsidiaries are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with Spare policies and standards, and local laws and regulations. This policy applies to employees, contractors, consultants, temporaries, and other workers at Spare, including all personnel affiliated with third parties. This policy applies to all Spare-controlled company and customer data as well as all equipment, systems, networks and software owned or leased by Spare. Security Incident Reporting All users are required to report known or suspected security events or incidents, including policy violations and observed security weaknesses. Incidents should be reported immediately or as soon as possible by security@sparelabs.com. In your email please describe the incident or observation along with any relevant details. Mobile Device Policy All end-user devices (e.g., mobile phones, tablets, laptops, desktops) must comply with this policy. Employees must use extreme caution when opening email attachments received from unknown senders, which may contain malware. System level and user level passwords must comply with the Access Control Policy. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited. All end-user, personal (BYOD) or company owned devices used to access Spare information systems (i.e. email) must adhere to the following rules and requirements: • Devices must be encrypted with a password-protected screensaver or screen lock after 30 minutes of inactivity • Devices must be locked whenever left unattended • Users must report any suspected misuse or theft of

- a mobile device immediately to Security Team
- Confidential information must not be stored on mobile devices or USB drives (this does not apply to business contact information, e.g., names, phone numbers, and email addresses)
- Any mobile device used to access company email must not be shared with any other person
- Upon termination users agree to return all company owned devices and delete all company information and accounts from any personal devices

Remote Access Policy

Laptops and other computer resources that are used to access the Spare network must conform to the security requirements outlined in Spare's Information Security Policies and adhere to the following standards:

- To ensure mobile devices do not connect a compromised device to the company network, Antivirus policies require the use and enforcement of client-side antivirus software
- Users must not connect to any outside network without a secure, up-to-date software firewall configured on the mobile computer.
- Users are prohibited from changing or disabling any organizational security controls such as personal firewalls, antivirus software on systems used to access Spare resources
- Use of remote access software and/or services (e.g., VPN client) is allowable as long as it is provided by the company and configured for multi factor authentication (MFA)
- Unauthorized remote access technologies may not be used or installed on any Spare system
- If you access from a public computer (e.g., business center, hotel, etc.), log out of session and don't save anything. Don't check "remember me, collect all printed materials and delete downloaded files (generally is discouraged)

Acceptable Use Policy

Spare proprietary and customer information stored on electronic and computing devices whether owned or leased by Spare, the employee or a third party, remains the sole property of Spare for the purposes of this policy. Employees and contractors must ensure through legal or technical means that proprietary information is protected in accordance with the Data Management Policy. The use of Google Drive for business file storage is required for users of laptops or company issued devices. Storing important

	documents on the file share is how you “backup” your laptop. You have a responsibility to promptly report the theft, loss, or unauthorized disclosure of Spare proprietary information. You may access, use or share Spare proprietary information only to the extent it is authorized and necessary to fulfill your assigned job duties. Employees are responsible for exercising good judgment regarding the reasonableness of personal use of company-provided devices. For security and network maintenance purposes, authorized individuals within Spare may monitor equipment, systems and network traffic at any time. Spare reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy. Unacceptable Use The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities. Under no circumstances is an employee of Spare authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing Spare-owned resources. The list below is not exhaustive, but attempts to provide a framework for activities which fall into the category of unacceptable use. The following activities are strictly prohibited, with no exceptions: 1. Violations of the rights of any person or company protected by copyright, trade secret, patent, or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Spare. 2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books, or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Spare or the end user does not have an active license. 3. Accessing data, a server, or an account for any purpose other than conducting Spare business, even if you have authorized access, is prohibited. 4. Exporting software, technical information, encryption software, or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of

any material that is in question.

5. Introduction of malicious programs into the network or systems (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
6. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
7. Using a Spare computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws.
8. Making fraudulent offers of products, items, or services originating from any Spare account. 9. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
9. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient, or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
10. Port scanning or security scanning is expressly prohibited unless prior notification to the Spare engineering team is made.
11. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
12. Circumventing user authentication or security of any host, network, or account. 14. Introducing honeypots, honeynets, or similar technology on the Spare network.
13. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
14. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's session, via any means.
15. Providing information about, or lists of: Spare employees, contractors, partners, or customers to parties outside Spare without authorization.

Email and Communication Activities

When using company resources to access and use the Internet, users must realize they represent the company and act accordingly.

The following activities are strictly prohibited, with no exceptions:

1. Sending unsolicited email messages, including the sending of "junk mail", or other advertising material to individuals who did not specifically request such material (email spam).
2. Any form of harassment via email, telephone, or texting, whether through language, frequency, or size of messages.
3. Unauthorized use, or forging, of email header information.
4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
5. Creating or forwarding "chain letters", "Ponzi", or other "pyramid" schemes of any type.
6. Use of unsolicited email originating from within Spare networks or other service providers on behalf of, or to advertise, any service hosted by Spare or connected via Spare's network.

Additional Policies and Procedures

Incorporated by Reference

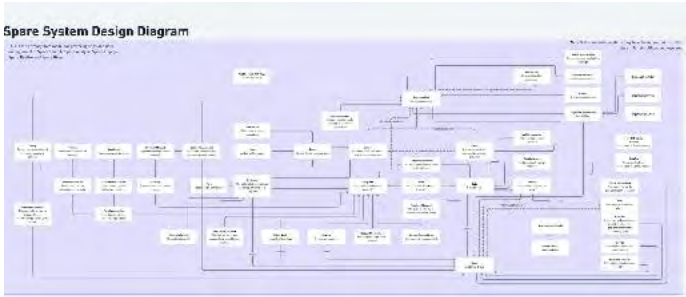
Role	Purpose
<u>@Access Control Policy</u>	To limit access to information and information processing systems, networks, and facilities to authorized parties in accordance with business objectives.
<u>@Asset Management Policy</u>	To identify organizational assets and define appropriate protection responsibilities.
<u>@Business Continuity and Disaster Recovery Plan</u>	To prepare Spare in the event of extended service outages caused by factors beyond our control (e.g., natural disasters, man-made events), and to restore services to the widest extent possible in a minimum time frame.
<u>@Cryptograp hy Policy</u>	To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information.

	<u>@Data Management Policy</u>	To ensure that information is classified and protected in accordance with its importance to the organization.
	<u>@Human Resource Security Policy</u>	To ensure that employees and contractors meet security requirements, understand their responsibilities, and are suitable for their roles.
	<u>@Incident Response Plan</u>	Policy and procedures for suspected or confirmed information security incidents.
	<u>@Operations Security Policy</u>	To ensure the correct and secure operation of information processing systems and facilities.
	<u>@Physical Security Policy</u>	To prevent unauthorized physical access or damage to the organization's information and information processing facilities.
	<u>@Risk Management Policy</u>	To define the process for assessing and managing Spare's information security risks in order to achieve the company's business and information security objectives.
	<u>@Secure Development Policy</u>	To ensure that information security is designed and implemented within the development lifecycle for applications and information systems.
	<u>@Third-Party Management Policy</u>	To ensure protection of the organization's data and assets that are shared with, accessible to, or managed by suppliers, including external parties or third-party organizations such as service providers, vendors, and customers, and to maintain an agreed level of information security and service delivery in line with supplier agreements.
Documentation Policy Security Policies may be modified at any given time by compliance personnel, provided that changes are documented. Compliance personnel is responsible for maintaining a historical record of all policies implemented for 6 years from the date of creation. Policy history is		

	tracked in Notion by maintain a record of all previously implemented versions. Policy Compliance Spare will measure and verify compliance to this policy through various methods, including but not limited to, business tool reports, and both internal and external audits. Exceptions Requests for an exception to this policy must be submitted to the CTO for approval. Violations & Enforcement Any known violations of this policy should be reported to the CTO. Violations of this policy can result in immediate withdrawal or suspension of system and network privileges and/or disciplinary action in accordance with company procedures up to and including termination of employment. Risk Management Policy Purpose To define the methodology for assessing and managing Spare's information security risks in order to achieve the company's business and information security objectives. Scope The risk assessment process may be applied to all business processes, information, information systems, networks, devices, and information processing facilities that are owned or used by Spare applicants, employees, contractors, consultants, vendors, partners, and other users affiliated with Spare, or others using or accessing Spare networks and/or information systems. Policy Spare will ensure that risk management plays an integral part in the governance and management of the organization at a strategic and operational level. The purpose of a risk management policy is designed to ensure that the company achieves its stated business and

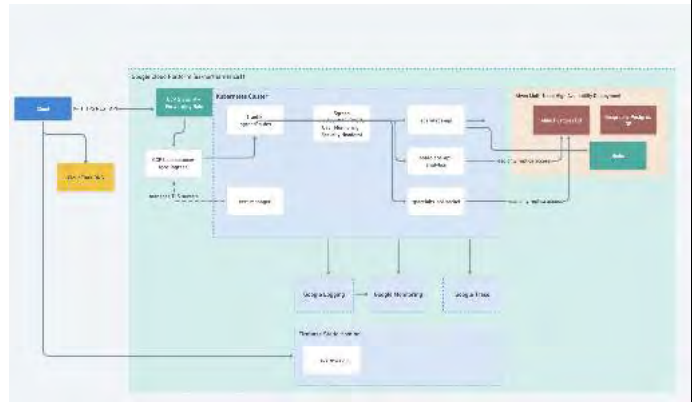
	security goals and objectives. Risk Management Strategy Spare has developed processes to identify those risks that would hinder the achievement of its strategic and operational objectives. Spare will therefore ensure that it has in place the means to identify, analyze, control, and monitor the strategic and operational risks it faces using this risk management policy based on best practices. The CTO will ensure the risk management strategy and policy are reviewed regularly and that: • The risk management policy is applied to relevant areas at Spare • The risk management policy and its operational application are annually reviewed • Non-compliance is reported to appropriate company officers and authorities Practical Application of Risk Management Spare may use a variety of risk reporting formats for the identification of risks, their classification, and evaluation based on factors such as vendors utilized, methodology employed, and the scope of the assessment. In general, and where possible, risks shall be assessed and ranked according to their impact and their likelihood of occurrence. In addition, an internal audit of the information security management system (ISMS) (i.e., information security controls and management processes) shall be performed at least annually. Security risks shall be evaluated at various stages of the software design and development lifecycle as needed. Risk Categories Some risks are within the control of Spare while others may be only to a lesser degree. Spare will consider the risks within each of the following categories: • Technical • Reputational • Contractual • Economic/Financial • Regulatory/Compliance • Fraud

	Each identified risk will be assessed as to its likelihood and impact. Likelihood can be assessed as not likely, somewhat likely, or very likely. Impact can be assessed as not impactful, somewhat impactful, and very impactful. The likelihood and impact will be considered together to formulate an overall risk ranking. Risk Criteria The criteria for determining risk is the combined likelihood and impact of an event adversely affecting the confidentiality, availability, integrity, or privacy of customer data, personally identifiable information (PII), or business critical systems. For all risk inputs such as risk assessments, penetration tests, vulnerability scans, etc., Spare management shall reserve the right to modify automated or third-party provided risk rankings based on its assessment of the nature and criticality of the system processing, as well as the nature, criticality and exploitability (or other relevant factors and considerations) of the identified vulnerability. Risk Response and Treatment Risks will be prioritized and mapped using the approach contained in this policy. The following responses to risk should be employed. Where Spare chooses a risk response other than “Accept,” it shall develop a Risk Treatment Plan. • Mitigate: Spare may take actions or employ strategies to reduce the risk. • Accept: Spare may decide to accept and monitor the risk at the present time. This may be necessary for some risks that arise from external events. • Transfer: Spare may decide to pass the risk on to another party. For example, contractual terms may be agreed to ensure that the risk is not borne by Spare, or insurance may be appropriate for protection against financial loss. • Eliminate: The risk may be such that Spare could decide to cease the activity or to change it in such a way as to end the risk. Risk Management Procedure The procedure for managing risk will meet the following criteria: • Spare will maintain a Risk Register and Treatment

	Plan. • Risks shall be ranked by 'likelihood' and 'severity/impact' as critical, high, medium, low, or negligible. • Overall risk shall be determined through a combination of likelihood and impact. • Risks may be valued to estimate potential monetary loss where practical, or may be considered relative to a control objective • Spare will respond to risks in a prioritized fashion. Remediation priority will consider the risk likelihood and impact, cost, work effort, and availability of resources. Multiple remediations may be undertaken simultaneously. • Periodic reports will be made to the senior leadership of Spare to ensure risks are being mitigated appropriately, and in accordance with business priorities and objectives. Amendment & Termination of this Policy Spare reserves the right to modify, amend or terminate this policy at any time. Exceptions Requests for an exception to this Policy must be submitted to the CTO for approval.
5. Data Flow Diagrams: The purpose of a data flow diagram is to graphically represent data in all forms as it traverses systems including what changes the data and where it is stored at any given time. Examples of what could be represented in this	<i>Provide a data flow diagram(s) that include all information systems that store, process, and/or transmit NCDOT/DMV data.</i>
diagram include data elements (name, address, phone, etc.), data format, encryption and compression, authentication, permissions, session, and registration (HTTP, SNMP, FTP, IRC, SSH, SSL, TLS, DES, 3-DES, AES, SSH, IMAP, RPC, SQL, NFS, API's, Sockets and WinSock). i. Provide data flow diagram(s) of the third-party contractor's services. Attached is an example high level data flow diagram.	 The diagram, titled 'Spare System Design Diagram', illustrates a complex network of data flows. It features numerous interconnected boxes representing different systems, databases, and services. The flows are indicated by lines connecting these components, showing the movement of data across the system architecture. The diagram is presented on a light blue background with a grid pattern.

6. Network Architecture Diagrams: The purpose of network architecture diagrams is to graphically represent the structure of a network and shows the components that make up a network and how they interact, including routers, devices, hubs, firewalls, servers, workstations, printer, etc.

i. Provide network architecture diagrams of the third party contractor's services.



7. Does the third-party contractor have an external risk assessment report that demonstrates the third-party's compliance to industry accepted guidelines (e.g., SOC 2 Type II, ISO 27001, FedRAMP, etc.) that addresses the scope of their proposed services?

i. Provide a copy of the third-party contractor's external risk assessment report.

ii. Describe in detail how the third-party contractor will ensure all external entities supporting the third-party's proposed services receive and maintain SOC 2 Type II (or equivalent) certifications for their roles in supporting the third-party contractor's proposed services and solution.

iii. Does the third-party contractor have and maintain formal agreements with external entities, such as for maintenance and service support for the third-party contractor's service?

NOTE: *It is important to understand a SOC 2 Type II (or equivalent) only indicates the third-party's policies, standards, and procedures were assessed as being compliant with generic industry accepted guidelines. A SOC 2 Type II (or equivalent) does not certify the third-party's services as being compliant with the State's information security policies, guidelines, and standards (e.g., account lockout thresholds, employment background checks (local/State/Federal), minimum password*

Spare undergoes an annual SOC 2 Type II certification.

Please find report attached.

To ensure the same level of security for all external entities supporting our proposed services, we have stringent requirements in place.

When engaging third-party contractors to support our services and solutions, we mandate that they also obtain and maintain SOC 2 Type II (or equivalent) certifications. This certification ensures that the third-party contractor follows the established standards and best practices for security, availability, processing integrity, confidentiality, and privacy of data.

To ensure compliance, we have a comprehensive process in place for selecting and vetting third-party contractors. Before engaging any external entity, we thoroughly evaluate their security controls, practices, and certifications. This evaluation process includes reviewing their SOC 2 Type II reports or equivalent certification reports.

Additionally, we require third-party contractors to undergo regular audits and assessments to maintain their certifications. This ensures that they consistently meet the necessary security standards and that any changes or updates to their systems and processes are reviewed and verified.

Furthermore, we maintain a strong working relationship with our third-party contractors, establishing clear lines of communication and regular check-ins to ensure ongoing

requirements, data classification, change management, etc.). Third-party contractor must periodically perform formal security crosswalks between the third-party contractor's policies/standards and the State's policies/standards to ensure the proper security controls are in place to protect State data.

(References: N.C.G.S § 143B-1375, § 143B-1378; [SISM PS-7](#), [CA-7](#), [RA-3](#)).

compliance with our security requirements. We encourage open dialogue and information sharing regarding any changes or updates in their security practices or certifications.

In the event that a third-party contractor fails to meet or maintain the required SOC 2 Type II or equivalent certification, we take immediate action. This may include reassessing our relationship with the contractor and potentially terminating the partnership if necessary.

Overall, by imposing the requirement for SOC 2 Type II (or equivalent) certifications on our third-party contractors, we ensure that all entities supporting our proposed services meet the same rigorous security standards and practices that we maintain. This approach helps to safeguard our customers' data and maintain the integrity and confidentiality of our services and solutions.

iii. Does the third-party contractor have and maintain formal agreements with external entities, such as for maintenance and service support for the third-party contractor's service?

Yes, as a software-as-a-service business, we ask our third-party contractors to have formal agreements in place with external entities for maintenance and service support related to the services they provide on our behalf. These formal agreements outline the responsibilities, obligations, and expectations of all parties involved.

These agreements typically cover various aspects, such as:

Scope of services: The agreement clearly defines the specific services to be provided by the external entities, including maintenance and service support activities. It outlines the level of support required, response times, and any service-level agreements (SLAs) that need to be met.

Security requirements: The agreements include provisions that ensure the external entities adhere to our security standards and protocols. This may include

	requirements for data encryption, access controls, incident response, and other security measures necessary to protect customer data. Confidentiality and data protection: The agreements establish the confidentiality obligations of the external entities, emphasizing the importance of protecting any sensitive or proprietary information they may have access to during the provision of services. This may include clauses related to data handling, data storage, and data retention. Compliance with regulations and certifications: The agreements may require the external entities to comply with relevant regulations and certifications, such as SOC 2 Type II, to ensure the security and integrity of the services they provide. Termination and dispute resolution: The agreements include provisions for termination, outlining the conditions under which either party may terminate the agreement. Additionally, they may outline procedures for dispute resolution, including mediation or arbitration, to address any conflicts that may arise. By formalizing these agreements, we establish a clear framework for collaboration and ensure that all external entities involved in supporting our services are held accountable for their roles and responsibilities. These agreements serve as a means to align expectations, maintain security standards, and protect the interests of both our customers and our organization.

8. Describe in detail how the third-party contractor's proposed services support NCDOT's Multi-factor authentication (MFA) policy, guidelines, and standards. Specifically speak to Remote Access (SISM AC-17), and Nonlocal Maintenance (SISM MA 4). i. Do the third-party contractor's services enforce MFA for all administrative functions? Explain in detail. ii. Do the third-party contractor's services enforce MFA for all remote access to information systems that process State data? Explain in detail.	Response: 1. Yes MFA may be enforced for all administrative functions. 2. Spare uses WorkOS to integrate with an external identity provider using SAML. This allows agencies to utilize and manage their own authentication protocols and have control over password policy etc. Here is how it works: 1. Configure your Identity Provider (IdP):

- Set up your preferred Identity Provider (e.g., Okta, OneLogin, Azure AD, ADFS) and configure it to work with SAML.
 - Obtain the necessary metadata from your IdP, such as the Entity ID and SSO (Single Sign-On) URL.
2. Set up your Service Provider (SP) with workOS:
- Sign up for a workOS account and create a new project.
 - Install the workOS SDK in your application's backend.
3. Configure workOS settings:
- In your workOS project, navigate to the "Authentication" section and select "SAML."
 - Provide the metadata from your IdP to workOS.
 - Configure other settings, such as the SAML Audience (SP Entity ID) and SAML ACS (Assertion Consumer Service) URL.
4. Implement the SAML flow in your application:
- When a user tries to access a protected resource, redirect them to the workOS /sso/saml endpoint with the appropriate parameters, such as the desired redirect URL after authentication.
 - workOS will initiate the SAML flow and redirect the user to your IdP's SSO URL.
 - The IdP will authenticate the user and generate a SAML response containing the user's identity information.
 - The IdP will redirect the user back to the SAML ACS URL provided by workOS.
 - workOS will validate the SAML response and generate a JWT (JSON Web Token) containing the user's identity.
 - Retrieve the JWT in your application backend and validate it.
 - If the JWT is valid, log the user in and grant access to the requested resource.
5. Handle user logout:
- When a user logs out of your application, redirect them to the workOS /sso/saml/logout endpoint.
 - workOS will initiate the SAML logout flow and redirect the user to the IdP's logout URL.
 - The IdP will handle the logout process and redirect the user back to your

	application's specified logout URL. 2. Spare is a SAAS solution so no remote access is enabled or required.
9. The North Carolina Identity Management Service (NCID) is the standard identity and access management platform provided by the Department of Information Technology. NCID is a web-based application that provides a secure environment for state agency, local government, business, and individual users to log in and gain access to real-time resources, such as customer-based applications and information retrieval. i. Are the third-party contractor's proposed services capable of integrating with the State's NCID solution? ii. Describe in detail how the third-party contractor's services integrate with the North Carolina Identity (NCID) Service. References: https://it.nc.gov/ncid/ https://it.nc.gov/ncid-frequently-asked-questions https://it.nc.gov/ncid-application-integration-requirements-airn-saml-based	<i>Third-party provides a comprehensive response here. Please review and understand the SISM requirements before responding.</i> Response: 1. Yes, Spare will be able to integrate with State's NCID solution using WorkOS. 2. Here is how Spare would integrate with NCID using WorkOS: To illustrate how to use workOS with NCDOT (North Carolina Department of Transportation) identity management, we can create a high-level integration plan. Please note that this plan is a general outline and may require customization based on the specific requirements and configurations of your organization and the workOS platform. Here's a suggested plan: 1. Identify Integration Requirements: - Determine the specific integration requirements between workOS and NCDOT identity management (NCID). - Define the use cases and functionalities that need to be supported through the integration. 2. Set up workOS Account: - Sign up for a workOS account if you haven't already. - Familiarize yourself with workOS documentation and resources. 3. Configure workOS: - Access the workOS dashboard and navigate to the appropriate settings. - Configure the required authentication settings and protocols, such as SAML v2, to align with NCID requirements. - Set up the necessary authentication callbacks and endpoints to handle authentication requests and responses. 4. Establish Connection with NCID: - Obtain the required integration details and credentials from NCID, such as the SAML metadata and service provider configuration. - Configure workOS to establish a connection with

NCID using the provided integration details.

5. Implement SAML Integration:

- Develop the necessary code or configuration changes in your application or system to support SAML-based authentication using workOS.
- Integrate the workOS SDK or libraries into your application to handle SAML authentication flows and communicate with NCID.

6. Test and Validate Integration:

- Perform thorough testing to ensure the integration between workOS and NCID is functioning as expected.
- Test various authentication scenarios and edge cases to validate the reliability and security of the integration.
- Collaborate with NCDOT or NCID representatives to conduct joint testing and obtain their feedback.

7. Security and Compliance:

- Ensure that the integration adheres to the required security and compliance standards set by NCDOT and NCID.
- Implement any necessary security measures, such as encryption and secure data handling, to protect user information.

8. Documentation and User Training:

- Create documentation and user guides that explain how to use the integrated system, including authentication procedures and any specific instructions related to workOS and NCID.
- Provide training or informational sessions to relevant stakeholders, administrators, and end users to familiarize them with the new authentication process.

9. Deployment and Go-Live:

- Prepare for the production deployment of the integrated system, ensuring all necessary configurations and settings are in place.
- Coordinate with NCDOT or NCID teams for the final approval and scheduling of the go-live process.

10. Ongoing Maintenance and Support:

- Establish a process for ongoing maintenance and support of the integrated system, including monitoring for any issues or updates related to workOS or NCID.
- Stay updated with workOS and NCID documentation, releases, and security updates to ensure the integration remains robust and up to date.

	Please note that this plan provides a high-level overview of the integration process. It is important to consult with the appropriate technical teams and follow any specific guidelines or requirements provided by NCDOT and workOS to ensure a successful integration.
10. Provide a list of all entities that support the third-party contractor's services along with a detailed description of their roles and responsibilities.	Data Processors • Aiven LTD: Cloud storage management • Google LLC (GCP): Cloud computing, storage, and networking; physical security of hardware. • Amazon Web Services (AWS): Cloud computing, storage, and networking; physical security of hardware. • Intercom: Application utilization tracking. • Functional Software, Inc (Sentry): System error logging. • Sqreen Inc.: Application security monitoring. • Twilio Inc.: Transmission of SMS, phone calls. • MessageBird: Transmission of SMS, phone calls. • Sendgrid: Transmission of email. • Zapier: Custom-built data integrations enabled upon customer request.
11. All operating systems (OS) AND major application software components (e.g., Microsoft SQL, Apache Tomcat, Oracle Weblogic, etc.), must NOT be past N-1. Applications which are not operating on the most recent platform MUST have a roadmap to upgrade with a State approved timeline. i. Do the third-party contractor's proposed services support the State's N-1 requirement? ii. Explain in detail how the third-party maintains the N-1 standard.	Spare ensures that only the latest versions of all software components are used. This automatically ensures that states N-1 requirement is met.
12. Does the third-party contractor's proposed services meet Federal Records Management Requirements, including the ability to support record holds, National Archives and Records Administration (NARA) requirements, and Freedom of Information Act (FOIA) requirements?	Yes, Spare will develop a comprehensive policy to meet NARA and FOIA requirements as per the following structure: 1. Introduction - Purpose of the Policy - Scope and Applicability 2. Policy Statement - Commitment to complying with Federal Records Management Requirements - Recognition of the importance of record

holds, National Archives and Records Administration (NARA) requirements, and Freedom of Information Act (FOIA) requirements

3. Definitions

- Key terms related to Federal Records Management

4. Roles and Responsibilities

4.1 Records Management Officer (RMO)

- Designation of a qualified RMO responsible for overseeing records management activities
- Responsibilities include developing and implementing records management policies, procedures, and training programs

4.2 Records Custodians

- Designation of records custodians responsible for managing records within their respective areas
- Responsibilities include record creation, classification, retention, and disposal in accordance with the policy

4.3 Legal and Compliance Department

- Collaboration with the legal and compliance department to ensure adherence to legal requirements, record holds, and FOIA requests

5. Record Creation and Capture

- Procedures for creating and capturing records in a manner consistent with Federal requirements
- Standards for metadata and indexing to facilitate records management

6. Record Classification and Retention

- Guidelines for classifying records based on their business value and legal requirements
- Establishment of retention periods in accordance with NARA guidelines and other applicable regulations
- Procedures for periodic review and disposition of records

7. Record Holds

- Process for implementing and managing record holds in response to litigation, investigations, or other legal requirements
- Notification procedures and communication channels for record hold directives

- Documentation of record holds, including dates, reasons, and release criteria
8. Records Storage and Access
 - Secure storage and protection of physical records
 - Guidelines for secure electronic storage and access control
 - Procedures for retrieving and providing access to records in compliance with FOIA requirements
 - Protection of records from unauthorized access, alteration, or destruction
 9. Records Maintenance and Disposition
 - Procedures for maintaining the integrity and authenticity of records throughout their lifecycle
 - Methods for secure disposal and destruction of records in accordance with approved schedules and legal requirements
 - Documentation of disposal actions, including dates and methods used
 10. Records Management Training and Awareness
 - Training programs to educate employees on Federal Records Management Requirements
 - Training on record creation, classification, retention, and disposal procedures
 - Regular communication and awareness campaigns to promote compliance and best practices
 11. Compliance Monitoring and Auditing
 - Regular monitoring of records management practices to ensure compliance
 - Internal audits to assess adherence to the policy and identify areas for improvement
 - Corrective actions and continuous improvement measures based on audit findings
 12. Documentation and Reporting
 - Documentation of records management policies, procedures, and activities
 - Reporting mechanisms for record holds, NARA compliance, and FOIA requests
 - Record of training activities, including attendance and completion certificates
 13. Review and Updates
 - Regular review of the policy to ensure its

	effectiveness and relevance - Procedures for updating the policy to reflect changes in regulations or organizational requirements - Documentation of policy reviews and updates
13. Does the third-party contractor's services handle, store, process and/or transmit State data outside the physical boundaries of the United States? If yes, explain in detail.	No, all data is stored and processed within the boundaries of the United States.
14. Are FIPS 140-2 Validated or National Security Agency (NSA)- Approved cryptographic modules consistently used where cryptography is required? Explain in detail. The Statewide Data Classification and Handling Policy is located here: https://it.nc.gov/documents/statewide-policies/state-wide-data-classification-handling-policy/open The Statewide Media Protection Policy is located here: https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Media_Protection.pdf	Spare will evaluate the risks inherent in processing and storing data, implementing cryptographic controls to mitigate those risks where deemed appropriate. Where encryption is in use, strong cryptography with associated key management processes and procedures shall be implemented and documented. All encryption shall be performed in accordance with industry standards, including NIST SP 800-57. For all personal data, Spare shall consider the state of the art, the costs of implementation and the nature, scope, context, and purposes of processing. We also consider the risk of varying likelihood and severity to the rights and freedoms of natural persons, implementing appropriate technical and organizational measures surrounding the pseudonymization and encryption of data to ensure a level of security appropriate to the risk. Currently the CTO (Alexey Indeev) and personnel approved by the CTO have access to the encryption keys.
15. Do the third-party contractor's services encrypt State data in transit and at rest? Explain in detail.	Aiven at-rest data encryption covers both active service instances as well as service backups in cloud object storage. Service instances and the underlying VMs use full volume encryption using LUKS with a randomly generated ephemeral key per each instance and each volume. The key is never re-used and will be trashed at the destruction of the instance, so there's a natural key rotation with roll-forward upgrades. We use the LUKS2 default mode aes-xts-plain64:sha256 with a 512-bit key.

	Backups are encrypted with a randomly generated key per file. These keys are in turn encrypted with RSA key-encryption key-pair and stored in the header section of each backup segment. The file encryption is performed with AES-256 in CTR mode with HMAC-SHA256 for integrity protection. The RSA key-pair is randomly generated for each service. The key lengths are 256-bit for block encryption, 512-bit for the integrity protection and 3072-bits for the RSA key.
16. Do any information system components used by the third-party contractor to store, process, transmit, and/or can impact the security and privacy of NCDOT data use deprecated transport layer protocols (e.g., SSL, TLS 1.0, TLS 1.1)? 1.1)? Explain in detail.	No, only TLS 1.2 or above is used for encryption of data during transit.
17. State requires minimum 8-character complex passwords (Upper, Lower, Special Character and Numerical)? i. Explain in detail how the third-party's services enforce the State's password policy and standards (SISM AC , IA , MA , SC , SI , SA).	By using NCID for authentication, Spare will enable NCDIT to enforce exactly the type of password policy it wants including the 8-character complex password requirement.
18. Explain in detail how the third-party contractor's services detect, contain, and eradicate malicious software? [SISM SI-3 , SISM SI-3 , SISM MA-3]	Anti-malware protections shall be utilized on all employee issued laptops except for those running operating systems not normally prone to malicious software. Additionally, threat detection and response software shall be utilized for company email. The anti-malware protections utilized shall be capable of detecting all common forms of malicious threats. Spare should scan all files upon their introduction to systems, and continually scan files upon access, modification, or download. Anti-malware definition updates should be configured to be downloaded and installed automatically whenever new updates are available. Known or suspected malware incidents must be reported as a security incident. It is a violation of company policy to disable or alter the configuration of anti-malware protections without authorization.
19. Explain in detail how the third-party contractor's services store audit data in a tamper-resistant manner and meets chain of custody and e-discovery requirements? [SISM AU-7 , SISM AU 9]	Only the CTO or authorized persons can edit audit data which is encrypted at rest. We also leverage Google KMS for encryption key management and key rotation for protection of key data elements.

20. Explain in detail how the third-party contractor's services detect unauthorized or malicious use of the systems, including insider threat and external intrusions? [[SISM SI-4](#), [SISM SI-4 \(4\)](#), [SISM SI-7](#), [SISM SI-7 \(7\)](#)]

Below is part of our Operational Security Policy:

Information about technical vulnerabilities of information systems being used shall be obtained in a timely fashion, the organization's exposure to such vulnerabilities shall be evaluated, and appropriate measures taken to address the associated risk. A variety of methods shall be used to obtain information about technical vulnerabilities, including vulnerability scanning, penetration tests, and the bug bounty program.

External vulnerability scans shall be run on the production environment at least quarterly. Interior vulnerability scans shall be run against test environments which mirror production configurations.

Penetration tests of the applications and production network shall be performed at least annually. Additional scanning and testing shall be performed following major changes to production systems.

The IT and Engineering departments shall evaluate the severity of vulnerabilities, and if it is determined to be a critical or high-risk vulnerability, a service ticket will be created. The Spare assessed severity level may differ from the level automatically generated by scanning software or determined by external researchers based on Spare's internal knowledge and understanding of technical architecture and real-world impact/exploitability. Tickets are assigned to the system, application, or platform owners for further investigation and/or remediation.

Vulnerabilities assessed by Spare shall be remediated in the following timeframes:

Critical - 30 days

High - 30 days

Medium - 60 days

Low - 90 days

Informational- as needed

Service tickets for any vulnerability which cannot be remediated within the standard timeline must show a risk treatment plan and planned remediation timeline.

21. Explain in detail how the third-party contractor performs security code analysis (static and dynamic) and evaluates code for security flaws, as well as identify, track, and remediate security flaws? [SISM SA-11]	Spare follows secure coding practices that includes the following: Changes to systems within the development lifecycle shall be controlled by the use of formal change control procedures. Change control procedures and requirements are described in the Spare Operations Security Policy. Significant code changes must be reviewed and approved by software engineer before being merged into any production branch in accordance with the Code Review guidelines.
22. Explain in detail how the third-party contractor's records retention policy, standards, practices, and information systems adhere to the State's functional records schedule. [DNCR Functional Schedule, DNCR Information Technology, DNCR Risk Management, SISM AU-7, SISM AU-11]? A "Record" is defined as a set of data (logical and physical) treated as a unit. Examples include, but are not limited to, IT Security Program documents, data flow and architecture diagrams, system/application diagrams, change management activities, risk management activities, vulnerability scan results, <u>system/application logs</u>, etc. i. 911.3 Data Documentation Records Records concerning data in automated systems; includes data element dictionary, file layout, code book or table, Entity relationships tables, and other records related to the structure, management, and Entity of data RETAIN UNTIL: System is discontinued and/or replaced PLUS: 3 years THEN: Destroy ii. 914.< Digitization and Scanning Records Records concerning data entry and imaging operations; includes quality control records and paper records that are digitized. RETAIN UNTIL: Digitized PLUS: 10 days THEN: Destroy NOTE: The digital surrogate becomes the record copy and must be retained according to the disposition instructions for that record type.	Spare's data management policy guides records management that would be further refined should Spare be chosen for NCDOT's projects: Purpose To ensure that information is classified, protected, retained and securely disposed of in accordance with its importance to the organization. Scope All Spare data, information and information systems. Policy Spare classifies data and information systems in accordance with legal requirements, sensitivity, and business criticality in order to ensure that information is given the appropriate level of protection. Data owners are responsible for identifying any additional requirements for specific data or exceptions to standard handling requirements. Information systems and applications shall be classified according to the highest classification of data that they store or process. Data Classification To help Spare and its employees easily understand requirements associated with different kinds of information, the company has created three classes of data. Confidential Highly sensitive data requiring the highest levels of protection; access is restricted to specific employees or departments, and these records can only be passed to others with approval from the data owner, or a company

iii. [915.3 Electronic Records Policies](#)

Records documenting the policies and procedures employed by the agency to maintain authentic and accessible electronic records.

RETAIN UNTIL: Superseded/Obsolete

PLUS: 3 years

THEN: Destroy

iv. [924.1\(1\) Network and System Security Records](#)

Records documenting the security of networks and systems; includes records concerning firewalls, anti-virus programs, and other related records.

RETAIN FROM: Creation

PLUS: 1 year

THEN: Destroy*

v. [924.1\(2\) Network and System Security Records](#)

records documenting access requests and authorizations, system access logs, and other related records

RETAIN FROM: Creation

PLUS: 1 year

THEN: Destroy

vi. [924.2 Network and System Security Records](#)

Records documenting incidents involving unauthorized attempted entry or probes on data processing systems, information technology systems, telecommunications networks, and electronic security systems, including associated software and hardware; includes logs, extracts, compilations of data, and other related records

RETAIN FROM: Creation

PLUS: 2 years

THEN: Destroy*

vii. [926.3 System Documentation](#)

records documenting operating systems, application programs, structure and form of datasets, system structure, and system-to-system communication; includes system

overviews, dataset inventories, server names, IP addresses, purpose of the systems, Entity-supplied documentation, installed software, and current source code.

RETAIN UNTIL: Superseded/Obsolete

PLUS: 3 years

THEN: Destroy

viii. [1623.3 Disaster Recovery Records](#)

Records concerning minor or routine agency recovery operations that are managed with minimal disruption to

executive. Example include:

- Customer Data
- Personally identifiable information (PII)
- Company financial and banking data
- Salary, compensation and payroll information
- Strategic plans
- Incident reports
- Risk assessment reports
- Technical vulnerability reports
- Authentication credentials
- Secrets and private keys
- Source code
- Litigation data

Restricted

Spare proprietary information requiring thorough protection; access is restricted to employees with a “need-to-know” based on business requirements. This data can only be distributed outside the company with approval. This is default for all company information unless stated otherwise. Examples include:

- Internal policies
- Legal documents
- Meeting minutes and internal presentations
- Contracts
- Internal reports
- Slack messages
- Email

Public

Documents intended for public consumption which can be freely distributed outside Spare. Examples include:

- Marketing materials
- Product descriptions
- Release notes
- External facing policies

Labeling

Confidential data should be labeled “confidential” whenever paper copies are produced for distribution.

Data Handling

Confidential Data Handling

Confidential data is subject to the following protection and handling requirements:

- Access for non-preapproved-roles requires documented approval from the data owner
- Access is restricted to specific employees, roles and/or departments
- Confidential systems shall not allow

normal operations
RETAIN UNTIL: Complete
PLUS: 3 years
THEN: Destroy

ix. [1314.2 Consultant, Contractor, Provider, and Entity Due Diligence Records](#)

Records documenting the evaluation of consultants, contractors, providers, and entities with whom the agency conducts business; includes financial stability, information security risk assessments, and other related records
RETAIN UNTIL: Contract expires
PLUS: 2 years
THEN: Destroy

unauthenticated or anonymous access

- Confidential Customer Data shall not be used or stored in non-production systems/environments
- Confidential data shall be encrypted in transit over public networks
- Mobile device hard drives containing confidential data, including laptops, shall be encrypted
- Mobile devices storing or accessing confidential data shall be protected by a log-on password or passcode and shall be configured to lock the screen after five (5) minutes of non-use
- Backups shall be encrypted
- Confidential data shall not be stored on personal phones or devices or removable media including USB drives, CD's, or DVD's
- Paper records shall be labeled "confidential" and securely stored and disposed
- Hard drives and mobile devices used to store confidential information must be securely wiped prior to disposal or physically destroyed
- Transfer of confidential data to people or entities outside the company shall only be done in accordance with a legal contract or arrangement, and the explicit written permission of management or the data owner

Restricted Data Handling

Restricted data is subject to the following protection and handling requirements:

- Access is restricted to users with a need-to-know based on business requirements
- Restricted systems shall not allow unauthenticated or anonymous access
- Transfer of restricted data to people or entities outside the company or authorized users shall require management approval and shall only be done in accordance with a legal contract or arrangement, or the permission of the data owner
- Paper records shall be securely stored and disposed
- Hard drives and mobile devices used to store restricted information must be securely wiped prior to disposal or physically destroyed

Public Data Handling

No special protection or handling controls are required for public data. Public data may be freely distributed.

Data Retention

Spare shall retain data as long as the company has a need for its use, or to meet regulatory or contractual

	requirements. Once data is no longer needed, it shall be securely disposed of or archived. Please find our current Data Retention Matrix here:  Data Retention Matrix and Procedure Data & Device Disposal Data classified as restricted or confidential shall be securely deleted when no longer needed. Spare shall assess the data and disposal practices of third-party vendors in accordance with the Third-Party Management Policy. Only third-parties who meet Spare requirements for secure data disposal shall be used for store and process restricted or confidential data. Spare shall ensure that all restricted and confidential data is securely deleted from company devices prior to, or at the time of disposal. Annual Data Review Management shall review data retention requirements during the annual review of this policy. Data shall be disposed of in accordance with this policy. Legal Requirements Under certain circumstances, Spare may become subject to legal proceedings requiring retention of data associated with legal holds, lawsuits, or other matters as stipulated by Spare legal counsel. Such records and information are exempt from any other requirements specified within this Data Management Policy and are to be retained in accordance with requirements identified by the Legal department. All such holds and special retention requirements are subject to annual review with Spare's legal counsel.
23. Does the third-party contractor have the capability to notify the State within 24 hours of suspected and/or confirmed incidents? Explain in detail.	Yes, Spare commits to informing the state within 24 hours of suspects or confirmed incidents as part of the incident management policy.
24. If the third-party contractor's services provide email "send as" capabilities, does it support DMARC and DKIM for email protection? If not, explain in detail.	Not Applicable
25. Describe in detail how the third-party contractor's services support NCDOT's Data Protection and Classification policy, guidelines, and standards. Specifically speak to Security Impact Analysis (SISM CM-4), Media Protection Policy (SISM MP-1), Media Marking (SISM MP-3), Media Storage (SISM MP 4), Media Transport (SISM MP-5), Media Sanitization (SISM MP-6), Media Use (SISM MP-7), Prohibit	Data Classification To help Spare and its employees easily understand requirements associated with different kinds of information, the company has created three classes of data.

Use Without Owner ([SISM MP-7\(1\)](#)), Security Categorization ([SISM RA-2](#)), and the Statewide Data Classification Policy.

Confidential

Highly sensitive data requiring the highest levels of protection; access is restricted to specific employees or departments, and these records can only be passed to others with approval from the data owner, or a company executive. Example include:

- Customer Data
- Personally identifiable information (PII)
- Company financial and banking data
- Salary, compensation and payroll information
- Strategic plans
- Incident reports
- Risk assessment reports
- Technical vulnerability reports
- Authentication credentials
- Secrets and private keys
- Source code
- Litigation data

Restricted

Spare proprietary information requiring thorough protection; access is restricted to employees with a “need-to-know” based on business requirements. This data can only be distributed outside the company with approval. This is default for all company information unless stated otherwise. Examples include:

- Internal policies
- Legal documents
- Meeting minutes and internal presentations
- Contracts
- Internal reports
- Slack messages
- Email

Public

Documents intended for public consumption which can be freely distributed outside Spare. Examples include:

- Marketing materials
- Product descriptions
- Release notes
- External facing policies

Labeling

Confidential data should be labeled “confidential” whenever paper copies are produced for distribution.

26. Describe in detail how the third-party contractor's services support NCDOT's **Incident Response** policy, guidelines, and standards. Specifically speak to Incident Response Plan Testing ([SISM IR-3](#)), Incident Response Plan Testing ([SISM IR-3\(2\)](#)), Incident Handling ([SISM IR-4](#)), Incident Monitoring ([SISM IR-5](#)), Incident Reporting ([SISM IR-6](#)), and Incident Response Plan ([SISM IR-8](#)).

Incident Response Plan

Purpose

This document establishes the plan for managing information security incidents and events, and offers guidance for employees or incident responders who believe they have discovered, or are responding to, a security incident.

Scope

This policy covers all information security or data privacy events or incidents.

Incident and Event Definitions

A security event is an observable occurrence relevant to the confidentiality, availability, integrity, or privacy of company controlled data, systems or networks. A security incident is a security event which results in loss or damage to the confidentiality, availability, integrity, or privacy of company controlled data, systems or Networks.

Incident Reporting & Documentation

Reporting

If a Spare employee, contractor, user, or customer becomes aware of an information security event or incident, possible incident, imminent incident, unauthorized access, policy violation, security weakness, or suspicious activity, then they shall immediately report the information using one of the following communication channels:

- Email security@sparelabs.com information or reports about the event or incident
- Contact members of the security team through Slack

Reporters should act as a good witness and behave as if they are reporting a crime.

Reports should include specific details about what has been observed or discovered.

Severity

Security team shall monitor incident and event tickets and shall assign a ticket severity based on the following categories. S3/S4 - Low and Medium Severity

	Issues meeting this severity are simply suspicions or odd behaviours. They are not verified and require further investigation. There is no clear indicator that systems have tangible risk and do not require emergency response. This includes lost/stolen laptop with disk encryption, suspicious emails, outages, strange activity on a laptop, etc. S2 - High Severity High severity issues relate to problems where an adversary or active exploitation hasn't been proven yet, and may not have happened, but is likely to happen. This may include lost/stolen laptop without encryption, vulnerabilities with direct risk of exploitation, threats with risk or adversarial persistence on our systems (e.g.: backdoors, malware), malicious access of business data (e.g.: passwords, vulnerability data, payments information), or threats that put any individual at risk of physical harm. S1 - Critical Severity Critical issues relate to actively exploited risks and involve a malicious actor. Identification of active exploitation is required to meet this severity category. Escalation and Internal Reporting S1 - Critical Severity: S1 issues require immediate notification to Engineering management. S2 - High Severity: A Jira ticket must be completed and the appropriate manager (see S1 above) must also be notified via Slack with a reference to the ticket number. S3/S4 - Medium and Low Severity: A Jira ticket must be created and assigned to the appropriate department for response. Documentation All reported security events, incidents, and response activities shall be documented in Jira. A root cause analysis may be performed on all verified S1 security incidents. A root cause analysis report shall be documented and referenced in the incident ticket. The root cause analysis shall be reviewed by the CTO who shall determine if a post-mortem meeting will be called.

	Incident Response Process For critical issues, the response team will follow an iterative response process designed to investigate, contain exploitation, eradicate the threat, recover system and services, remediate vulnerabilities, and document a post-mortem with the lessons of an incident. • Summary • Event reported • Triage and analysis • Investigation • Containment & neutralization (short term work) • Recovery & vulnerability remediation • Hardening & Detection improvements (lessons learned, long term work) CTO / COO / Engineering Manager / Operations Manager will manage the incident response effort. A central “War Room” will be designated, which may be a physical or virtual location (i.e Slack channel). A recurring Incident Response Meeting will occur at regular intervals until the incident is resolved. Legal and executive staff will be informed as needed Incident Response Meeting Agenda • Update Incident Ticket and timelines • Document new Indicators of Compromise (IOCs) • Perform investigative Q&A • Apply emergency mitigations • Plan long term mitigations • Document Root Cause Analysis (RCA) • Additional items as needed Special Considerations Internal Issues Issues where the malicious actor is an internal employee, contractor, vendor, or partner requires sensitive handling. The incident manager shall contact the Executive Team directly and will not discuss with other employees. These are critical issues where follow-up must occur.

	Compromised Communications Incident responders must have Slack messaging arranged before listing themselves as incident members. If there are IT communication risks, an out of band solution will be chosen, and communicated to incident responders via phone calls or text messaging. Additional Requirements • Suspected and reported events and incidents shall be documented. • Suspected incidents shall be assessed and classified as either an event or an incident. • Incident response shall be performed according to this plan and any associated procedures. • All incidents shall be formally documented, and a documented root cause analysis shall be performed. • Suspected and confirmed unauthorized access events shall be reviewed by the Incident Response Team. Breach determinations shall only be made by the CEO and legal counsel in coordination with executive management. • Spare shall promptly and properly notify customers, partners, users, affected parties, and regulatory agencies of relevant incidents or breaches in accordance with Spare policies, contractual commitments, and regulatory requirements. Roles & Responsibilities Every employee and user of any Spare information resources has responsibilities toward the protection of the information assets. The table below establishes the specific responsibilities of the incident responder roles. Incident Manager The Incident Manager is the primary and ultimate decision maker during the response period. The Incident Manager is ultimately responsible for resolving the incident and formally closing incident response actions. Incident Manager

	should be an engineering manager or an engineer (if primary resources are not available). These responsibilities include: • Ensuring the right people from all functions are actively involved at all times Status updates are communicated to the appropriate persons at regular intervals • Incidents are resolved in the immediate term • Determining necessary follow-up actions • Assigning follow-up activities to the appropriate people • Promptly reporting incident details which may trigger breach reporting, in writing to the CTO. Incident Response Team (IRT): The individuals who have been engaged and are actively working on the incident. All members of the IRT will remain engaged in incident response until the incident is formally resolved, or they are formally dismissed by the Incident Manager. Engineers (Support and Development) Qualified engineers will be placed into the on-call rotation and may act as the Incident Manager (if primary resources are not available) or a member of the IRT when engaged to respond to an incident. Engineers are responsible for understanding the technologies and components of the information systems, the security controls in place including logging, monitoring, and alerting tools, appropriate communications channels, incident response protocols, escalation procedures, and documentation requirements. When Engineers are engaged in incident response, they become members of the IRT. Users Employees and contractors of Spare. Users are responsible for following policies, reporting problems, suspected problems, weaknesses, suspicious activity, and security incidents and events. Customers Customers are responsible for reporting problems with their use of Spare services. Customers are responsible for verifying

	that reported problems are resolved. Legal Counsel Responsible, in conjunction with the CEO and executive management, for determining if an incident shall be considered a reportable breach. Counsel shall review and approve in writing all external breach notices before they are sent to any external party. Executive Management Responsible, in conjunction with the CEO and legal counsel, for determining if an incident shall be considered a reportable breach. An appropriate company officer shall review and approve in writing all external breach notices before they are sent to any external party. Spare shall seek stakeholder consensus when determining whether a breach has occurred. The Spare CEO shall make a final breach determination in the event that consensus cannot be reached. Management Commitment Spare management has approved this policy and commits to providing the resources, tools and training needed to reasonably respond to identified security events and incidents with the potential to adversely affect the company or its customers. Exceptions Requests for an exception to this Policy must be submitted to and authorized by the CTO for approval. Exceptions shall be documented. Violations & Enforcement Any known violations of this policy should be reported to the CTO. Violations of this policy may result in immediate withdrawal or suspension of system and network privileges and/or disciplinary action in accordance with company procedures up to and including termination of employment.
27. Describe in detail how the third-party contractor's services support NCDOT's Contingency Planning policy, guidelines, and standards. Specifically speak to Contingency Planning Policy (SISM CP-1), Contingency Plan (SISM CP-2),	Business Continuity and Disaster Recovery Plan

Contingency Plan Training (SISM CP-3), Contingency Plan Testing and Exercises (SISM CP-4), Contingency Plan Alternate Storage Site (SISM CP-6), Contingency Plan Alternate Processing Site (SISM CP-7), Information System Backup (SISM CP-9), Testing for Reliability/Integrity (CP-9(1)), and Information System Recovery and Reconstitution (SISM CP-10). i. Describe in detail how the third-party contractor's services recover the system(s) to a known and functional state following an outage, breach, DoS attack, or disaster? [SISM CP-2, SISM CP-9, SISM CP-10] ii. Do the third-party contractor's services have alternate storage and processing facilities? [SISM CP-6, SISM CP 7]. If yes, explain in detail. iii. Does the third-party contractor have service level agreements (SLAs) in place with all third-party service providers including telecommunications providers? [SISM CP-8] iv. Describe in detail the third-party contractor's information systems log recovery capabilities for each of the systems that handle, store, process, transmit, and/or can impact the security and privacy of NCDOT data? v. Provide copies of the Business Impact Analysis (BIA) and Disaster Recovery Plan (DRP) for the third-party's proposed services. Attached are templates. NCDIT-T_Disaster_R NCDIT-T_Business_I ecovery_Plan_(DRP)_ mpact_Analysis_(BIA)	Effective Date: April 4, 2023 Purpose The purpose of this business continuity plan is to prepare Spare in the event of extended service outages caused by factors beyond our control (e.g., natural disasters, man-made events), and to restore services to the widest extent possible in a minimum time frame. In case of a remote first company like Spare, it is sufficient to have simple contingency plans in the form of service-level agreements with companies that host our data and services. Scope All Spare production systems that are business critical. This policy applies to all employees of Spare and to all relevant external parties. The following scenarios are excluded from the BC/DR plan scope: - Loss of availability for a production hosting service providers (i.e., Google Cloud Platform, Aiven) - Loss of availability of any Spare offices (these will be considered incidents) In the event of a loss of availability of a hosting service provider, the primary engineering incident responders will confer with the customer success staff and executive staff to determine an appropriate response strategy. Policy In the event of a major disruption to production services, senior managers and executive staff shall determine mitigation actions. A disaster recovery test, including a test of backup restoration processes, shall be performed on an annual basis.

	Continuity of information security shall be considered along with operational continuity. In the case of an information security event or incident, refer to the Incident Response Plan. Communications and Escalation Executive staff and senior managers should be notified of any disaster affecting Spare operations. Communications shall take place over any available regular channels including Slack, email and Zoom. Plan Activation For a business continuity plan to be effective, it needs to be triggered as soon as possible; too early or late can reduce its efficacy. Key decision points to consider when a BCP has to be triggered or invoked are given below: - When an incident turns into an event like a disaster, breach - When the estimated time of resolution for a potential breach is greater than the normal estimated time for regular security incidents - When the recovery of an incident is uncertain, a decision must be made to invoke the business continuity plan if the disruption cannot be resolved within the specified incident recovery timelines.
28. Describe in detail how the third-party contractor's services support NCDOT's Configuration Management policy, guidelines, and standards. Specifically speak to Configuration Management Policy (SISM CM-1), Baseline Configuration (SISM CM-2), Configuration Change Control (SISM CM-3), Security Impact Analysis (SISM CM-4), Access Restrictions for Change (SISM CM-5), Configuration Settings (SISM CM-6), Least Functionality	Change Management comes under the purview of Spare's Operations Security Policy:

([SISM CM-7](#)), Information System Component Inventory ([SISM CM-8](#)), Automated Unauthorized Component Detection ([SISM CM-8\(3\)](#)), Configuration Management Plan ([SISM CM-9](#)), Software Usage Restrictions ([SISM CM-10](#)), Separation of Duties ([SISM AC-5](#)), Remote Access ([SISM AC-17](#)), Timely Maintenance ([SISM MA-6](#)), Continuous Monitoring ([SISM CA-7](#)), Flaw Remediation ([SISM SI-2](#)), Malicious Code Protection ([SISM SI-3](#)), System Development Life Cycle ([SISM SA-3](#)), and Developer Configuration Management ([SISM SA-10](#)).

- i. Provide a copy of the third-party contractor's Change Management Policy, Standards and Procedures.
- ii. Provide a copy of the third-party contractor's Configuration Management Plan, Policy, Standards and Procedures.
- iii. Does the third-party contractor's change management capability include a fully functioning Change Advisory Boards (CAB)/ Technical Review Boards (TRB)?
- iv. Does the third-party contractor have and use development and/or test environments to verify changes before implementing them in the production environment?
- v. Within the third-party contractor's proposed solution, are all products and services still actively supported?
- vi. Does the third-party contractor have a lifecycle management plan that ensures products are updated before they reach the end of life?
- vii. Provide a copy of the third-party contractor's Security Impact Analysis (SIA) for the third-party's proposed solution. Below is a Security Impact Analysis template ([SISM CM-4](#)).

NCDIT-T_Security_Impact_Analysis_(SIA)_T

Change Management

Changes to the organization, business processes, information processing facilities, and systems that affect information security in the production environment and financial systems shall be controlled. All significant changes to in-scope systems must be documented.

Change management processes shall include:

- Processes for planning and testing of changes, including remediation measures
- Documented managerial approval and authorization before proceeding with changes that may have a significant impact on information security, operations, or the production platform
- Advance communication/warning of changes, including schedules and a description of reasonably anticipated effects, provided to all relevant internal and external stakeholders
- Documentation of all emergency changes and subsequent review
- A process for remediating unsuccessful changes

29. Describe in detail how the third-party contractor's services support NCDOT's **System and Communications Protection** policy, guidelines, and standards. Specifically speak to Policy ([SISM SC-1](#)), Application Partitioning ([SISM SC-2](#)), Information in Shared Resources ([SISM SC-4](#)), Denial of Service Protection ([SISM SC-5](#)), Boundary Protection ([SISM SC-7](#)), Transmission Confidentiality and Integrity ([SISM SC-8](#)), Network Disconnect ([SISM SC-10](#)), Cryptographic Key Establishment and Management ([SISM SC-12](#)), Cryptographic Protection ([SISM SC-13](#)), Public Key Infrastructure Certificates ([SISM SC-17](#)), and Mobile Code ([SISM SC-18](#)).

Purpose

To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information. This policy establishes requirements for the use and protection of cryptographic keys throughout their entire lifecycle.

Scope

All information systems developed and/or controlled by Spare which store or transmit confidential data.

Policy

Spare shall evaluate the risks inherent in the processing and storing data, and shall implement cryptographic controls to mitigate those risks where deemed appropriate. Where encryption is in use, strong cryptography with associated key management processes and procedures shall be implemented and documented. All encryption shall be performed in accordance with industry standards, including NIST SP 800-57.

For all personal data, Spare shall consider the state of the art, the costs of implementation and the nature, scope, context, and purposes of processing as well as the risk of varying likelihood and severity to the rights and freedoms of natural persons, and implement appropriate technical and organizational measures surrounding the pseudonymization and encryption of data to ensure a level of security appropriate to the risk.

For all web traffic sent over the public Internet containing confidential, the TLS v1.2 protocol or better must be utilized.

Key Management

Access to keys and secrets shall be tightly controlled in accordance with the Access Control Policy.

Exceptions

Requests for an exception to this policy must be submitted to the CTO for approval.

Violations & Enforcement

Any known violations of this policy should be reported to the CTO. Violations of this policy can result in immediate withdrawal or suspension of system and network privileges and/or disciplinary action in accordance with company procedures

	up to and including termination of employment.
30. Describe in detail how the third-party contractor's services support NCDOT's Identification & Authentication policy, guidelines, and standards. Specifically speak to Access Control (SISM AC-1), Account Management (SISM AC-2), Automated System Account Management (SISM AC-2(1)), Removal of Temporary / Emergency Accounts (SISM AC-2(2)), Disable Inactive Accounts (SISM AC-2(3)), Automated Audit Actions (SISM AC-2(4)), Access Enforcement (SISM AC-3), Information Flow Enforcement (SISM AC-4), Separation of Duties (SISM AC-5), Least Privilege (SISM AC-6), Unsuccessful Logon Attempts (SISM AC-7), System Use Notification (SISM AC-8), Session Lock (SISM AC-11), Pattern-Hiding Displays (SISM AC-11(1)), Session Termination (SISM AC-12), Remote Access (SISM AC-17), Remote Access Automated Monitoring / Control (SISM AC-17(1)), Remote Access – Protection of Confidentiality / Integrity Using Encryption (SISM AC-17(2)), Remote Access – Managed Access Control Points (SISM AC 17(3)), Remote Access – Privileged Commands / Access (SISM AC-17(4)), Access Control for Mobile Devices (SISM AC-19), Access Control for Mobile Devices – Full Device / Container- Based Encryption (SISM AC-19(5)), Use of External Information Systems (SISM AC-20), Use of External Information Systems – Limits on Authorized Use (SISM AC 20(1)), Information Sharing (SISM AC-21), and Publicly Accessible Content (SISM AC-22).	Given NCDOT's stringent authentication requirements, Spare proposes to integrate with NCDOT's NCID authentication system via SAML. Once a user is authenticated, roles based permissions apply. No remote access is provided to any customer users and only Spare employees have access to underlying systems. The following roles, with the following user permissions, are available: • Administrator: Administrators have full view and write access to the entire suite of Spare Launch features, including, but not limited to: creating and editing services, setting and editing duties, creating and editing vehicles, creating and modifying requests, creating and modifying users, changing user permissions, as well as access to Spare Analyze and Realize (if applicable). • Operations Manager: An Operation Manager looks after day to day operations. Their access is similar to the Administrator, but they are not able to create/edit services and financial aspects of the platform (Promos, Passes, Refunds, Payment Methods, etc.). • Booking Agent: Booking agents only have write access to the User and Request menus, allowing them to create and edit non-administrator users as well as to create, edit, and delete trip requests. They can also view the Live Map, services, stops, favorite locations, reviews, and charges. • Scheduler: Schedulers have the same permissions as booking agents, but can also create, edit, and delete driver duties and vehicles. • Service Planner: Service Planners create the Service within the platform. They have access to create and edit Services and their dependent resources (Fleets, Zones, Stops, TimeRules). They can also create Groups and Rider Notifications. • Finance Manager: The Finance Manager has access to create and edit the Financial aspects of the platform. Those

	include promotions, refunds, and service revenue. • Access to Reporting: Allows for the creation of reports from Spare Analyze. • Access to Analytics: Allows the user to view the real-time analytics in Spare Analyze. Access Control Policy Effective Date: April 4, 2023 Purpose To limit access to information and information processing systems, networks, and facilities to authorized parties in accordance with business objectives. Scope All Spare information systems that process, store, or transmit **confidential** data as defined in the [Data Management Policy]. This policy applies to all employees of Spare and to all external parties with access to Spare engineering networks and system resources. Policy Access to information computing resources is limited to personnel with a business requirement for such access. Access rights shall be granted or revoked in accordance with this Access Control Policy. Business Requirements of Access Control Access Control Policy Spare shall determine the type and level of access granted to individual users based on the “principle of least privilege.” This principle states that users are only granted the level of access absolutely required to perform their job functions, and is dictated by Spare’s business and security requirements. Permissions and access rights not expressly granted shall be, by default, prohibited. Spare’s primary method of assigning and maintaining consistent access controls and access rights shall be through the implementation of Role-Based Access Control

(RBAC). Wherever feasible, rights and restrictions shall be allocated to groups. Individual user accounts may be granted additional permissions as needed with approval from the system owner or authorized party.

All privileged access to production systems should use Multi-Factor Authentication (MFA).

Access to Networks and Network Services

The following security standards shall govern access to Spare networks and network services:

- Only authorized Spare employees and third-parties working off a signed contract or statement of work, with a business need, shall be granted access to the Spare production networks
- Spare guests may be granted access to guest networks after registering with office staff without a documented request
- Remote connections to production systems and networks must be encrypted

User Access Management

Spare requires that all personnel have a unique user identifier for system access, and that user credentials and passwords are not shared between multiple personnel. Users with multiple levels of access (e.g. administrators) should be given separate accounts for normal system use and for administrative functions wherever feasible. Root, service, and administrator accounts may use a password management system to share passwords for business continuity purposes only. Administrators shall only use shared administrative accounts as needed.

User Registration and Deregistration

Only authorized administrators shall be permitted to create new user IDs, and may only do so upon receipt of a documented request from authorized parties. User provisioning requests must include approval from data owners or Spare management authorized to grant system access. Prior to account creation, administrators should verify that the account does not violate any Spare security or system access control policies such as segregation of duties, fraud prevention measures, or access

rights restrictions.

User IDs shall be promptly disabled or removed when users leave the organization or contract work ends. User IDs shall not be re-used.

These requirements apply for all systems that connect to our production environment and contain any customer data.

User Access Provisioning

- New employees and/or contractors are not to be granted access to any Spare production systems containing customer data until after they have completed all HR onboarding tasks, which may include but is not limited to signed employment agreement, intellectual property agreement, and information security policy
- Access should be restricted to only what is necessary to perform job duties
- No access may be granted earlier than the official employee start date
- Access requests shall be documented. No permissions shall be granted without approval from the system or data owner or management

Management of Privileged Access

Granting of administrative rights shall be strictly controlled, and requires approval from the asset owner.

User Access Reviews

Administrators shall perform access rights reviews of user, administrator, and service accounts on a quarterly basis to verify that user access is limited to systems that are required for their job function. Access reviews shall be documented according to with our System Access Review Procedure.

Access reviews may include group membership as well as evaluations of any specific or exception-based permission. Access rights shall also be reviewed as part of any job role change, including promotion, demotion, or transfer within the company.

Removal & Adjustment of Access Rights

The access rights of all users shall be promptly removed upon termination of their employment

or contract, or when rights are no longer needed due to a change in job function or role. The maximum allowable time period for access termination is 24 business hours.

Access Provisioning, Deprovisioning, and Change Procedure

The Access Management Procedure for Spare systems and tools can be found in Notion at [Tooling Access Procedures].

User Responsibility for the Management of Secret Authentication Information

Control and management of individual user passwords is the responsibility of all Spare personnel and third-party users. Users shall protect secret authentication information in accordance with the Information Security Policy.

Password Policy

All Spare employees are required to use company-provided **1Password** for managing passwords for all their application/system accounts.

All hardware computer passwords should be complex and be 8 minimum characters in length and contain minimum 1 symbol. This is enforced by our MDM software, JAMF.

For applications/systems, passwords created should be strong and contain 20 characters and above whenever possible. Since we are using 1Password, it is easy to do this everywhere. Passwords should never be re-used between systems.

All authentication to Data Center access or to systems that manage our data center should be done through Google SSO with 2FA.

System and Application Access

Information Access Restriction

Applications must restrict access to program functions and information to authorized users and support personnel in accordance with the defined access control policy. The level and type of restrictions applied by each application should be based on the individual application

requirements, as identified by the data owner. The application-specific access control policy must also conform to Spare policies regarding access controls and data management.

Prior to implementation, evaluation criteria are to be applied to application software to determine the necessary access controls and data policies. Assessment criteria include, but are not limited to:

- Sensitivity and classification of data.
- Risk to the organization of unauthorized access or disclosure of data
- The ability to, and granularity of, control(s) on user access rights to the application and data stored within the application
- Restrictions on data outputs, including filtering sensitive information, controlling output, and restricting information access to authorized personnel
- Controls over access rights between the evaluated application and other applications and systems
- Programmatic restrictions on user access to application functions and privileged instructions
- Logging and auditing functionality for system functions and information access
- Data retention and aging features

All unnecessary default accounts must be removed or disabled before making a system available on the network. Specifically, vendor default passwords and credentials must be changed on all Spare systems, devices, and infrastructure prior to deployment. This applies to ALL default passwords, including but not limited to those used by operating systems, software that provides security services, application and system accounts.

Secure Log-on Procedures

Secure log-on controls shall be designed and selected in accordance with the sensitivity of data and the risk of unauthorized access based on the totality of the security and access control architecture.

Password Management System

Systems for managing passwords should be interactive and assist Spare personnel in maintaining password standards by enforcing

	password strength criteria including minimum length, and password complexity where feasible. All storage and transmission of passwords is to be protected using appropriate cryptographic protections, either through hashing or encryption. Use of Privileged Utility Programs Use of utility programs, system files, or other software that might be capable of overriding system and application controls or altering system configurations must be restricted to the minimum personnel required. Systems are to maintain logs of all use of system utilities or alteration of system configurations. Extraneous system utilities or other privileged programs are to be removed or disabled as part of the system build and configuration process. Management approval is required prior to the installation or use of any ad hoc or third-party system utilities. Access to Program Source Code Access to program source code and associated items, including designs, specifications, verification plans, and validation plans shall be strictly controlled in order to prevent the introduction of unauthorized functionality into software, avoid unintentional changes, and protect Spare intellectual property. All access to source code shall be based on business needs and must be logged for review and audit. Exceptions Requests for an exception to this Policy must be submitted to the CTO (IT Manager) for approval. Violations & Enforcement Any known violations of this policy should be reported to the CTO (IT Manager). Violations of this policy can result in immediate withdrawal or suspension of the system and network privileges and/or disciplinary action in accordance with company procedures up to and including termination of employment.

31. Describe in detail how the third-party's services support NCDOT's Media Protection policy, guidelines, and standards. Specifically speak to Policy (SISM MP-1), Media Access (SISM MP-2), Media Marking (SISM MP-3), Media Storage (SISM MP-4), Media Transport (SISM MP-5), Media Sanitization (SISM MP-6), Media Use (SISM MP-7), and Media Use – Prohibit Use Without Owner (SISM MP-7(1)).	Spare does not collect or store personal media.
32. Describe in detail how the third-party contractor's services support NCDOT's Personnel Security policy, guidelines, and standards. Specifically speak to Policy (SISM PS-1), Position Risk Designation (SISM PS-2), Personnel Screening (SISM PS-3), Personnel Termination (SISM PS-4), Personnel Transfer (SISM PS-5), Access Agreements (SISM PS-6), and Third Party Personnel Security (SISM PS-7).	Spare follows standard background check and screening process for all employees. More specific background check and personnel policy will adopted should NCDOT choose Spare as a partner.
33. Describe in detail how the third-party contractor's services support NCDOT's Risk Assessment policy, guidelines, and standards. Specifically speak to Policy (SISM RA-1), Security Categorization (SISM RA-2), Risk Assessment (SISM RA-3), Vulnerability Scanning (SISM RA-5), Vulnerability Scanning – Update Tool Capability (SISM RA-5(1)), Vulnerability Scanning – Frequency of Updates (SISM RA-5(2)), and Vulnerability Scanning – Privileged Access (SISM RA-5(5)).	Effective Date: April 4, 2023 Purpose To define the methodology for assessing and managing Spare's information security risks in order to achieve the company's business and information security objectives. Scope The risk assessment process may be applied to all business processes, information, information systems, networks, devices, and information processing facilities that are owned or used by Spare applicants, employees, contractors, consultants, vendors, partners, and other users affiliated with Spare, or others using or accessing Spare networks and/or information systems. Policy Spare will ensure that risk management plays an integral part in the governance and management of the organization at a strategic and operational level. The purpose of a risk management policy is designed to ensure that the company achieves its stated business and security goals and objectives.

Risk Management Strategy

Spare has developed processes to identify those risks that would hinder the achievement of its strategic and operational objectives. Spare will therefore ensure that it has in place the means to identify, analyze, control, and monitor the strategic and operational risks it faces using this risk management policy based on best practices.

The CTO will ensure the risk management strategy and policy are reviewed regularly and that:

- The risk management policy is applied to relevant areas at Spare
- The risk management policy and its operational application are annually reviewed
- Non-compliance is reported to appropriate company officers and authorities

Practical Application of Risk Management

Spare may use a variety of risk reporting formats for the identification of risks, their classification, and evaluation based on factors such as vendors utilized, methodology employed, and the scope of the assessment. In general, and where possible, risks shall be assessed and ranked according to their impact and their likelihood of occurrence.

In addition, an internal audit of the information security management system (ISMS) (i.e., information security controls and management processes) shall be performed at least annually.

Security risks shall be evaluated at various stages of the software design and development lifecycle as needed.

Risk Categories

Some risks are within the control of Spare while others may be only to a lesser degree. Spare will consider the risks within each of

	the following categories: • Technical • Reputational • Contractual • Economic/Financial • Regulatory/Compliance • Fraud Each identified risk will be assessed as to its likelihood and impact. Likelihood can be assessed as not likely, somewhat likely, or very likely. Impact can be assessed as not impactful, somewhat impactful, and very impactful. The likelihood and impact will be considered together to formulate an overall risk ranking. Risk Criteria The criteria for determining risk is the combined likelihood and impact of an event adversely affecting the confidentiality, availability, integrity, or privacy of customer data, personally identifiable information (PII), or business critical systems. For all risk inputs such as risk assessments, penetration tests, vulnerability scans, etc., Spare management shall reserve the right to modify automated or third-party provided risk rankings based on its assessment of the nature and criticality of the system processing, as well as the nature, criticality and exploitability (or other relevant factors and considerations) of the identified vulnerability. Risk Response and Treatment Risks will be prioritized and mapped using the approach contained in this policy. The following responses to risk should be employed. Where Spare chooses a risk response other than “Accept,” it shall develop a Risk Treatment Plan. • Mitigate: Spare may take actions or employ strategies to reduce the risk. • Accept: Spare may decide to accept and monitor the risk at the present time. This may be necessary for some risks that arise from external

	events. • Transfer: Spare may decide to pass the risk on to another party. For example, contractual terms may be agreed to ensure that the risk is not borne by Spare, or insurance may be appropriate for protection against financial loss. • Eliminate: The risk may be such that Spare could decide to cease the activity or to change it in such a way as to end the risk. Risk Management Procedure The procedure for managing risk will meet the following criteria: • Spare will maintain a Risk Register and Treatment Plan. • Risks shall be ranked by 'likelihood' and 'severity/impact' as critical, high, medium, low, or negligible. • Overall risk shall be determined through a combination of likelihood and impact. • Risks may be valued to estimate potential monetary loss where practical, or may be considered relative to a control objective • Spare will respond to risks in a prioritized fashion. Remediation priority will consider the risk likelihood and impact, cost, work effort, and availability of resources. Multiple remediations may be undertaken simultaneously. • Periodic reports will be made to the senior leadership of Spare to ensure risks are being mitigated appropriately, and in accordance with business priorities and objectives. Risk Acceptance Levels Amendment & Termination of this Policy Spare reserves the right to modify, amend or terminate this policy at any time.

	Exceptions Requests for an exception to this Policy must be submitted to the CTO for approval. Violations & Enforcement Any known violations of this policy should be reported to the CTO. Violations of this policy can result in immediate withdrawal or suspension of system and network privileges and/or disciplinary action in accordance with company procedures up to and including termination of employment.
34. Describe in detail how the third-party contractor's services support NCDOT's Physical & Environmental Protection policy, guidelines, and standards. Specifically speak to Policy (SISM PE-1), Physical Access Authorizations (SISM PE-2), Physical Access Control (SISM PE-3), Access Control for Transmission Medium (SISM PE-4), Access Control for Output Devices (SISM PE-5), Monitoring Physical Access (SISM PE 6), Monitoring Physical Access – Intrusion Alarms (SISM PE 6(1)), Visitor Access Records (SISM PE-8), Power Equipment and Cabling (SISM PE-9), Emergency Power (SISM PE-11), Fire Protection (SISM PE-13), Fire Protection – Automatic Fire Suppression (SISM PE-13(3)), Delivery and Removal (SISM PE-16), Alternate Work Site (SISM PE-17), and Location of Information System Components (SISM PE-18).	Effective Date: April 4, 2023 Purpose To prevent unauthorized physical access or damage to the organization's information and information processing facilities. Scope All Spare offices and locations. This Policy applies to all employees of Spare, and to all external parties with physical access to Spare-owned or leased facilities. Policy Physical Security Perimeter Physical offices and processing facilities shall meet all local building codes for construction materials for walls, windows, doors, and access control mechanisms. Some interior zones may be identified as secure areas where physical access is further restricted to a subset of Spare personnel; such as private offices, wiring closets, print and server rooms, and server racks. Physical Entry Controls

Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access. Where possible, Spare access control systems shall be tied to a centralized system that provides granular access control for individual personnel. Access events shall be appropriately logged and reviewed as needed according to risk. Cameras and intrusion detection systems shall be used at facilities that store or process production data.

Securing Offices, Rooms & Facilities

Physical security for offices, rooms and facilities shall be designed and applied to protect from theft, misuse, environmental threats, unauthorized access, and other threats to the confidentiality, integrity, and availability of classified data and systems.

Protecting Against External & Environmental Threats

Physical protection against natural disasters, malicious attack or accidents shall be designed and applied. Secure areas shall be monitored through the use of intrusion detection systems, alarms, and/or video surveillance systems where feasible. Visitor and third-party access to secure areas shall be restricted to reduce the risk of information loss and theft.

Production processing facilities shall be equipped with appropriate environmental and business continuity controls including fire-suppression systems, climate control and monitoring systems, and emergency backup power systems. Physical information system hardware and supporting infrastructure shall be regularly serviced and maintained in accordance with the manufacturer's recommendations.

Working in Secure Areas / Visitor Management

Visitors, delivery personnel, outside support technicians, and other external agents shall

not be permitted access to secure areas without escort and/or appropriate oversight. Third-parties in secure areas shall sign in and out on a visitor log and shall be escorted or monitored by Spare personnel. Spare personnel observing unescorted visitors should approach the visitor, confirm their status, and ensure they return to approved areas or report the observation to the responsible authority as needed. External party access to secure areas shall be confirmed with appropriate Spare personnel prior to being granted access. Spare personnel providing access to external parties into secure areas are responsible for ensuring that the third-party personnel adhere to all security requirements, and are accountable for all actions taken by outsiders they provide with access. Visitors may be allowed to work unescorted provided that the Spare sponsoring party can ensure that they will not have unauthorized access to Spare information systems, networks, or data.

Delivery & Loading Areas

Access points such as delivery and loading areas and other points where unauthorized persons could enter secure areas shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.

Supplier, Vendor, and Third-Party Security

Suppliers, vendors, and third parties shall comply with Spare physical security and environmental controls requirements. Spare shall assess the adequacy of third-party physical security controls as part of the vendor management process, in accordance with the Third-Party Management Policy.

Exceptions

Requests for an exception to this policy must be submitted to the People Lead for approval.

	Violations & Enforcement Any known violations of this policy should be reported to the People Lead. Violations of this policy can result in immediate withdrawal or suspension of system and network privileges and/or disciplinary action in accordance with company procedures up to and including termination of employment.
35. When Critical or High software vulnerability are identified and patching is not an option, what Continuous Monitoring activities does the third-party perform to maintain visibility and identify if the known vulnerabilities been exploited? i. How does the third-party contractor track known vulnerabilities that cannot be remediated? ii. Submit a Corrective Actions Plan (CAP) that identifies all third-party contractor vulnerabilities and security controls that do not comply with or meet the intent of the security requirements established in the State of North Carolina Statewide Information Security Manual (SISM). The CAP template can be found here: https://it.nc.gov/documents/files/corrective-action-plan-template-v1/open The CAP instructions can be found here: https://it.nc.gov/documents/files/corrective-action-plan-instructions/open	<i>Third-party provides a comprehensive response here. Please review and understand the SISM requirements before responding.</i> As a software-as-a-service business with robust security systems and protocols, we prioritize the timely patching of critical or high software vulnerabilities. However, in situations where patching is not immediately possible, we have comprehensive continuous monitoring activities in place to maintain visibility and identify if known vulnerabilities have been exploited. These activities include: Intrusion Detection and Prevention Systems (IDPS): We employ IDPS tools that continuously monitor network traffic and identify any suspicious or malicious activities that may indicate an exploitation attempt. These systems generate real-time alerts and logs, allowing us to quickly detect and respond to potential security breaches. Log Monitoring and Analysis: We have mechanisms to collect, analyze, and monitor system logs, including event logs, access logs, and audit trails. By actively monitoring these logs, we can identify any unusual or unauthorized activities that could signify an exploit or compromise. Security Information and Event Management (SIEM) System: Our SIEM system collects and correlates security events from various sources, providing us with a centralized view of

	potential security incidents. It helps us identify patterns, anomalies, and indicators of compromise related to known vulnerabilities. Vulnerability Scanning and Penetration Testing: We conduct regular vulnerability scanning and penetration testing exercises to proactively identify vulnerabilities and assess the effectiveness of our security controls. This includes identifying and confirming the presence of known vulnerabilities and their potential exploitation. Threat Intelligence Monitoring: We stay updated with the latest threat intelligence feeds and security advisories related to known vulnerabilities. This allows us to assess the risk landscape and respond promptly to emerging threats. Incident Response and Forensics: In the event of a suspected or confirmed exploitation, we have a well-defined incident response plan. This plan includes procedures to investigate, contain, mitigate, and recover from security incidents. It may involve forensic analysis to determine the extent of the exploitation and identify any compromised systems or data. By implementing these continuous monitoring activities, we maintain a strong visibility into our systems, promptly detect any attempts to exploit known vulnerabilities, and respond effectively to mitigate potential risks. Our dedicated security teams are vigilant in monitoring and responding to any security incidents, ensuring the integrity and security of the services we provide.

36. Policies, Procedures, and Training

The third-party contractor must indicate the status of their policies, standards, and procedures coverage.

To answer “**Yes**” to a policy, it must be fully developed, documented, and disseminated; and it must address purpose, scope, roles, responsibilities, management commitment, coordination among entities, and compliance. A single policy document may address more than one family provided the requirements of each

"1" are fully addressed.

Third-party contractors must establish their own set of policies, standards, and procedures. They cannot be inherited from a leveraged system or service provider. Any exceptions and/or missing policy and procedure elements must be explained in comments section.

Family	Policy		Standards		Procedures		Document Title, Version, and Last Review Date	Comments
	Yes	No	Yes	No	Yes	No		
Access Control [SISM AC-1]	Yes		Yes		Yes		Policy: Access Control Policy, reviewed April 2023 Standards: Included in policy Procedures: Included in policy	
Awareness & Training [SISM AT-1]	Yes		Yes		Yes		Policy: Information Security Policy, reviewed April 2023 Standards: Included in policy Procedures: Included in policy	
Audit & Accountability [SISM AU-1]	Yes		Yes		Yes		Policy: Code of Conduct Policy, reviewed April 2023 Standards: Included in policy Procedures: Included in policy	
Security Assessment & Authorization [SISM CA-1]	Yes		Yes		Yes		Policy: Human Resource Security Policy, reviewed April 2023 Standards: Included in policy Procedures: Included in policy	
Configuration Management [SISM CM-1]	Yes		Yes		Yes		Policy: Operations Resource Security Policy, reviewed April 2023 Standards: Included in policy Procedures: Included in policy	
Contingency Planning [SISM CP-1]	Yes		Yes		Yes		Policy: Operations Resource Security Policy, reviewed April 2023 Standards: Included in policy Procedures: Included in policy	
Identification & Authentication [SISM IA-1]	Yes		Yes		Yes		Policy: Information Security Policy, reviewed April 2023 Standards: Included in policy Procedures: Included in policy	

Incident Response [SISM IR-1]	Yes		Yes		Yes		Policy: Incident Response Policy, reviewed April 2023 Standards: Included in policy Procedures: Included in policy	
Maintenance [SISM MA-1]	Yes		Yes		Yes		Policy: Secure Development Policy, reviewed April 2023 Standards: Included in policy Procedures: Included in policy	
Media Protection [SISM MP-1]	Yes		Yes		Yes		Policy: Information Security Policy • version 4, April 4, 2023 Procedure(s): • version 4, April 4, 2023	
Physical & Environmental Protection [SISM PE-1]	Yes		Yes		Yes		Policy: Physical Security Policy, reviewed April 2023 Standards: Included in policy Procedures: Included in policy	
Personnel Security [SISM PS-1]	Yes		Yes		Yes		Policy: Human Resource Security Policy, reviewed April 2023 Standards: Included in policy Procedures: Included in policy	
Risk Assessment [SISM RA-1]	Yes		Yes		Yes		Policy: Risk Management Policy, reviewed April 2023 Standards: Included in policy Procedures: Included in policy	
System & Services Acquisition [SISM SA-1]	Yes		Yes		Yes		Policy: Third Party Management Policy, reviewed April 2023 Standards: Included in policy Procedures: Included in policy	
System & Communications Protection [SISM SC-1]	Yes		Yes		Yes		Policy: Information Security Policy, reviewed April 2023 Standards: Included in policy Procedures: Included in policy	
System & Information Integrity [SISM SI-1]	Yes		Yes		Yes		Policy: Information Security Policy, reviewed April 2023 Standards: Included in policy Procedures: Included in policy	

Planning [SISM PL-1]		No		No		No	Policy: N/A Standards: Procedures:	Policy has not been created yet but Spare commits to creating it if awarded contract for NCDOT



Access Control Policy

Policy Owner: 🧐 Alexey Indeev

Effective Date: April 4, 2023

Purpose

To limit access to information and information processing systems, networks, and facilities to authorized parties in accordance with business objectives.

Scope

All Spare information systems that process, store, or transmit **confidential** data as defined in the  Data Management Policy. This policy applies to all employees of Spare and to all external parties with access to Spare engineering networks and system resources. Our tools are currently categorized in Notion on this page:  Tools We Use

Policy

Access to information computing resources is limited to personnel with a business requirement for such access. Access rights shall be granted or revoked in accordance with this Access Control Policy.

Business Requirements of Access Control

Access Control Policy

Spare shall determine the type and level of access granted to individual users based on the “principle of least privilege.” This principle states that users are only granted the level of access absolutely required to perform their job functions, and is dictated by

Spare's business and security requirements. Permissions and access rights not expressly granted shall be, by default, prohibited.

Spare's primary method of assigning and maintaining consistent access controls and access rights shall be through the implementation of Role-Based Access Control (RBAC). Wherever feasible, rights and restrictions shall be allocated to groups. Individual user accounts may be granted additional permissions as needed with approval from the system owner or authorized party.

All privileged access to production systems should use Multi-Factor Authentication (MFA).

Access to Networks and Network Services

The following security standards shall govern access to Spare networks and network services:

- Only authorized Spare employees and third-parties working off a signed contract or statement of work, with a business need, shall be granted access to the Spare production networks
- Spare guests may be granted access to guest networks after registering with office staff without a documented request
- Remote connections to production systems and networks must be encrypted

User Access Management

Spare requires that all personnel have a unique user identifier for system access, and that user credentials and passwords are not shared between multiple personnel. Users with multiple levels of access (e.g. administrators) should be given separate accounts for normal system use and for administrative functions wherever feasible. Root, service, and administrator accounts may use a password management system to share passwords for business continuity purposes only. Administrators shall only use shared administrative accounts as needed.

User Registration and Deregistration

Only authorized administrators shall be permitted to create new user IDs, and may only do so upon receipt of a documented request from authorized parties. User provisioning

requests must include approval from data owners or Spare management authorized to grant system access. Prior to account creation, administrators should verify that the account does not violate any Spare security or system access control policies such as segregation of duties, fraud prevention measures, or access rights restrictions.

User IDs shall be promptly disabled or removed when users leave the organization or contract work ends. User IDs shall not be re-used.

These requirements apply for all systems that connect to our production environment and contain any customer data.

User Access Provisioning

- New employees and/or contractors are not to be granted access to any Spare production systems containing customer data until after they have completed all HR onboarding tasks, which may include but is not limited to signed employment agreement, intellectual property agreement, and information security policy
- Access should be restricted to only what is necessary to perform job duties
- No access may be granted earlier than the official employee start date
- Access requests shall be documented. No permissions shall be granted without approval from the system or data owner or management

Management of Privileged Access

Granting of administrative rights shall be strictly controlled, and requires approval from the asset owner.

User Access Reviews

Administrators shall perform access rights reviews of user, administrator, and service accounts on a quarterly basis to verify that user access is limited to systems that are required for their job function. **Access reviews shall be documented** according to with our 🧑 [System Access Review Procedure](#)

Access reviews may include group membership as well as evaluations of any specific or exception-based permission. Access rights shall also be reviewed as part of any job role change, including promotion, demotion, or transfer within the company.

Removal & Adjustment of Access Rights

The access rights of all users shall be promptly removed upon termination of their employment or contract, or when rights are no longer needed due to a change in job function or role. The maximum allowable time period for access termination is 24 business hours.

Access Provisioning, Deprovisioning, and Change Procedure

The Access Management Procedure for Spare systems and tools can be found in Notion at  [Tooling Access Procedures](#)

User Responsibility for the Management of Secret Authentication Information

Control and management of individual user passwords is the responsibility of all Spare personnel and third-party users. Users shall protect secret authentication information in accordance with the Information Security Policy.

Password Policy

All Spare employees are required to use company-provided **1Password** for managing passwords for all their application/system accounts.

All hardware computer passwords should be complex and be 8 minimum characters in length and contain minimum 1 symbol. This is enforced by our MDM software, JAMF.

For applications/systems, passwords created should be strong and contain 20 characters and above whenever possible. Since we are using 1Password, it is easy to do this everywhere. Passwords should never be re-used between systems.

All authentication to Data Center access or to systems that manage our data center should be done through Google SSO with 2FA.

System and Application Access

Information Access Restriction

Applications must restrict access to program functions and information to authorized users and support personnel in accordance with the defined access control policy. The level and type of restrictions applied by each application should be based on the individual application requirements, as identified by the data owner. The application-specific access control policy must also conform to Spare policies regarding access controls and data management.

Prior to implementation, evaluation criteria are to be applied to application software to determine the necessary access controls and data policies. Assessment criteria include, but are not limited to:

- Sensitivity and classification of data.
- Risk to the organization of unauthorized access or disclosure of data
- The ability to, and granularity of, control(s) on user access rights to the application and data stored within the application
- Restrictions on data outputs, including filtering sensitive information, controlling output, and restricting information access to authorized personnel
- Controls over access rights between the evaluated application and other applications and systems
- Programmatic restrictions on user access to application functions and privileged instructions
- Logging and auditing functionality for system functions and information access
- Data retention and aging features

All unnecessary default accounts must be removed or disabled before making a system available on the network. Specifically, vendor default passwords and credentials must be changed on all Spare systems, devices, and infrastructure prior to deployment. This applies to ALL default passwords, including but not limited to those used by operating systems, software that provides security services, application and system accounts.

Secure Log-on Procedures

Secure log-on controls shall be designed and selected in accordance with the sensitivity of data and the risk of unauthorized access based on the totality of the security and

access control architecture.

Password Management System

Systems for managing passwords should be interactive and assist Spare personnel in maintaining password standards by enforcing password strength criteria including minimum length, and password complexity where feasible.

All storage and transmission of passwords is to be protected using appropriate cryptographic protections, either through hashing or encryption.

Use of Privileged Utility Programs

Use of utility programs, system files, or other software that might be capable of overriding system and application controls or altering system configurations must be restricted to the minimum personnel required. Systems are to maintain logs of all use of system utilities or alteration of system configurations. Extraneous system utilities or other privileged programs are to be removed or disabled as part of the system build and configuration process.

Management approval is required prior to the installation or use of any ad hoc or third-party system utilities.

Access to Program Source Code

Access to program source code and associated items, including designs, specifications, verification plans, and validation plans shall be strictly controlled in order to prevent the introduction of unauthorized functionality into software, avoid unintentional changes, and protect Spare intellectual property.

All access to source code shall be based on business needs and must be logged for review and audit.

Exceptions

Requests for an exception to this Policy must be submitted to the CTO (IT Manager) for approval.

Violations & Enforcement

Any known violations of this policy should be reported to the CTO (IT Manager).
Violations of this policy can result in immediate withdrawal or suspension of the system and network privileges and/or disciplinary action in accordance with company procedures up to and including termination of employment.

Versions

 Version	 Description	 Date	 Author	 Approved by	 Attachment
<u>1</u>	First Version	@February 1, 2021	Alexey Indeev	Alexey Indeev	<u>Access_Control_Policy.pdf</u>
<u>2</u>	Minor updates	@March 22, 2022	Alexey Indeev	Alexey Indeev	<u>Access_Control_Policy.pdf</u>
<u>3</u>	Removed password rotation requirements	@January 4, 2023	Alexey Indeev	Alexey Indeev	
<u>4</u>	Renewed	@April 4, 2023	Alexey Indeev	Alexey Indeev	



Asset Management Policy

Policy Owner: 🧐 Alexey Indeev

Effective Date: April 4, 2023

Purpose

To identify organizational assets and define appropriate protection responsibilities. To ensure that information receives an appropriate level of protection in accordance with its importance to the organization. To prevent unauthorized disclosure, modification, removal, or destruction of information stored on media.

Scope

This policy applies to all Spare owned or managed information systems.

Policy

Inventory of Assets

Assets associated with information and information processing facilities that store, process, or transmit classified information shall be identified and an inventory of these assets shall be drawn up and maintained.

Ownership of Assets

Assets maintained in the inventory shall be owned by a specific individual or group within Spare.

Acceptable Use of Assets

Rules for the acceptable use of information, assets, and information processing facilities shall be identified and documented in the Information Security Policy.

Return of Assets

All employees and third-party users of Spare equipment shall return all of the organizational assets within their possession upon termination of their employment, contract, or agreement.

Handling of Assets

Employees and users who are issued or handle Spare equipment are expected to use reasonable judgment and exercise due care in protecting and maintaining the equipment.

Employees are responsible for ensuring that company equipment is secured and properly attended to whenever it is transported or stored outside of company facilities.

All mobile devices shall be handled in accordance with the Information Security Policy.

Exceptions

Requests for an exception to this policy must be submitted to the COO for approval.

Violations & Enforcement

Any known violations of this policy should be reported to the COO. Violations of this policy can result in immediate withdrawal or suspension of system and network privileges and/or disciplinary action in accordance with company procedures up to and including termination of employment.

Versions

 Version	 Description	 Date	 Author	 Approved by	 Attachment
<u>1</u>	First Version	@February 1, 2021	Alexey Indeev	Alexey Indeev	<u>Asset_Management_Policy.pdf</u>

Aa Version	Description	Date	Author	Approved by	Attachment
<u>2</u>	Minor updates	@March 22, 2022	Alexey Indeev	Alexey Indeev	
<u>3</u>	Renewed	@April 4, 2023	Alexey Indeev	Alexey Indeev	



Asset Management Policy HIPAA Addendum

Policy Owner: 🧑 Alexey Indeev

Effective Date: April 4, 2023

Purpose

This HIPAA policy addendum outlines Spare's approach to the management of company assets throughout their lifecycle to ensure confidentiality of ePHI within the company systems and networks. This addendum seeks to satisfy certain standards and requirements of HIPAA, the Privacy Rule and the Security Rule including Title 45, §§

- 164.308(a)(5)(ii)(A)
- 164.308(a)(5)(ii)(B)
- 164.308(a)(5)(ii)(C)
- 164.308(a)(5)(ii)(D)
- 164.310(b)
- 164.310(c)
- 164.310(d)(2)(i)
- 164.310(d)(2)(ii)
- 164.310(d)(2)(iii)
- 164.310(d)(2)(iv)
- 164.312(a)(2) of the Code of Federal Regulations ("CFR").

Definitions

Capitalized terms used in this document and not otherwise defined herein shall have the meanings set forth in the Privacy Rule and the Security Rule which definitions are incorporated in this document by reference. Protected Health Information (PHI) and electronic Protected Health Information (ePHI) when referred to in this document is defined in 45 CFR § 160.103.

Automatic Access Lock Mechanisms

All portable devices and workstations that can retrieve, modify, store or use ePHI must be locked using an automatic screen lock and unique password or pin that makes the device inaccessible by any other individual when unattended by the owner. Portable devices must have a maximum limit on sign in attempts and the password or PIN number must be consistent with requirements as stated in Spare's Password Policy. Portable devices that can retrieve, modify, store or use ePHI must have antivirus and/or malware protection monitoring installed, consistent with the Spare's Asset Management Policy. Physical protection for portable devices must be provided consistent with Spare's Asset Management Policy. If a portable device is misplaced, stolen or believed to be compromised this must be immediately reported to the HIPAA Security Officer. To protect the confidentiality and integrity of portable devices and to prevent ePHI data breaches in the event of portable device loss, Spare will employ secure communication mechanisms to remote lock or erase lost or misplaced devices.

Authorization for Use of Portable Devices

Portable Devices and Workstations, which includes smartphones, laptop computers, portable hard drives, portable USB drives, and tablets or other devices that are capable of storing, receiving, processing, or transmitting electronic Protected Health Information (ePHI), must be authorized prior to use or interaction with ePHI in accordance with the wider company asset management policy. This applies to personally owned devices as well as devices that are owned or leased by Spare to the workforce. Devices which cannot be or have not been configured to comply with Spare's Asset Management Policy or this addendum, are prohibited from use on the Spare network and from accessing ePHI on company systems. Authorization for use of Portable Device is the responsibility of the IT Department. Authorization can be revoked in a manner consistent with the Spare's Asset Management Policy or when deemed necessary by the HIPAA Security Officer. Portable device authorization for ePHI access is automatically revoked upon the termination of employee or contractor from Spare's workforce. The HIPAA Security Officer is responsible for periodic review of authorized devices and must conduct this review when alerted to a change in employee or contractor role. Violation of this addendum or any other company policy will result in immediate de-authorization of asset use.

Audits of Portable Devices

Any portable device may be subject to audit to ensure compliance with this and other Spare policies. This includes personally owned devices as well as devices owned or leased and provided by Spare.

Portable Device Owner Responsibilities

Portable device users/owners must ensure that ePHI, when stored on the portable device, is encrypted in a manner consistent with requirements for confidential data in Spare's Data Classification Policy. ePHI should not be stored on the portable device for any period longer than necessary for the purpose for which it is stored.

Shared Use of Portable Devices

Shared use of a portable device is only permitted when ePHI is encrypted and the configuration of the device has not been changed to render the device out of compliance with Spare's Asset Management Policy. When sharing a device, the responsibility of the device transfers to the individual who is now temporarily using the shared device. That individual must take every step to protect the device from being stolen, lost, misplaced, accessed without authorization, or information from the device being disclosed. Any such incidents must be immediately reported to the authorized owner of the device. The individual using the shared device must ensure to return it promptly to the owner when the purpose of temporary use is complete.

Asset Disposal and Recycling

Spare requires that prior to disposal or recycling of hardware or media that contains or previously contained ePHI that either the data will be securely overwritten, or the device and/or media be physically destroyed. Where the media or device will be reused, all information must be properly sanitized before it is transferred from the current owner. In order to protect ePHI confidentiality, the sanitization method used must ensure that ePHI on the media is irretrievably destroyed. Sanitization should be done by the HIPAA Security Officer or appointed designee before equipment is reused or finally disposed of. The methods of destruction and reuse should be reassessed periodically and methods for destruction or reuse selected to ensure thorough destruction of ePHI. The HIPAA Security Officer shall maintain documentation of all ePHI media sanitization and data destruction that lists the device, the date of destruction, the workforce personnel authorizing the destruction, general description of the ePHI or other sensitive information (if available), and the identity of the workforce personnel performing the destruction.

Our current disposal and recycling procedure can be found here:  [Asset Disposal and Recycling Procedure \(Wiping Computers\)](#)

Violations

The use of a portable device without authorization, while authorization is suspended, or after authorization has been terminated is a violation of this Policy. Any employee or contractor found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. Violation may also result in civil and criminal penalties to Spare as determined by federal and state laws and regulations related to loss of data. Any known violations of this policy should be reported to the HIPAA Security Officer.

Responsibility

The HIPAA Security Officer will be responsible for ensuring this policy is followed.

Versions

Aa Version	Description	Date	Author	Approved by	Attachment
<u>1</u>	First Version	@February 1, 2021	Alexey Indeev	Alexey Indeev	<u>Access_Control_Policy_HIPAA_Addendum.pdf</u>
<u>2</u>	No updates	@March 22, 2022	Alexey Indeev	Alexey Indeev	
<u>3</u>	Renewed	@April 4, 2023	Alexey Indeev	Alexey Indeev	



Backup Policy HIPAA Addendum

Policy Owner: 🧑 Alexey Indeev

Effective Date: April 4, 2023

Purpose

This HIPAA policy addendum outlines Spare's approach and plans for data backup and recovery to ensure the integrity and availability of ePHI on company systems and networks. The addendum seeks to satisfy certain standards and requirements of HIPAA, the Privacy Rule and the Security Rule, including, Title 45, §§

- 164.308(a)(7)(ii)(A) of the Code of Federal Regulations ("CFR").

Definitions

Capitalized terms used in this document and not otherwise defined herein shall have the meanings set forth in the Privacy Rule and the Security Rule, which definitions are incorporated in this document by reference. Protected Health Information (PHI) and electronic Protected Health Information (ePHI) when referred to in this document is defined in 45 CFR § 160.103.

ePHI Data Backup

Spare makes a commitment to backup and securely store all ePHI on its information systems and electronic media. The HIPAA Security Officer or nominated designee is responsible for ensuring effective training of the workforce members assigned to complete backups, for management of the backup media and for performing periodic testing of restored media. Stored data must be accessible and retrievable at all times and all data backups should be tested and data restored to ensure accuracy. Documentation of backup testing, or restore logs, should be maintained by the HIPAA Security Officer. Proper management of situations concerning data back-up/data recovery, such as emergencies or other occurrences are addressed in the Spare's Disaster Recovery Plan.

ePHI Data Integrity

The HIPAA Security Officer is responsible for implementation of the integrity controls to ensure integrity of ePHI data backups and for review and updating them as necessary. The HIPAA Security Official will ensure that actual and potential damage to the integrity of ePHI information is appropriately addressed.

Violations

Failure to backup a system in the absence of a system failure is a violation of this policy and may result in corrective disciplinary action, up to and including termination of employment. Violation may also result in civil and criminal penalties to Spare as determined by federal and state laws and regulations related to loss of data. Violation may also result in liability to Spare related to loss of data. Any known violations of this policy should be reported to the HIPAA Security Officer.

Responsibility

The HIPAA Security Officer will be responsible for implementing this policy and will ensure that further responsibility is assigned for the proper management of data. All documentation required by this policy addendum will be maintained for a period of six years from the date of creation or the date when it was last in effect, whichever is later.

Versions

 Version	 Description	 Date	 Author	 Approved by	 Attachment
<u>1</u>	First Version	@February 1, 2021	Alexey Indeev	Alexey Indeev	<u>Data_Management_Backup_Policy_HIPAA_Addendum.pdf</u>
<u>2</u>	No changes	@March 22, 2022	Alexey Indeev	Alexey Indeev	
<u>3</u>	Renewed	@April 4, 2023	Alexey Indeev	Alexey Indeev	



Business Continuity and Disaster Recovery Plan

Policy Owner: 🧑 Alexey Indeev

Effective Date: April 4, 2023

Purpose

The purpose of this business continuity plan is to prepare Spare in the event of extended service outages caused by factors beyond our control (e.g., natural disasters, man-made events), and to restore services to the widest extent possible in a minimum time frame. In case of a remote first company like Spare, it is sufficient to have simple contingency plans in the form of service-level agreements with companies that host our data and services.

Scope

All Spare production systems that are business critical. This policy applies to all employees of Spare and to all relevant external parties.

The following scenarios are excluded from the BC/DR plan scope:

- Loss of availability for a production hosting service providers (i.e., Google Cloud Platform, Aiven)
- Loss of availability of any Spare offices (these will be considered incidents)

In the event of a loss of availability of a hosting service provider, the primary engineering incident responders will confer with the customer success staff and executive staff to determine an appropriate response strategy.

Policy

In the event of a major disruption to production services, senior managers and executive staff shall determine mitigation actions.

A disaster recovery test, including a test of backup restoration processes, shall be performed on an annual basis.

Continuity of information security shall be considered along with operational continuity.

In the case of an information security event or incident, refer to the Incident Response Plan.

Communications and Escalation

Executive staff and senior managers should be notified of any disaster affecting Spare operations.

Communications shall take place over any available regular channels including Slack, email and Zoom.

Key contacts can be found here: 🖐️ [The Team](#)

Roles and Responsibilities

Aa Role	☰ Responsibility
Departmental Heads	Each department head shall be responsible for communications with their departmental staff and any actions needed to maintain continuity of their business functions.
Managers	Managers shall be responsible for communicating with their direct reports and providing any needed assistance for staff to continue performing their responsibilities.
Customer Success Manager	Customer Success Manager, in conjunction with the COO shall be responsible for any external and client communications regarding any disaster or business continuity actions that are relevant to customers and third parties.
CTO	The CTO, in conjunction with the Customer Success Manager, shall be responsible for leading efforts to maintain continuity of Spare services to customers during a disaster.
People Lead	People Lead shall be responsible for internal communications to employees as well as any action needed to maintain physical health and safety of the workforce.

Continuity of Critical Services

Strategy for maintaining continuity of services can be seen in the following table:

Aa KEY BUSINESS PROCESS	☰ CONTINUITY STRATEGY
Customer (Production) Service Delivery	Rely on GCP and Aiven availability commitments and SLAs
IT Operations	All systems are vendor-hosted SaaS applications.
Email	Utilize Gmail and its distributed nature, rely on Google's standard service level agreements.
Finance, Legal and HR	All systems are vendor-hosted SaaS applications.
Sales and Marketing	All systems are vendor-hosted SaaS applications.

Plan Activation

For a business continuity plan to be effective, it needs to be triggered as soon as possible; too early or late can reduce its efficacy. Key decision points to consider when a BCP has to be triggered or invoked are given below:

- When an incident turns into an event like a disaster, breach

- When the estimated time of resolution for a potential breach is greater than the normal estimated time for regular security incidents
- When the recovery of an incident is uncertain, a decision must be made to invoke the business continuity plan if the disruption cannot be resolved within the specified incident recovery timelines

Versions

 Version	 Description	 Date	 Author	 Approved by	 Attachment
<u>1</u>	First Version	@February 1, 2021	Alexey Indeev	Alexey Indeev	<u>Business Continuity and Disaster Recovery Plan.pdf</u>
<u>2</u>	No changes	@March 22, 2022	Alexey Indeev	Alexey Indeev	
<u>3</u>	Renewed	@April 4, 2023	Alexey Indeev	Alexey Indeev	



Code of Conduct

Policy Owner: 🧑‍💻 Mijay Pavon

Last Reviewed Date: April 4, 2023

Purpose

The goal of Spare's Code of Conduct is to provide a safe and inclusive work environment in which every Spare staff member is treated with respect and dignity. Spare are committed to maintaining a work environment that is free from all forms of discrimination, harassment, and bullying.

This Code of Conduct outlines our expectations for all Spare staff, steps to report violations, and consequences for unacceptable behaviour.

Scope

The Code of Conduct applies to all Spare staff. This includes full-time, part-time and contractor staff employed at every seniority level. The Code of Conduct is to be upheld during all work functions and events, including but not limited to business hours at the Spare office, during Spare-related extracurricular activities and events, while attending conferences and other professional events on behalf of Spare, and while working remotely and communicating on Spare resources with other staff.

We expect all Spare staff to abide by this Code of Conduct in all business matters -- online and in-person -- as well as in all one-on-one communications with other staff members, customers, and vendors pertaining to Spare business.

As an employee or contractor of Spare, in any country and any office, you have the right to a safe and inclusive work environment. You are responsible for complying with the regulatory standards of your country of work, including reporting unsafe work.

This Code of Conduct also applies to unacceptable behaviour occurring outside the scope of business activities when such behaviour has the potential to adversely affect

the safety and well-being of Spare staff and customers.

Definitions

Discrimination: has a wide meaning, and usually includes the following elements:

- not individually assessing the unique merits, capacities and circumstances of a person
- instead, making stereotypical assumptions based on a person's presumed traits (including based on a prohibited ground of discrimination)
- having the impact of excluding persons, denying benefits or imposing burdens.

Prohibited Grounds of Discrimination means any characteristic protected by applicable law. The prohibited grounds of discrimination are detailed in human rights legislation and include, but are not limited to: age, race/colour, ancestry, disability, religion or creed, place of or ethnic origin, marital status, sexual orientation, family status, gender identity, gender expression, and sex.

Workplace Bullying: means inappropriate conduct or comments by a person towards a worker that the person knew or reasonably ought to have known would cause that worker to be humiliated or intimidated. Bullying may include, but is not limited to, verbal aggression or insults, calling someone derogatory names, harmful hazing or initiation practices, vandalizing personal belongings and spreading malicious rumours.

Workplace Harassment: is engaging in vexatious comments or conduct against a worker in a workplace that might be known or ought reasonably to be known to be unwelcome, including workplace sexual harassment. Harassment may take many forms, including but not limited to the following:

- unwelcome remarks, jokes, innuendos or taunting;
- electronic or hard copy display of posters or literature that could be offensive to others;
- offensive electronic material including messages or content on email, websites, social media, and/or online chat;
- verbal abuse;
- refusal to work or converse with a person;

- imitation of a person's accent or mannerisms; and
- mocking a person's appearance or abilities.

Note: Reasonable action taken by Spare management or a manager relating to the management and direction of Spare staff is not workplace bullying or workplace harassment, unless such actions are carried out in an abusive or threatening manner. This is the case even if there are sometimes unpleasant consequences for Spare staff. Similarly, interpersonal conflict is not workplace bullying or workplace harassment unless it is threatening or abusive.

Sexual Harassment: is defined as (a) engaging in vexatious comments or conduct against a worker in a workplace because of sex, sexual orientation, gender identity or gender expression, where the comments or conduct is known or ought reasonably to be known to be unwelcome, or (b) making a sexual solicitation or advance where the person making the solicitation or advance is in a position to confer, grant or deny a benefit or advancement to the worker and the person knows or ought reasonably to know that the solicitation or advance is unwelcome. Types of behaviour that constitute sexual harassment include, but may not be limited to:

- sexist remarks or jokes;
- unwelcome comments or inquiries about a person's sex life;
- unwelcome flirtations, advances, propositions, leering;
- persistent unwelcome social invitations;
- requests for sexual favours; and
- unwanted physical contact.

Staff Responsibilities

A supplemental goal of this Code of Conduct is to encouraging Spare staff to recognize the relationships between our actions and their effects within Spare culture.

As a Spare staff member, you have a responsibility to maintain a safe and inclusive workplace that is free from all forms of discrimination, harassment, and bullying. It is your responsibility to ensure you are following the guidelines set out in this policy and to reach out to the People team if you are unclear on any aspects of this policy.

Staff members who believe that they are being subject to discrimination, workplace harassment, or workplace bullying, or who witness incidents of discrimination, workplace harassment or workplace bullying, are asked to immediately inform their manager, or if they do not feel comfortable informing their manager, then to inform the People team, in accordance with this Code of Conduct.

If someone's interactions with you make you uncomfortable, inform them. If you don't feel safe informing them yourself, ask a member of the People team for help. If someone informs you that you've made them feel uncomfortable, believe them. Even when you think you may know someone, people and circumstances can change. It is your responsibility to learn and respect their boundaries. You may not intend for your actions to be discriminatory, or a form of bullying and harassment, however, you are accountable for your actions if someone perceives them to be unwelcomed.

Be Curious. Not all of us will agree all the time, but when we don't understand someone's perspective, we seek to understand through getting curious and asking questions.

Be Inclusive. We strive to be a company that welcomes and supports people of all backgrounds and identities. This includes, but is not limited to members of any race, ethnicity, culture, national origin, colour, immigration status, social and economic class, educational level, sexual orientation, gender identity and expression, age, size, family status, political belief, religion, and mental and physical ability.

Have Integrity. We expect everyone to be respectful when working with others. We treat people with respect, fairness, and dignity. If we make a mistake, take responsibility and make changes.

Acceptable and Expected Behaviour

The following behaviours are expected and requested of all Spare staff:

- Participate in an authentic and active way. In doing so, you contribute to the health and longevity of Spare.
- Exercise consideration and respect in your speech and actions at all times.
- Attempt collaboration before conflict.
- Refrain from demeaning, discriminatory, or harassing behaviour and speech.

- Be mindful of your surroundings and of your fellow participants. Alert Spare leaders if you notice a dangerous situation, someone in distress, or violations of this Code of Conduct, even if they seem inconsequential.
- Remember that Spare events may be shared with members of the public and Spare customers; please be respectful to all patrons of these locations at all times.
- Using inclusive language outlined [here](#).

Unacceptable Behaviour

The following behaviours are considered harassment and are unacceptable within our community:

- Violence, threats of violence or violent language directed against another person.
- Sexist, racist, homophobic, transphobic, ableist or otherwise discriminatory jokes and language.
- Posting or displaying sexually explicit or violent material.
- Posting or threatening to post other people's personally identifying information ("doxing").
- Personal insults, particularly those related to gender, sexual orientation, race, religion, or disability.
- Inappropriate photography or recording.
- Inappropriate physical contact. You should have someone's consent before touching them in any manner.
- Unwelcome sexual attention. This includes sexualized comments or jokes; inappropriate touching, groping, and unwelcome sexual advances.
- Deliberate intimidation, stalking or following (online or in person).
- Advocating for, or encouraging, any of the above behaviour.
- Repeated harassment of others. In general, if someone asks you to stop, then stop.
- Other conduct which could reasonably be considered inappropriate in a professional setting.

Weapons Policy

No weapons will be allowed at Spare events, office locations, or in other spaces covered by the scope of this Code of Conduct. Weapons include but are not limited to guns, explosives (including fireworks), and large knives such as those used for hunting or display, as well as any other item used for the purpose of causing injury or harm to others.

Anyone seen in possession of one of these items will be asked to leave immediately and will be subject to punitive action up to and including termination and involvement of law enforcement authorities. Spare staff are further expected to comply with all federal, provincial, state and local laws on this matter.

Consequences of Unacceptable Behaviour

Unacceptable behaviour from any Spare staff, including those with decision-making authority, will not be tolerated.

Anyone asked to stop unacceptable behaviour is expected to comply immediately.

If a staff member engages in unacceptable behaviour, Spare leadership may take any action deemed appropriate, up to and including suspension or termination.

Employees who violate this policy may face disciplinary consequences in proportion to their violation.

Reporting Violations

If you experience or observe discrimination, bullying, or harassment, you have a right to bring a complaint to your manager, or VP of People without reprisal. You will be respectfully heard and have your complaint fairly and confidentially investigated within a reasonable time frame. We will then determine what corrective action is appropriate.

It is a violation of this policy to retaliate against any person making a complaint of discrimination, workplace harassment, or workplace bullying or against any person participating in the investigation of (including testifying as a witness to) any such allegation. Any retaliation or intimidation may be subject to disciplinary action, up to and including termination.

1. Concerns should be reported as soon as possible after an incident has occurred, preferably in writing to your direct manager, or if necessary, to the People team.

2. Upon receiving a complaint or being advised by a supervisor or manager that violation of this policy may be occurring, the VP of People will review the complaint.
3. The VP of People will initiate an investigation to determine whether there is a reasonable basis for believing that the alleged violation of this policy occurred. During the investigation, the VP of People may ask to speak with you again, or request to bring a member of the executive team onto the call.
4. Upon conclusion of an investigation, the VP of People will recommend appropriate disciplinary action commensurate with the severity of the situation.
5. Once a final decision is made, the VP of People will notify both parties of the outcome separately.

Versions

Aa Version	Description	Date	Author	Approved by	Attachment
<u>1</u>	First Version	@February 1, 2021	Erin Girard	Alexey Indeev	Code_of_Conduct.pdf
<u>2</u>	No changes	@March 22, 2022	Erin Girard	Alexey Indeev	
<u>3</u>	Second Version	@April 27, 2022	Erin Girard		
<u>4</u>	Third Version	@February 16, 2023	Mijay Pavon	Mijay Pavon	
<u>5</u>	Renew	@April 4, 2023	Mijay Pavon	Mijay Pavon	



Cryptography Policy

Policy Owner: 🧐 Alexey Indeev

Effective Date: April 4, 2023

Purpose

To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information. This policy establishes requirements for the use and protection of cryptographic keys throughout their entire lifecycle.

Scope

All information systems developed and/or controlled by Spare which store or transmit confidential data.

Policy

Spare shall evaluate the risks inherent in the processing and storing data, and shall implement cryptographic controls to mitigate those risks where deemed appropriate. Where encryption is in use, strong cryptography with associated key management processes and procedures shall be implemented and documented. All encryption shall be performed in accordance with industry standards, including NIST SP 800-57.

For all personal data, Spare shall consider the state of the art, the costs of implementation and the nature, scope, context, and purposes of processing as well as the risk of varying likelihood and severity to the rights and freedoms of natural persons, and implement appropriate technical and organizational measures surrounding the pseudonymization and encryption of data to ensure a level of security appropriate to the risk.

For all web traffic sent over the public Internet containing confidential, the TLS v1.2 protocol or better must be utilized.

Key Management

Access to keys and secrets shall be tightly controlled in accordance with the Access Control Policy.

The following table includes the recommended usage for cryptographic keys:

Aa Domain	≡ Key Type	≡ Algorithm	≡ Key Length	≡ Max Expiration
<u>Web Certificate</u>	Digital Signature	DSA or RSA PKCS#1	2048 bit	Up to 2 years for normal certificates, up to 10 years for root certificates.
<u>Web Cipher</u>	Encryption	AES	256 bit	N/A
<u>Confidential</u>	Encryption	AES	256 bit	1 Year
<u>Password</u>	Hash	Bcrypt, PBKDF2, or scrypt, ECDH	256 bit+10K Stretch	N/A
<u>Laptop HDD</u>	Encryption	AES	128 or 256 bit	N/A

Exceptions

Requests for an exception to this policy must be submitted to the CTO for approval.

Violations & Enforcement

Any known violations of this policy should be reported to the CTO. Violations of this policy can result in immediate withdrawal or suspension of system and network privileges and/or disciplinary action in accordance with company procedures up to and including termination of employment.

Versions

Aa Version	Description	Date	Author	Approved by	Attachment
<u>1</u>	First Version	@February 1, 2021	Alexey Indeev	Alexey Indeev	<u>Cryptography_Policy.pdf</u>
<u>2</u>	No changes	@March 22, 2022	Alexey Indeev	Alexey Indeev	
<u>Untitled</u>	Renewed	@April 4, 2023	Alexey Indeev	Alexey Indeev	



Data Classification Policy HIPAA Addendum

Policy Owner: 🧑 Alexey Indeev

Effective Date: April 4, 2023

Purpose

This HIPAA policy addendum outlines Spare's approach to data classification of ePHI to ensure the confidentiality, integrity and availability of ePHI on company systems and networks. This addendum seeks to satisfy certain standards and requirements of HIPAA, the Privacy Rule and the Security Rule, including, Title 45, §§

- 164.312(a)(2)(iv)

of the Code of Federal Regulations ("CFR").

Definitions

Capitalized terms used in this document and not otherwise defined herein shall have the meanings set forth in the Privacy Rule and the Security Rule, which definitions are incorporated in this document by reference.

Protected Health Information (PHI) and Electronic Protected Health Information (ePHI) when referred to in this document is defined in 45 CFR § 160.103.

Scope

This policy applies to any ePHI that customers of Spare collect from their user base via notes, custom fields, structured fields or uploaded files.

ePHI Data Encryption and Decryption

All ePHI will be encrypted, whether at rest or in transmission, where a risk analysis indicates that such encryption is necessary to protect the security of ePHI. Such risk analysis will consider the probability and impact of these risks to Spare's security.

Exceptions

Existing systems and applications containing ePHI which cannot use encryption because of a technological limitation may be granted a special exception by the HIPAA Security Officer. However, these systems and applications will be required to have a formal risk assessment performed by the HIPAA Security Officer to ensure that major risks are addressed via compensating controls to protect the data in lieu of encryption. Exceptions will be reviewed periodically and removed when a suitable solution is available.

Violations

Failure to encrypt ePHI when required in the absence of a system failure is a violation of this policy and may result in corrective disciplinary action, up to and including termination of employment. Violation may also result in civil and criminal penalties to Spare as determined by federal and state laws and regulations related to loss of data. Violation

may also result in liability to Spare related to loss of data. Any known violations of this policy should be reported to the HIPAA Security Officer.

Responsibility

The HIPAA Security Officer will be responsible for implementing this policy and will ensure that further responsibility is assigned for the proper management of data.

Versions

Aa Version	Description	Date	Author	Approved by	Attachment
<u>1</u>	First Version	@February 1, 2021	Alexey Indeev	Alexey Indeev	Data_Management_Classification_Policy_HIPAA_Addendum.pdf
<u>2</u>	No changes	@March 22, 2022	Alexey Indeev	Alexey Indeev	
<u>Untitled</u>	Renewed	@April 4, 2023	Alexey Indeev	Alexey Indeev	



Data Management Policy

Policy Owner: 🧑 Alexey Indeev

Effective Date: April 4, 2023

Purpose

To ensure that information is classified, protected, retained and securely disposed of in accordance with its importance to the organization.

Scope

All Spare data, information and information systems.

Policy

Spare classifies data and information systems in accordance with legal requirements, sensitivity, and business criticality in order to ensure that information is given the appropriate level of protection. Data owners are responsible for identifying any additional requirements for specific data or exceptions to standard handling requirements.

Information systems and applications shall be classified according to the highest classification of data that they store or process.

Data Classification

To help Spare and its employees easily understand requirements associated with different kinds of information, the company has created three classes of data.

Confidential

Highly sensitive data requiring the highest levels of protection; access is restricted to specific employees or departments, and these records can only be passed to others with approval from the data owner, or a company executive. Example include:

- Customer Data
- Personally identifiable information (PII)
- Company financial and banking data
- Salary, compensation and payroll information
- Strategic plans
- Incident reports
- Risk assessment reports
- Technical vulnerability reports
- Authentication credentials
- Secrets and private keys
- Source code
- Litigation data

Restricted

Spare proprietary information requiring thorough protection; access is restricted to employees with a “need-to-know” based on business requirements. This data can only be distributed outside the company with approval. This is default for all company information unless stated otherwise. Examples include:

- Internal policies
- Legal documents
- Meeting minutes and internal presentations
- Contracts
- Internal reports
- Slack messages

- Email

Public

Documents intended for public consumption which can be freely distributed outside Spare. Examples include:

- Marketing materials
- Product descriptions
- Release notes
- External facing policies

Labeling

Confidential data should be labeled “confidential” whenever paper copies are produced for distribution.

Data Handling

Confidential Data Handling

Confidential data is subject to the following protection and handling requirements:

- Access for non-preapproved-roles requires documented approval from the data owner
- Access is restricted to specific employees, roles and/or departments
- Confidential systems shall not allow unauthenticated or anonymous access
- Confidential Customer Data shall not be used or stored in non-production systems/environments
- Confidential data shall be encrypted in transit over public networks
- Mobile device hard drives containing confidential data, including laptops, shall be encrypted

- Mobile devices storing or accessing confidential data shall be protected by a log-on password or passcode and shall be configured to lock the screen after five (5) minutes of non-use
- Backups shall be encrypted
- Confidential data shall not be stored on personal phones or devices or removable media including USB drives, CD's, or DVD's
- Paper records shall be labeled "confidential" and securely stored and disposed
- Hard drives and mobile devices used to store confidential information must be securely wiped prior to disposal or physically destroyed
- Transfer of confidential data to people or entities outside the company shall only be done in accordance with a legal contract or arrangement, and the explicit written permission of management or the data owner

Restricted Data Handling

Restricted data is subject to the following protection and handling requirements:

- Access is restricted to users with a need-to-know based on business requirements
- Restricted systems shall not allow unauthenticated or anonymous access
- Transfer of restricted data to people or entities outside the company or authorized users shall require management approval and shall only be done in accordance with a legal contract or arrangement, or the permission of the data owner
- Paper records shall be securely stored and disposed
- Hard drives and mobile devices used to store restricted information must be securely wiped prior to disposal or physically destroyed

Public Data Handling

No special protection or handling controls are required for public data. Public data may be freely distributed.

Data Retention

Spare shall retain data as long as the company has a need for its use, or to meet regulatory or contractual requirements. Once data is no longer needed, it shall be securely disposed of or archived.

Please find our current Data Retention Matrix here:  [Data Retention Matrix and Procedure](#)

Data & Device Disposal

Data classified as restricted or confidential shall be securely deleted when no longer needed. Spare shall assess the data and disposal practices of third-party vendors in accordance with the Third-Party Management Policy. Only third-parties who meet Spare requirements for secure data disposal shall be used for store and process restricted or confidential data.

Spare shall ensure that all restricted and confidential data is securely deleted from company devices prior to, or at the time of disposal.

See our Asset Disposal and Recycling Procedure here:

 [Asset Disposal and Recycling Procedure \(Wiping Computers\)](#)

Annual Data Review

Management shall review data retention requirements during the annual review of this policy. Data shall be disposed of in accordance with this policy.

Legal Requirements

Under certain circumstances, Spare may become subject to legal proceedings requiring retention of data associated with legal holds, lawsuits, or other matters as stipulated by Spare legal counsel. Such records and information are exempt from any other requirements specified within this Data Management Policy and are to be retained in accordance with requirements identified by the Legal department. All such holds and special retention requirements are subject to annual review with Spare's legal counsel to evaluate continuing requirements and scope.

Policy Compliance

Spare will measure and verify compliance to this policy through various methods, including but not limited to, business tool reports, and both internal and external audits.

Exceptions

Requests for an exception to this policy must be submitted to the CTO for approval.

Violations & Enforcement

Any known violations of this policy should be reported to the CTO. Violations of this policy can result in immediate withdrawal or suspension of system and network privileges and/or disciplinary action in accordance with company procedures up to and including termination of employment.

Versions

 Version	 Description	 Date	 Author	 Approved by	 Attachment
<u>1</u>	First Version	@February 1, 2021	Alexey Indeev	Alexey Indeev	Data_Management_Policy.pdf
<u>2</u>	Minor updates to the recycling tracking process	@March 22, 2022	Alexey Indeev	Alexey Indeev	
<u>3</u>	Renewed	@April 4, 2023	Alexey Indeev	Alexey Indeev	



Disaster Recovery HIPAA Addendum

Policy Owner: 🧑 Alexey Indeev

Effective Date: April 4, 2023

Purpose

This HIPAA policy addendum outlines Spare's approach and plans for disaster recovery to ensure the availability of ePHI on company systems and networks in the event of a disaster. The addendum seeks to satisfy certain standards and requirements of HIPAA, the Privacy Rule and the Security Rule, including, Title 45, §§

- 164.308(a)(7)(ii)(B)
- 164.308(a)(7)(ii)(C)
- 164.308(a)(7)(ii)(D)
- 164.308(a)(7)(ii)(E)
- 164.312(a)(2)(ii) of the Code of Federal Regulations ("CFR").

Definitions

Capitalized terms used in this document and not otherwise defined herein shall have the meanings set forth in the Privacy Rule and the Security Rule, which definitions are incorporated in this document by reference. Protected Health Information (PHI) and electronic Protected Health Information (ePHI) when referred to in this document is defined in 45 CFR § 160.103.

ePHI Data Backup Recovery Plan

Spare will conduct periodic backups of user-level and system-level ePHI data in a manner consistent with Spare's Data Backup policy. ePHI stored on portable devices must also be saved to Spare owned network devices to ensure complete backup of ePHI data. Data backup procedures outlined in the Data Backup Plan shall be tested periodically to ensure that exact copies of ePHI are maintained and retrievable. Periodic testing schedules will be consistent with Spare's Backup policy. All media used for backing up ePHI is stored in a physically secure environment, such as a secure, off-site storage facility or a physically secure on-premises location, different from the location of the computer systems in order to protect those backups from loss or damage. The

HIPAA Security Officer must approve any changes to the Spare's Backup Plan with regards to the treatment of ePHI information and backup process.

ePHI Disaster Recovery Plan

To ensure that Spare can recover from the loss of data due to an emergency or disaster impacting systems containing ePHI, Spare will establish and implement disaster recovery procedures as outlined in Spare's Disaster Recovery Plan.

ePHI Emergency Mode Plan

Spare shall establish and implement (as needed) procedures to enable continuation of critical business processes for protection of the security of ePHI while operating in emergency mode. Emergency mode operation involves those critical business processes that shall occur to protect the security of ePHI during and immediately after a crisis situation consistent with the Spare's Business Continuity Policy. Emergency mode operation procedures outlined in the Emergency Mode Operation Plan shall be tested on the same periodic basis as other Disaster Recovery exercises to ensure that critical business processes as consistent with Spare's Business Continuity Policy. The HIPAA Security Officer shall oversee the creation, evaluation, testing, and updating of the various contingency plans described herein. Any procedures developed by the HIPAA Security Officer or designees, shall be consistent with the Spare HIPAA policies and not deviate from the Spare standards.

Responsibility

The HIPAA Security Officer will be responsible for ensuring this policy is followed.

Versions

 Version	 Description	 Date	 Author	 Approved by	 Attachment
<u>1</u>	First Version	@February 1, 2021	Alexey Indeev	Alexey Indeev	Disaster_Recovery_HIPAA_Addendum.pdf
<u>2</u>	No changes	@March 22, 2022	Alexey Indeev	Alexey Indeev	
<u>3</u>	Renewed	@April 4, 2023	Alexey Indeev	Alexey Indeev	
<u>Untitled</u>					



HIPAA Breach Notification Policy

Policy Owner: 🧑 Alexey Indeev

Effective Date: April 4, 2023

Purpose

The following policy will outline the steps that will be taken in the event unsecured PHI is breached in a manner prohibited under HIPAA.

This addendum seeks to satisfy requirements of HIPAA, the Privacy Rule and the Security Rule including, Title 45, §§ - 164.404 - 164.406 - 164.408 - 164.410 - 164.412 - 164.414 of the Code of Federal Regulations ("CFR").

Definitions

Capitalized terms used in this document and not otherwise defined herein shall have the meanings set forth in the Privacy Rule and the Security Rule, which definitions are incorporated in this document by reference. Protected Health Information (PHI) and electronic Protected Health Information (ePHI) when referred to in this document is defined in 45 CFR § 160.402.

Employee Training

Executive leadership and every employee whose role requires coming in contact with ePHI data will receive appropriate HIPAA privacy and security compliance training and will acknowledge that he/she has received and reviewed this policy.

Policies and procedures in the event of a potential breach of unsecured ePHI

It is the policy of Spare that all employees will access, use, and disclose PHI only as authorized and permitted by HIPAA, and that all employees shall be vigilant with respect to guarding ePHI at all times. However, in the event that a potential breach occurs, the following policies and procedures shall be followed.

Step 1 – Discovery

A breach of PHI will be deemed “discovered” as of the first day Spare knows of the breach. If a potential breach is discovered, it is very time sensitive and must be immediately reported. It is company policy to follow due diligence with regards to data access reviews and to identify breaches as quickly as possible.

Step 2 – Internal reporting

If an employee suspects that a potential breach of PHI has occurred, they must immediately notify the HIPAA Privacy Officer or an appointed designee.

The notification report should contain as much information as possible regarding the potential breach. This includes names of all employees involved, all data recipients and all others (including third parties) with knowledge of the breach, dates, the nature of the PHI potentially breached, the manner of the disclosure (e.g, email, verbal or otherwise), and any associated documentation that may exist regarding the breach.

Notification and associated documentation may itself contain PHI and should only be given to the HIPAA Privacy Officer or designee.

Reporters of a potential breach should not discuss the potential breach nor attempt to conduct an investigation. These tasks will be performed by the HIPAA Privacy Officer.

Step 3 – Investigation

Upon receipt of notification of a potential breach the HIPAA Privacy Officer, or his/her designee, shall promptly conduct an investigation.

The investigation should include interviewing employees involved, evidence collection and completion of a written record of the investigation and incident.

All documentation related to potential breach investigation is to be stored securely for a minimum of six years.

Step 4 - Risk assessment and recommendations

Once the investigation is complete, the HIPAA Privacy Officer or designee will conduct a Risk Assessment to determine if a use or disclosure of PHI constitutes a breach and requires further notification to affected parties or governing bodies. The HIPAA Privacy Officer or designee must document the Risk Assessment and make a recommendation to leadership regarding whether notification to affected parties or governing bodies regarding the potential breach is warranted. The HIPAA Privacy Officer or designee shall have final authority to determine whether a breach of unsecured PHI occurred and what, if any, further action is warranted.

The HIPAA Privacy Officer or designee will be expected to use their reasoned judgment for the Risk Assessment and ensure that they considered factors such as who, where, when, why and how the unsecured PHI was exposed as well as the extent of the exposure and its impact.

Step 5 – Notification timeliness

In the event that the HIPAA Privacy Officer or designee determines that notice to an affected party, media or governing body is warranted, the HIPAA Privacy Officer or designee shall promptly prepare and send a notice to these parties.

A delay in notification is permissible if a law enforcement official states that a breach notification would impede a criminal investigation or cause damage to national security. In that event, the law enforcement statement must be in writing and must specify the length of the delay required.

Step 6 - Documentation

All steps of this process must be documented in detail for every case and in a manner sufficient to demonstrate that all appropriate steps were completed. All supporting documentation associated with the potential breach shall be kept for a period of 6 years.

Sanctions

Spare employees who fail to fully comply with this Breach Notification Policy will be subject to sanctions as deemed appropriate by management in accordance with the company Sanctions Policy.

Versions

 Version	 Description	 Date	 Author	 Approved by	 Attachment
<u>1</u>	First Version	@February 1, 2021	Alexey Indeev	Alexey Indeev	HIPAA_Breach_Notification_Policy.pdf
<u>2</u>	No changes	@March 22, 2022	Alexey Indeev	Alexey Indeev	
<u>3</u>	Renewed	@April 4, 2023	Alexey Indeev	Alexey Indeev	



HIPAA Sanctions Policy

Policy Owner: 🧐 Alexey Indeev

Effective Date: April 4, 2023

Purpose

This HIPAA policy outlines Spare's approach to sanctions that would be applied in cases where there is a provable violation of the HIPAA rules or company policy. Spare commits to safeguarding the confidentiality, integrity, and availability of ePHI within its systems and networks. Spare commits to proactively address issues in securing the privacy and security of health information through implementation of sanction practice standards. In the event, that an employee of Spare is responsible for a violation of HIPAA, the following sanction guidelines would apply.

The policy seeks to satisfy certain standards and requirements of HIPAA, the Privacy Rule and the Security Rule, including, Title 45, §§

- 164.308(a)(1)(ii)(C) of the Code of Federal Regulations ("CFR").

Definitions

Capitalized terms used in this document and not otherwise defined herein shall have the meanings set forth in the Privacy Rule and the Security Rule which definitions are incorporated in this document by reference. Protected Health Information (PHI) and electronic Protected Health Information (ePHI) when referred to in this document is defined in 45 CFR § 160.103. Spare commits to safeguarding the confidentiality, integrity, and availability of ePHI within its systems and networks. Spare commits to proactively address issues in securing the privacy and security of health information through implementation of sanction practice standards. In the event, that an employee of Spare is responsible for a violation of HIPAA, the following sanction guidelines would apply.

Offense Classification

Offenses under this policy can be defined by Level (1 - 5) where level is determined by the severity and intention of the action. Level I offenses are defined as an unintentional breach of privacy or security that may be caused by lack of knowledge, lack of judgment, or human error including accessing information not required for your job or sharing, copying and changing ePHI without authorization. Level II offenses are defined as an unintentional breach of privacy or security that may be caused by carelessness, such as losing a computer, misdirection of documents containing ePHI information or discussing confidential information with unauthorized persons. Level III offenses are defined as a failure to follow policies and procedures. Any repeat Level II or Level I offense will be classified as a Level III offense. Level IV offenses are defined as deliberate or purposeful violation without harmful intent. This is an intentional violation due to curiosity or desire to gain information for personal use. Level V offenses are defined as deliberate unauthorized disclosure of ePHI for malice or personal gain. Multiple Level I, II or III offenses will be classified as a Level V offense.

Sanctions

Level 1 through IV offenses may be subject to, but not limited to, verbal or written reprimand, retraining on HIPAA Awareness or other company policy or termination of employment.

Level V offenses may include, but not limited to, termination of employment and civil or criminal penalties under applicable Federal/State/City laws.

Responsibility to Report

Workforce members and business associates have a responsibility to report known HIPAA violations to Spare. Reports are to be made to the HIPAA Security Officer. Failure to report a known HIPAA violation may result in disciplinary action in accordance with Spare policies. All training regarding this policy will be provided by the HIPAA Security Officer.

Investigation

Upon receipt of a report of a HIPAA violation, the Spare Security Officer or a designated shall conduct a confidential and timely investigation of the report. If necessary, advice

may be sought from legal assistance at any point during the investigation. Based upon the circumstances of the violation or breach, management or human resources will determine the specific disciplinary action that is to be taken for the employee.

Sanction Exemptions

Sanctions will not apply to disclosures by employees who are whistleblowers and who act in good faith on the belief that Spare has engaged in conduct that is unlawful or otherwise violates professional standards.

Mitigation

Spare will mitigate, to the extent practicable, any harmful effect that is known to be the result of the use or disclosure of ePHI in violation of HIPAA regulations. Spare will not allow retaliatory action against a workforce member. There will be no intimidation, threatening, coercion, or discrimination against an individual who participates in the reporting of a HIPAA violation.

Documentation and Audit Processes

Spare will periodically review sanction history to ensure consistent and equitable application across roles by violation category. Sanction data, such as number and severity of sanctions as well as workforce role to which the sanction was applied should be retained for reporting and audit purposes. Review of this data should be used to identify gaps and opportunities for improvements in Spare's privacy and security programs.

Responsibility

The HIPAA Security Officer will maintain all documentation of any investigation, sanctions applied, and actions taken to mitigate recurrence for a minimum of six years after the conclusion of the investigation.

Versions

Aa Version	Description	Date	Author	Approved by	Attachment
<u>1</u>	First Version	@February 1, 2021	Alexey Indeev	Alexey Indeev	<u>HIPAA Sanctions Policy.pdf</u>
<u>2</u>	No changes	@March 22, 2022	Alexey Indeev	Alexey Indeev	
<u>3</u>	Renewed	@April 4, 2023	Alexey Indeev	Alexey Indeev	



Human Resource Security Policy

Policy Owner: 🧑🏻 Alexey Indeev

Effective Date: April 4, 2023

Purpose

To ensure that employees and contractors meet security requirements, understand their responsibilities, and are suitable for their roles.

Scope

This policy applies to all employees of Spare, consultants, contractors and other third-party entities with access to Spare production networks and system resources.

Policy

Competence Assessment

The skills and competence of employees and contractors shall be assessed by human resources staff and the hiring manager or his or her designees as part of the hiring process. Required skills and competencies shall be listed in job descriptions and requisitions. Competency evaluations may include reference checks, education and certification verifications, technical testing, and interviews.

All Spare employees will undergo performance reviews at least annually which will include an assessment of job performance, competence in the role, adherence to company policies and code of conduct, and achievement of role-specific objectives.

Terms & Conditions of Employment

Company policies and information security roles and responsibilities shall be communicated to employees and third-parties at the time of hire or engagement. Employees and third-parties with access to company or customer information shall sign an appropriate non-disclosure or confidentiality agreement. Contractual agreements shall state responsibilities for information

security as needed. Employees and relevant third-parties shall follow all Spare information security policies.

Management Responsibilities

Management shall be responsible for ensuring that information security policies and procedures are reviewed annually, distributed and available, and that employees and contractors abide by those policies and procedures for the duration of their employment or engagement. Annual policy review shall include a review of any linked or referenced procedures, standards or guidelines.

Management shall ensure that information security responsibilities are communicated to individuals, through written job descriptions, policies or some other documented method which is accurately updated and maintained. Compliance with information security policies and procedures and fulfillment of information security responsibilities shall be evaluated as part of the performance review process wherever applicable.

Information Security Awareness, Education & Training

All Spare employees and third-parties with administrative or privileged technical access to Spare production systems and networks shall complete security awareness training at the time of hire and annually thereafter. Management shall monitor training completion and shall take appropriate steps to ensure compliance with this policy. Employees and contractors shall be aware of relevant information security policies and procedures.

Disciplinary Process

Employees and third-parties who violate Spare information security policies shall be subject to the Spare progressive disciplinary process, up to and including termination of employment or contract.

Exceptions

Requests for an exception to this policy must be submitted to the People Lead for approval.

Violations & Enforcement

Any known violations of this policy should be reported to the People Lead. Violations of this policy can result in immediate withdrawal or suspension of system and network privileges and/or disciplinary action in accordance with company policies up to and including termination of employment.

Versions

 Version	 Description	 Date	 Author	 Approved by	 Attachment
<u>1</u>	First Version	@February 1, 2021	Alexey Indeev	Alexey Indeev	<u>Human_Resource_Security_Policy.pdf</u>
<u>2</u>	No changes	@March 22, 2022	Alexey Indeev	Alexey Indeev	
<u>3</u>	Renewed	@April 4, 2023	Alexey Indeev	Alexey Indeev	



Incident Response Plan

Policy Owner: 🧐 Alexey Indeev

Effective Date: April 4, 2023

Purpose

This document establishes the plan for managing information security incidents and events, and offers guidance for employees or incident responders who believe they have discovered, or are responding to, a security incident.

Scope

This policy covers all information security or data privacy events or incidents.

Incident and Event Definitions

A security event is an observable occurrence relevant to the confidentiality, availability, integrity, or privacy of company controlled data, systems or networks.

A security incident is a security event which results in loss or damage to the confidentiality, availability, integrity, or privacy of company controlled data, systems or networks.

Incident Reporting & Documentation

Reporting

If a Spare employee, contractor, user, or customer becomes aware of an information security event or incident, possible incident, imminent incident, unauthorized access,

policy violation, security weakness, or suspicious activity, then they shall immediately report the information using one of the following communication channels:

- Email security@sparelabs.com information or reports about the event or incident
- Contact members of the security team through Slack

Reporters should act as a good witness and behave as if they are reporting a crime. Reports should include specific details about what has been observed or discovered.

Severity

Security team shall monitor incident and event tickets and shall assign a ticket severity based on the following categories.

S3/S4 - Low and Medium Severity

Issues meeting this severity are simply suspicions or odd behaviours. They are not verified and require further investigation. There is no clear indicator that systems have tangible risk and do not require emergency response. This includes lost/stolen laptop with disk encryption, suspicious emails, outages, strange activity on a laptop, etc.

S2 - High Severity

High severity issues relate to problems where an adversary or active exploitation hasn't been proven yet, and may not have happened, but is likely to happen. This may include lost/stolen laptop without encryption, vulnerabilities with direct risk of exploitation, threats with risk or adversarial persistence on our systems (e.g.: backdoors, malware), malicious access of business data (e.g.: passwords, vulnerability data, payments information), or threats that put any individual at risk of physical harm.

S1 - Critical Severity

Critical issues relate to actively exploited risks and involve a malicious actor. Identification of active exploitation is required to meet this severity category.

Escalation and Internal Reporting

The incident escalation contacts can be found below in notion: 🙌 [The Team](#)

S1 - Critical Severity: S1 issues require immediate notification to Engineering management.

S2 - High Severity: A Jira ticket must be completed and the appropriate manager (see S1 above) must also be notified via Slack with a reference to the ticket number.

S3/S4 - Medium and Low Severity: A Jira ticket must be created and assigned to the appropriate department for response.

Documentation

All reported security events, incidents, and response activities shall be documented in Jira.

A root cause analysis may be performed on all verified S1 security incidents. A root cause analysis report shall be documented and referenced in the incident ticket. The root cause analysis shall be reviewed by the CTO who shall determine if a post-mortem meeting will be called.

Incident Response Process

For critical issues, the response team will follow an iterative response process designed to investigate, contain exploitation, eradicate the threat, recover system and services, remediate vulnerabilities, and document a post-mortem with the lessons of an incident.

Summary

- Event reported
- Triage and analysis
- Investigation
- Containment & neutralization (short term work)
- Recovery & vulnerability remediation
- Hardening & Detection improvements (lessons learned, long term work)

Detailed

- CTO / COO / Engineering Manager / Operations Manager will manage the incident response effort
- A central “War Room” will be designated, which may be a physical or virtual location (i.e Slack channel)
- A recurring Incident Response Meeting will occur at regular intervals until the incident is resolved.
- Legal and executive staff will be informed as needed

Incident Response Meeting Agenda

- Update Incident Ticket and timelines
- Document new Indicators of Compromise (IOCs)
- Perform investigative Q&A
- Apply emergency mitigations
- Plan long term mitigations
- Document Root Cause Analysis (RCA)
- Additional items as needed

Special Considerations

Internal Issues

Issues where the malicious actor is an internal employee, contractor, vendor, or partner requires sensitive handling. The incident manager shall contact the Executive Team directly and will not discuss with other employees. These are critical issues where follow-up must occur.

Compromised Communications

Incident responders must have Slack messaging arranged before listing themselves as incident members. If there are IT communication risks, an out of band solution will be chosen, and communicated to incident responders via phone calls or text messaging.

Additional Requirements

- Suspected and reported events and incidents shall be documented.
- Suspected incidents shall be assessed and classified as either an event or an incident.
- Incident response shall be performed according to this plan and any associated procedures.
- All incidents shall be formally documented, and a documented root cause analysis shall be performed.
- Suspected and confirmed unauthorized access events shall be reviewed by the Incident Response Team. Breach determinations shall only be made by the CEO and legal counsel in coordination with executive management.
- Spare shall promptly and properly notify customers, partners, users, affected parties, and regulatory agencies of relevant incidents or breaches in accordance with Spare policies, contractual commitments, and regulatory requirements.

Roles & Responsibilities

Every employee and user of any Spare information resources has responsibilities toward the protection of the information assets. The table below establishes the specific responsibilities of the incident responder roles.

Response Team Members

Aa Role	≡ Responsibility

Aa Role	≡ Responsibility
<u>Incident Manager</u>	The Incident Manager is the primary and ultimate decision maker during the response period. The Incident Manager is ultimately responsible for resolving the incident and formally closing incident response actions. Incident Manager should be an engineering manager or an engineer (if primary resources are not available). Contact information for engineering management can be found here: 🖐 <u>The Team</u> These responsibilities include: • Ensuring the right people from all functions are actively involved at all times • Status updates are communicated to the appropriate persons at regular intervals • Incidents are resolved in the immediate term • Determining necessary follow-up actions • Assigning follow-up activities to the appropriate people • Promptly reporting incident details which may trigger breach reporting, in writing to the CTO.
<u>Incident Response Team (IRT)</u>	The individuals who have been engaged and are actively working on the incident. All members of the IRT will remain engaged in incident response until the incident is formally resolved, or they are formally dismissed by the Incident Manager.
<u>Engineers (Support and Development)</u>	Qualified engineers will be placed into the on-call rotation and may act as the Incident Manager (if primary resources are not available) or a member of the IRT when engaged to respond to an incident. Engineers are responsible for understanding the technologies and components of the information systems, the security controls in place including logging, monitoring, and alerting tools, appropriate communications channels, incident response protocols, escalation procedures, and documentation requirements. When Engineers are engaged in incident response, they become members of the IRT.
<u>Users</u>	Employees and contractors of Spare. Users are responsible for following policies, reporting problems, suspected problems, weaknesses, suspicious activity, and security incidents and events.
<u>Customers</u>	Customers are responsible for reporting problems with their use of Spare services. Customers are responsible for verifying that reported problems are resolved.
<u>Legal Counsel</u>	Responsible, in conjunction with the CEO and executive management, for determining if an incident shall be considered a reportable breach. Counsel shall review and approve in writing all external breach notices before they are sent to any external party.

Aa Role	≡ Responsibility
<u>Executive Management</u>	Responsible, in conjunction with the CEO and legal counsel, for determining if an incident shall be considered a reportable breach. An appropriate company officer shall review and approve in writing all external breach notices before they are sent to any external party. Spare shall seek stakeholder consensus when determining whether a breach has occurred. The Spare CEO shall make a final breach determination in the event that consensus cannot be reached.

Management Commitment

Spare management has approved this policy and commits to providing the resources, tools and training needed to reasonably respond to identified security events and incidents with the potential to adversely affect the company or its customers.

Exceptions

Requests for an exception to this Policy must be submitted to and authorized by the CTO for approval. Exceptions shall be documented.

Violations & Enforcement

Any known violations of this policy should be reported to the CTO. Violations of this policy may result in immediate withdrawal or suspension of system and network privileges and/or disciplinary action in accordance with company procedures up to and including termination of employment.

Versions

Aa Version	≡ Description	📅 Date	≡ Author	≡ Approved by	📎 Attachment
<u>1</u>	First Version	@February 1, 2021	Alexey Indeev	Alexey Indeev	<u>Incident_Response_Plan.pdf</u>
<u>2</u>	No changes	@March 22, 2022	Alexey Indeev	Alexey Indeev	

Aa Version	Description	Date	Author	Approved by	Attachment
<u>3</u>	Renewed	@April 4, 2023	Alexey Indeev	Alexey Indeev	

Brainstorm Solution Alignment (60 min): 9:00-10:00am



Incident Response Policy HIPAA Addendum

Policy Owner: 🧑 Alexey Indeev

Effective Date: April 4, 2023

Purpose

This HIPAA policy addendum outlines our approach to incident reporting and resolution in cases where a HIPAA violation has reported.

This addendum seeks to satisfy certain standards and requirements of HIPAA, the Privacy Rule and the Security Rule, including, Title 45, §§ 164.308(a)(6)(ii) of the Code of Federal Regulations ("CFR").

Definitions

Capitalized terms used in this document and not otherwise defined herein shall have the meanings set forth in the Privacy Rule and the Security Rule which definitions are incorporated in this document by reference. Electronic Protected Health Information (ePHI) when referred to in this document is defined in 45 CFR § 160.103.

Incident Response Plan

For all security incidents that involve ePHI, both internal and with external vendors, the primary aim for Spare's response is to reduce the impact of the incident and prevent future occurrences of the same or a similar incident. ePHI incident reporting and response plans will follow the Spare's Incident Response Policy with the addition of the HIPAA Security Officer as member of the incident management team.

Versions

Aa Version	Description	Date	Author	Approved by	Attachmnet
<u>1</u>	First Version	@February 1, 2021	Alexey Indeev	Alexey Indeev	Incident_Response_Policy_HIPAA_Addendum.pdf
<u>2</u>	No changes	@March 22, 2022	Alexey Indeev	Alexey Indeev	
<u>3</u>	Renewed	@April 4, 2023	Alexey Indeev	Alexey Indeev	



Information Security Policy

Policy Owner: 🧑 Alexey Indeev

Effective Date: April 4, 2023

Overview

This Information Security Policy is intended to protect Spare's employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, web browsing, and file transfers, are the property of Spare. These systems are to be used for business purposes in serving the interests of the company, and of our clients and customers in the course of normal operations.

Effective security is a team effort involving the participation and support of every Spare employee or contractor who deals with information and/or information systems. It is the responsibility of every team member to read and understand this policy, and to conduct their activities accordingly.

Purpose

The purpose of this policy is to communicate our information security policies and outline the acceptable use and protection of Spare's information and assets. These rules are in place to protect customers, employees, and Spare. Inappropriate use exposes Spare to risks including virus attacks, compromise of network systems and services, and legal and compliance issues.

The Spare "Information Security Policy" comprises this policy and all Spare policies referenced and/or linked within this document.

Scope

This policy applies to the use of information, electronic and computing devices, and network resources to conduct Spare business or interact with internal networks and business systems, whether owned or leased by Spare, the employee, or a third party. All employees, contractors, consultants, temporary, and other workers at Spare and its subsidiaries are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with Spare policies and standards, and local laws and regulations.

This policy applies to employees, contractors, consultants, temporaries, and other workers at Spare, including all personnel affiliated with third parties. This policy applies to all Spare-controlled company and customer data as well as all equipment, systems, networks and software owned or leased by Spare.

Security Incident Reporting

All users are required to report known or suspected security events or incidents, including policy violations and observed security weaknesses. Incidents should be reported immediately or as soon as possible by security@sparelabs.com.

In your email please describe the incident or observation along with any relevant details.

Mobile Device Policy

All end-user devices (e.g., mobile phones, tablets, laptops, desktops) must comply with this policy. Employees must use extreme caution when opening email attachments received from unknown senders, which may contain malware.

System-level and user-level passwords must comply with the Access Control Policy. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.

All end-user, personal (BYOD) or company-owned devices used to access Spare information systems (i.e. email) must adhere to the following rules and requirements:

- Devices must be encrypted with a password-protected screensaver or screen lock after 30 minutes of inactivity
- Devices must be locked whenever left unattended

- Users must report any suspected misuse or theft of a mobile device immediately to Security Team
- Confidential information must not be stored on mobile devices or USB drives (this does not apply to business contact information, e.g., names, phone numbers, and email addresses)
- Any mobile device used to access company email must not be shared with any other person
- Upon termination, users agree to return all company-owned devices and delete all company information and accounts from any personal devices

Remote Access Policy

Laptops and other computer resources that are used to access the Spare network must conform to the security requirements outlined in Spare's Information Security Policies and adhere to the following standards:

- To ensure mobile devices do not connect a compromised device to the company network, Antivirus policies require the use and enforcement of client-side antivirus software
- Users must not connect to any outside network without a secure, up-to-date software firewall configured on the mobile computer.
- Users are prohibited from changing or disabling any organizational security controls such as personal firewalls, antivirus software on systems used to access Spare resources
- Use of remote access software and/or services (e.g., VPN client) is allowable as long as it is provided by the company and configured for multi factor authentication (MFA)
- Unauthorized remote access technologies may not be used or installed on any Spare system
- If you access from a public computer (e.g., business center, hotel, etc.), log out of session and don't save anything. Don't check "remember me, collect all printed materials and delete downloaded files (generally is discouraged)

Acceptable Use Policy

Spare proprietary and customer information stored on electronic and computing devices whether owned or leased by Spare, the employee, or a third party, remains the sole property of Spare for the purposes of this policy. Employees and contractors must ensure through legal or technical means that proprietary information is protected in accordance with the Data Management Policy. The use of Google Drive for business file storage is required for users of laptops or company-issued devices. Storing important documents on the file share is how you “backup” your laptop.

You have a responsibility to promptly report the theft, loss, or unauthorized disclosure of Spare proprietary information. You may access, use or share Spare proprietary information only to the extent it is authorized and necessary to fulfill your assigned job duties. Employees are responsible for exercising good judgment regarding the reasonableness of personal use of company-provided devices.

For security and network maintenance purposes, authorized individuals within Spare may monitor equipment, systems, and network traffic at any time.

Spare reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities. Under no circumstances is an employee of Spare authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing Spare-owned resources. The list below is not exhaustive, but attempts to provide a framework for activities which fall into the category of unacceptable use.

The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent, or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Spare.
2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books, or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Spare or the end user does not have an active license.

3. Accessing data, a server, or an account for any purpose other than conducting Spare business, even if you have authorized access, is prohibited.
4. Exporting software, technical information, encryption software, or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
5. Introduction of malicious programs into the network or systems (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
6. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
7. Using a Spare computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws.
8. Making fraudulent offers of products, items, or services originating from any Spare account.
9. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
10. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient, or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
11. Port scanning or security scanning is expressly prohibited unless prior notification to the Spare engineering team is made.
12. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
13. Circumventing user authentication or security of any host, network, or account.
14. Introducing honeypots, honeynets, or similar technology on the Spare network.
15. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).

16. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's session, via any means.
17. Providing information about, or lists of: Spare employees, contractors, partners, or customers to parties outside Spare without authorization.

Email and Communication Activities

When using company resources to access and use the Internet, users must realize they represent the company and act accordingly.

The following activities are strictly prohibited, with no exceptions:

1. Sending unsolicited email messages, including the sending of "junk mail", or other advertising material to individuals who did not specifically request such material (email spam).
2. Any form of harassment via email, telephone, or texting, whether through language, frequency, or size of messages.
3. Unauthorized use, or forging, of email header information.
4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
5. Creating or forwarding "chain letters", "Ponzi", or other "pyramid" schemes of any type.
6. Use of unsolicited email originating from within Spare networks or other service providers on behalf of, or to advertise, any service hosted by Spare or connected via Spare's network.

Additional Policies and Procedures Incorporated by Reference

Aa Role	≡ Purpose
<u>@Access Control Policy</u>	To limit access to information and information processing systems, networks, and facilities to authorized parties in accordance with business objectives.

Aa Role	≡ Purpose
<u>@Asset Management Policy</u>	To identify organizational assets and define appropriate protection responsibilities.
<u>@Business Continuity and Disaster Recovery Plan</u>	To prepare Spare in the event of extended service outages caused by factors beyond our control (e.g., natural disasters, man-made events), and to restore services to the widest extent possible in a minimum time frame.
<u>@Cryptography Policy</u>	To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information.
<u>@Data Management Policy</u>	To ensure that information is classified and protected in accordance with its importance to the organization.
<u>@Human Resource Security Policy</u>	To ensure that employees and contractors meet security requirements, understand their responsibilities, and are suitable for their roles.
<u>@Incident Response Plan</u>	Policy and procedures for suspected or confirmed information security incidents.
<u>@Operations Security Policy</u>	To ensure the correct and secure operation of information processing systems and facilities.
<u>@Physical Security Policy</u>	To prevent unauthorized physical access or damage to the organization's information and information processing facilities.
<u>@Risk Management Policy</u>	To define the process for assessing and managing Spare's information security risks in order to achieve the company's business and information security objectives.
<u>@Secure Development Policy</u>	To ensure that information security is designed and implemented within the development lifecycle for applications and information systems.
<u>@Third-Party Management Policy</u>	To ensure protection of the organization's data and assets that are shared with, accessible to, or managed by suppliers, including external parties or third-party organizations such as service providers, vendors, and customers, and to maintain an agreed level of information security and service delivery in line with supplier agreements.

Documentation Policy

Security Policies may be modified at any given time by compliance personnel, provided that changes are documented. Compliance personnel is responsible for maintaining a historical record of all policies implemented for 6 years from the date of creation. Policy history is tracked in Notion by maintain a record of all previously implemented versions.

Policy Compliance

Spare will measure and verify compliance to this policy through various methods, including but not limited to, business tool reports, and both internal and external audits.

Exceptions

Requests for an exception to this policy must be submitted to the CTO for approval.

Violations & Enforcement

Any known violations of this policy should be reported to the CTO. Violations of this policy can result in immediate withdrawal or suspension of system and network privileges and/or disciplinary action in accordance with company procedures up to and including termination of employment.

Versions

 Version	 Description	 Date	 Author	 Approved by	 Attachment
<u>1</u>	First Version	@February 1, 2021	Alexey Indeev	Alexey Indeev	<u>Information_Security_Policy.pdf</u>
<u>1.1</u>	Small change to indicate we want to store security policies for 6 years	@April 27, 2021	Alexey Indeev	Alexey Indeev	<u>Information_Security_Policy.pdf</u>

Aa Version	Description	Date	Author	Approved by	Attachment
<u>2</u>	No changes	@March 22, 2022	Alexey Indeev	Alexey Indeev	
<u>3</u>	Renewed	@April 4, 2023	Alexey Indeev	Alexey Indeev	



Information Security Policy HIPAA Addendum

Policy Owner: 😊 Alexey Indeev

Effective Date: April 4, 2023

Purpose

This HIPAA policy addendum outlines Spare's approach to the security training for employees to ensure the confidentiality and integrity of ePHI on company systems and networks. The addendum seeks to satisfy certain standards and requirements of HIPAA, the Privacy Rule and the Security Rule, including, Title 45, §§

- 164.308(a)(5)(ii) of the Code of Federal Regulations ("CFR").

Definitions

Capitalized terms used in this document and not otherwise defined herein shall have the meanings set forth in the Privacy Rule and the Security Rule, which definitions are incorporated in this document by reference. Electronic Protected Health Information (ePHI) when referred to in this document is defined in 45 CFR § 160.103.

HIPAA Security Awareness Training

The HIPAA Security Officer will provide appropriate workforce members with security awareness training regarding handling of ePHI and related security measures, such as encryption methods implemented to protect ePHI from unauthorized alteration, transmission security measures implemented to prevent destruction during transmission over communication networks and asset management requirements for authorization and use. Training will be renewed annually, and personnel attendance recorded by the HIPAA Security Officer.

Violations

Any known violations of this policy should be reported to the HIPAA Security Officer. Violations of this policy can result in immediate withdrawal or suspension of system and network privileges and/or disciplinary action in accordance with Spare procedures. Spare may advise law enforcement agencies when a criminal offence may have been committed.

Responsibility

The HIPAA Security Officer will be responsible for ensuring this policy is followed.

Versions

 Version	 Description	 Date	 Author	 Approved by	 Attachment
<u>1</u>	First Version	@February 1, 2021	Alexey Indeev	Alexey Indeev	<u>Information_Security_Policy_HIPAA_Addendum.pdf</u>
<u>2</u>	No changes	@March 22, 2022	Alexey Indeev	Alexey Indeev	
<u>3</u>	Renewed	@April 4, 2023	Alexey Indeev	Alexey Indeev	



Information Security Roles and Responsibilities

Policy Owner: 🧑 Alexey Indeev

Effective Date: April 4, 2023

Statement of Policy

Spare is committed to conducting business in compliance with all applicable laws, regulations, and company policies. Spare has adopted this policy to outline the security measures required to protect electronic information systems and related equipment from unauthorized use.

Objective

This policy and associated guidance establish the roles and responsibilities within Spare, which is critical for effective communication of information security policies and standards. Roles are required within the organization to provide clearly defined responsibilities and an understanding of how the protection of information is to be accomplished. Their purpose is to clarify, coordinate activity, and actions necessary to disseminate security policy, standards, and implementation.

Applicability

This policy is applicable to all Spare infrastructure, network segments, and systems.

Audience

The audience for this policy includes all Spare employees and contractors who are involved with the Information Security Program. Awareness of this policy applies for all other agents of Spare with access to Spare information and network. This includes, but not limited to partners, affiliates, contractors, temporary employees, trainees, guests, and volunteers. The titles will be referred collectively hereafter as “Spare community”.

Aa Roles	☰ Responsibilities
<u>Board of Directors</u>	• Oversighn over Cyber-Risk and internal control for information security, privacy and compliance • Consults with Executive Leadership to understand Spare IT mission and risks and provides guidance to bring them into alignment

Aa Roles	☰ Responsibilities
<u>Executive Leadership</u>	• Approves Capital Expenditures for Information Security • Oversight over the execution of the information security risk management program and risk treatments • Communication Path to Spare Board of Directors • Aligns Information Security Policy and Posture based on Spare's mission, strategic objectives and risk appetite
<u>CTO (IT Manager)</u>	• Oversight over the implementation of information security controls for infrastructure and IT processes • Responsible for the design, development, implementation, operation, maintenance and monitoring of IT security controls • Ensures IT puts into practice the Information Security Framework • Responsible for conducting IT risk assessments, documenting the identified threats and maintaining risk register • Communicates information security risks to executive leadership • Reports information security risks annually to Spare's leadership and gains approvals to bring risks to acceptable levels • Coordinates the development and maintenance of information security policies and standards • Works with applicable executive leadership to establish an information security framework and awareness program • Serve as liaison to the Board of Directors, Law Enforcement, Internal Audit and General Council. • Oversight over Identity Management and Access Control processes
<u>CTO (VP of Engineering)</u>	• Oversight over information security in the software development process • Responsible for the design, development, implementation, operation, maintenance and monitoring of development and commercial cloud hosting security controls • Responsible for oversight over policy development • Responsible for implementing risk management in the development process
<u>Customer Success Manager</u>	• Execution of customer data retention and deletion processes
<u>Systems Owners</u>	• Manage the confidentiality, integrity and availability of the information systems for which they are responsible in compliance with Spare policies on information security and privacy. • Approval of technical access and change requests for non-standard access
<u>Spare Employees, Contractors, temporary workers, etc.</u>	• Acting at all times in a manner which does not place at risk the health and safety of themselves, other person in the workplace, and the information and resources they have use of • Helping to identify areas where risk management practices should be adopted • Taking all practical steps to minimize Spare's exposure to contractual and regulatory liability • Adhering to company policies and standards of conduct • Reporting incidents and observed anomalies or weaknesses
<u>Chief Human Resources Officer</u>	• Ensuring employees and contractors are qualified and competent for their roles • Ensuring appropriate testing and background checks are completed • Ensuring that employees and relevant contractors are presented with company policies and the Code of Conduct (CoC) • Ensuring that employee performance and adherence the CoC is periodically evaluated • Ensuring that employees receive appropriate security training
<u>CFO</u>	• Responsible for oversight over third-party risk management process • Responsible for review of vendor service contracts

Policy Compliance

The CTO (IT Manager) will measure the compliance to this policy through various methods, including, but not limited to—reports, internal/external audits, and feedback to the policy owner. Exceptions to the policy must be approved by the CTO (IT Manager) in advance. Non-compliance will be addressed with management and Human Resources and can result in disciplinary action in accordance with company procedures up to and including termination of employment.

Versions

Aa Version	Description	Date	Author	Approved by	Attachment
<u>1</u>	First Version	@February 1, 2021	Alexey Indeev	Alexey Indeev	<u>Information_Security_Roles_and_Responsibilities.pdf</u>
<u>2</u>	No changes	@March 22, 2022	Alexey Indeev	Alexey Indeev	
<u>3</u>	Renewed	@April 4, 2023	Alexey Indeev	Alexey Indeev	



Operations Security Policy

Policy Owner: 🧑🏻 Alexey Indeev

Effective Date: April 4, 2023

Purpose

To ensure the correct and secure operation of information processing systems and facilities.

Scope

All Spare information systems that are business critical and/or process, store, or transmit company data. This Policy applies to all employees of Spare and other third-party entities with access to Spare networks and system resources.

Operations Security

Documented Operating Procedures

Operating procedures shall be documented and made available to all users who need them.

Change Management

Changes to the organization, business processes, information processing facilities, and systems that affect information security in the production environment and financial systems shall be controlled. All significant changes to in-scope systems must be documented.

Change management processes shall include:

- Processes for planning and testing of changes, including remediation measures

- Documented managerial approval and authorization before proceeding with changes that may have a significant impact on information security, operations, or the production platform
- Advance communication/warning of changes, including schedules and a description of reasonably anticipated effects, provided to all relevant internal and external stakeholders
- Documentation of all emergency changes and subsequent review
- A process for remediating unsuccessful changes

Capacity Management

The use of processing resources and system storage shall be monitored and adjusted to ensure that system availability and performance meets Spare requirements.

Human resource skills, availability, and capacity shall be reviewed and considered as a component of capacity planning and as part of the annual risk assessment process.

Scaling resources for additional processing or storage capacity, without changes to the system, can be done outside of the standard change management and code deployment process.

Separation of Development, Staging and Production Environments

Development and staging environments shall be strictly segregated from production SaaS environments to reduce the risks of unauthorized access or changes to the operational environment. Confidential production customer data must not be used in development or test environments without the express approval of the Customer Success Manager.

For a full description, see the Data Management Policy for a description of Confidential data. If production customer data is approved for use in the course of development or testing, it shall be scrubbed of any such sensitive information whenever feasible.

Systems and Network Configuration, Hardening, and Review

Firewalls shall be used to control network traffic to and from the production environment in accordance with this policy.

Production firewall rules shall be reviewed at least annually. Tickets shall be created to obtain approvals for any needed changes.

Protection from Malware

In order to protect the company's infrastructure against the introduction of malicious software, detection, prevention, and recovery controls to protect against malware shall be implemented, combined with appropriate user awareness.

Anti-malware protections shall be utilized on all employee issued laptops except for those running operating systems not normally prone to malicious software. Additionally, threat detection and response software shall be utilized for company email. The anti-malware protections utilized shall be capable of detecting all common forms of malicious threats.

Spare should scan all files upon their introduction to systems, and continually scan files upon access, modification, or download. Anti-malware definition updates should be configured to be downloaded and installed automatically whenever new updates are available. Known or suspected malware incidents must be reported as a security incident.

It is a violation of company policy to disable or alter the configuration of anti-malware protections without authorization.

Information Backup

The need for backups of systems, databases, information and data shall be considered and appropriate backup processes shall be designed, planned and implemented.

Security measures to protect backups shall be designed and applied in accordance with the confidentiality or sensitivity of the data. Backup copies of information, software and system images shall be taken regularly to protect against loss of data. Backups and restore capabilities shall be periodically tested, not less than annually.

Spare does not regularly backup user devices like laptops. Users are expected to store critical files and information in company-sanctioned file storage repositories.

Backups are configured to run daily on in-scope systems. The backup schedules are maintained within the backup application software.

Logging & Monitoring

Production infrastructure shall be configured to produce detailed logs appropriate to the function served by the system or device. Event logs recording user activities, exceptions, faults and information security events shall be produced, kept and reviewed through manual or automated processes as needed. Appropriate alerts shall be configured for events that represent a significant threat to the confidentiality, availability or integrity of production systems or Confidential data.

Protection of Log Information

Logging facilities and log information shall be protected against tampering and unauthorized access.

Administrator & Operator Logs

System administrator and system operator activities shall be logged and reviewed and/or alerted in accordance with the system classification and criticality.

Clock Synchronization

The clocks of all relevant information processing systems within an organization or security domain shall be synchronized to network time servers using reputable time sources.

File Integrity Monitoring and Intrusion Detection

Unauthorized intrusions and access attempts or changes to Spare systems shall be investigated and remediated in accordance with the Incident Response Plan.

Control of Operational Software

The installation of software on production systems shall follow the change management requirements defined in this policy.

Technical Vulnerability Management

Information about technical vulnerabilities of information systems being used shall be obtained in a timely fashion, the organization's exposure to such vulnerabilities shall be evaluated, and appropriate measures taken to address the associated risk. A variety of methods shall be used to obtain information about technical vulnerabilities, including vulnerability scanning, penetration tests, and the bug bounty program.

External vulnerability scans shall be run on the production environment at least quarterly. Interior vulnerability scans shall be run against test environments which mirror production configurations.

Penetration tests of the applications and production network shall be performed at least annually. Additional scanning and testing shall be performed following major changes to production systems.

The IT and Engineering departments shall evaluate the severity of vulnerabilities, and if it is determined to be a critical or high-risk vulnerability, a service ticket will be created. The Spare assessed severity level may differ from the level automatically generated by scanning software or determined by external researchers based on Spare's internal knowledge and understanding of technical architecture and real-world impact/exploitability. Tickets are assigned to the system, application, or platform owners for further investigation and/or remediation.

Vulnerabilities assessed by Spare shall be remediated in the following timeframes:

Aa Determined Severity	☰ Remediation Time
<u>Critical</u>	30 Days
<u>High</u>	30 Days
<u>Medium</u>	60 Day
<u>Low</u>	90 Days
<u>Informational</u>	As needed

Service tickets for any vulnerability which cannot be remediated within the standard timeline must show a risk treatment plan and planned remediation timeline.

Restrictions on Software Installation

Rules governing the installation of software by users shall be established and implemented in accordance with the Spare Information Security Policy.

Information Systems Audit Considerations

Audit requirements and activities involving verification of operational systems shall be carefully planned and agreed to minimize disruptions to business processes.

Exceptions

Requests for an exception to this policy must be submitted to the CTO (IT Manager) for approval.

Violations & Enforcement

Any known violations of this policy should be reported to the CTO (IT Manager). Violations of this policy can result in immediate withdrawal or suspension of system and network privileges and/or disciplinary action in accordance with company procedures up to and including termination of employment.

Versions

 Version	 Description	 Date	 Author	 Approved by	 Attachment
<u>1</u>	First Version	@February 1, 2021	Alexey Indeev	Alexey Indeev	<u>Operations_Security_Policy.pdf</u>
<u>2</u>	No changes	@March 22, 2022	Alexey Indeev	Alexey Indeev	
<u>3</u>	Renewed	@April 4, 2023	Alexey Indeev	Alexey Indeev	



Physical Security Policy

Policy Owner: 🧐 Alexey Indeev

Effective Date: April 4, 2023

Purpose

To prevent unauthorized physical access or damage to the organization's information and information processing facilities.

Scope

All Spare offices and locations. This Policy applies to all employees of Spare, and to all external parties with physical access to Spare-owned or leased facilities.

Policy

Physical Security Perimeter

Physical offices and processing facilities shall meet all local building codes for construction materials for walls, windows, doors, and access control mechanisms. Some interior zones may be identified as secure areas where physical access is further restricted to a subset of Spare personnel; such as private offices, wiring closets, print and server rooms, and server racks.

Physical Entry Controls

Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access. Where possible, Spare access control systems shall be tied to a centralized system that provides granular access control for individual personnel. Access events shall be appropriately logged and reviewed as

needed according to risk. Cameras and intrusion detection systems shall be used at facilities that store or process production data.

Securing Offices, Rooms & Facilities

Physical security for offices, rooms and facilities shall be designed and applied to protect from theft, misuse, environmental threats, unauthorized access, and other threats to the confidentiality, integrity, and availability of classified data and systems.

Protecting Against External & Environmental Threats

Physical protection against natural disasters, malicious attack or accidents shall be designed and applied. Secure areas shall be monitored through the use of intrusion detection systems, alarms, and/or video surveillance systems where feasible. Visitor and third-party access to secure areas shall be restricted to reduce the risk of information loss and theft.

Production processing facilities shall be equipped with appropriate environmental and business continuity controls including fire-suppression systems, climate control and monitoring systems, and emergency backup power systems. Physical information system hardware and supporting infrastructure shall be regularly serviced and maintained in accordance with the manufacturer's recommendations.

Working in Secure Areas / Visitor Management

Visitors, delivery personnel, outside support technicians, and other external agents shall not be permitted access to secure areas without escort and/or appropriate oversight. Third-parties in secure areas shall sign in and out on a visitor log and shall be escorted or monitored by Spare personnel. Spare personnel observing unescorted visitors should approach the visitor, confirm their status, and ensure they return to approved areas or report the observation to the responsible authority as needed. External party access to secure areas shall be confirmed with appropriate Spare personnel prior to being granted access. Spare personnel providing access to external parties into secure areas are responsible for ensuring that the third-party personnel adhere to all security requirements, and are accountable for all actions taken by outsiders they provide with access. Visitors may be allowed to work unescorted provided that the Spare sponsoring party can ensure that they will not have unauthorized access to Spare information systems, networks, or data.

Delivery & Loading Areas

Access points such as delivery and loading areas and other points where unauthorized persons could enter secure areas shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.

Supplier, Vendor, and Third-Party Security

Suppliers, vendors, and third parties shall comply with Spare physical security and environmental controls requirements. Spare shall assess the adequacy of third-party physical security controls as part of the vendor management process, in accordance with the Third-Party Management Policy.

Exceptions

Requests for an exception to this policy must be submitted to the People Lead for approval.

Violations & Enforcement

Any known violations of this policy should be reported to the People Lead. Violations of this policy can result in immediate withdrawal or suspension of system and network privileges and/or disciplinary action in accordance with company procedures up to and including termination of employment.

Versions

 Version	 Description	 Date	 Author	 Approved by	 Attachment
<u>1</u>	First Version	@February 1, 2021	Alexey Indeev	Alexey Indeev	Physical_Security_Policy.pdf
<u>2</u>	No changes	@March 22, 2022	Alexey Indeev	Alexey Indeev	
<u>3</u>	Renewed	@April 4, 2023	Alexey Indeev	Alexey Indeev	



Physical Security Policy HIPAA Addendum

Policy Owner: 🗨️ Alexey Indeev

Effective Date: April 4, 2023

Purpose

This HIPAA policy addendum outlines Spare's plans to secure access to facilities that host ePHI or PHI data on premises. The purpose of this addendum is to satisfy certain standards and requirements of HIPAA, the Privacy Rule and the Security Rule, including, Title 45, §§

- 164.310(a)(2)(ii)
- 164.310(a)(2)(iii)
- 164.310(a)(2)(iv) of the Code of Federal Regulations ("CFR").

Definitions

Capitalized terms used in this document and not otherwise defined herein shall have the meanings set forth in the Privacy Rule and the Security Rule which definitions are incorporated in this document by reference. Protected Health Information (PHI) and electronic Protected Health Information (ePHI) when referred to in this document is defined in 45 CFR § 160.103.

Physical Access to Locations with ePHI

Spare is committed to limiting physical access to ePHI systems and the facility or facilities in which such systems are housed, while still ensuring that proper authorized access is allowed. Spare will implement appropriate procedures and access control mechanisms to manage and validate Spare employees, contractors and visitor access to all facilities where ePHI could be disclosed or used in a manner consistent with the Spare's Physical Access Policy. Spare will implement appropriate procedures and access control mechanisms to identify all employees, contractors and business associates so as to permit access to ePHI only in authorized cases and as needed to perform their work in a manner consistent with Spare's System Access Policy. The HIPAA Security Officer should be informed of any lost keys or ID badges if these are required by Spare's Physical Access Policy. The HIPAA Security Officer is responsible for raising the need for physical access changes (e.g. changes to locks or access mechanisms) as a result of the risk created by the lost key or badge. If ePHI is housed on premises, the office/building areas that require physical access will require a signature log of all employees accessing these areas and these logs will be recorded for a minimum of 6 years.

Premises Maintenance

Prior to approving plans for physical area maintenance, the HIPAA Security Officer will determine whether this maintenance or the processes involved may increase the security risk of ePHI for example through unauthorized access or exposure. This includes work completed on the internal and/or external perimeter of the physical area. Where security risks to ePHI are identified, the HIPAA Security Officer will implement risk mitigation actions consistent with Spare's Physical Access Policy. The HIPAA Security Officer maintains all documentation of maintenance visits including the reason for said maintenance and who completed it for a minimum of six years.

Violations

Any individual, found to have violated this policy, may be subject to disciplinary action up to and including termination of employment. Visitors in violation of this policy are subject to loss of vendor privileges and/or termination of services.

Responsibility

The HIPAA Security Officer is responsible for ensuring that this policy is followed.

Versions

 Version	 Description	 Date	 Author	 Approved by	 Attachment
<u>1</u>	First Version	@February 1, 2021	Alexey Indeev	Alexey Indeev	Physical_Security_Policy_HIPAA_Addendum.pdf
<u>2</u>	No changes	@March 22, 2022	Alexey Indeev	Alexey Indeev	
<u>3</u>	Renewed	@April 4, 2023	Alexey Indeev	Alexey Indeev	



Risk Management Policy

Policy Owner: 🧐 Alexey Indeev

Effective Date: April 4, 2023

Purpose

To define the methodology for assessing and managing Spare's information security risks in order to achieve the company's business and information security objectives.

Scope

The risk assessment process may be applied to all business processes, information, information systems, networks, devices, and information processing facilities that are owned or used by Spare applicants, employees, contractors, consultants, vendors, partners, and other users affiliated with Spare, or others using or accessing Spare networks and/or information systems.

Policy

Spare will ensure that risk management plays an integral part in the governance and management of the organization at a strategic and operational level. The purpose of a risk management policy is designed to ensure that the company achieves its stated business and security goals and objectives.

Risk Management Strategy

Spare has developed processes to identify those risks that would hinder the achievement of its strategic and operational objectives. Spare will therefore ensure that it has in place the means to identify, analyze, control, and monitor the strategic and operational risks it faces using this risk management policy based on best practices.

The CTO will ensure the risk management strategy and policy are reviewed regularly and that:

- The risk management policy is applied to relevant areas at Spare
- The risk management policy and its operational application are annually reviewed
- Non-compliance is reported to appropriate company officers and authorities

Practical Application of Risk Management

Spare may use a variety of risk reporting formats for the identification of risks, their classification, and evaluation based on factors such as vendors utilized, methodology employed, and the scope of the assessment. In general, and where possible, risks shall be assessed and ranked according to their impact and their likelihood of occurrence.

In addition, an internal audit of the information security management system (ISMS) (i.e., information security controls and management processes) shall be performed at least annually.

Security risks shall be evaluated at various stages of the software design and development lifecycle as needed.

Risk Categories

Some risks are within the control of Spare while others may be only to a lesser degree. Spare will consider the risks within each of the following categories:

- Technical
- Reputational
- Contractual
- Economic/Financial
- Regulatory/Compliance
- Fraud

Each identified risk will be assessed as to its likelihood and impact. Likelihood can be assessed as not likely, somewhat likely, or very likely. Impact can be assessed as not impactful, somewhat impactful, and very impactful. The likelihood and impact will be considered together to formulate an overall risk ranking.

Risk Criteria

The criteria for determining risk is the combined likelihood and impact of an event adversely affecting the confidentiality, availability, integrity, or privacy of customer data, personally identifiable information (PII), or business critical systems.

For all risk inputs such as risk assessments, penetration tests, vulnerability scans, etc., Spare management shall reserve the right to modify automated or third-party provided risk rankings based on its assessment of the nature and criticality of the system processing, as well as the nature, criticality and exploitability (or other relevant factors and considerations) of the identified vulnerability.

Risk Response and Treatment

Risks will be prioritized and mapped using the approach contained in this policy. The following responses to risk should be employed. Where Spare chooses a risk response other than “Accept,” it shall develop a Risk Treatment Plan.

- Mitigate: Spare may take actions or employ strategies to reduce the risk.
- Accept: Spare may decide to accept and monitor the risk at the present time. This may be necessary for some risks that arise from external events.
- Transfer: Spare may decide to pass the risk on to another party. For example, contractual terms may be agreed to ensure that the risk is not borne by Spare, or insurance may be appropriate for protection against financial loss.
- Eliminate: The risk may be such that Spare could decide to cease the activity or to change it in such a way as to end the risk.

Risk Management Procedure

The procedure for managing risk will meet the following criteria:

- Spare will maintain a Risk Register and Treatment Plan.
- Risks shall be ranked by ‘likelihood’ and ‘severity/impact’ as critical, high, medium, low, or negligible.
- Overall risk shall be determined through a combination of likelihood and impact.

- Risks may be valued to estimate potential monetary loss where practical, or may be considered relative to a control objective
- Spare will respond to risks in a prioritized fashion. Remediation priority will consider the risk likelihood and impact, cost, work effort, and availability of resources. Multiple remediations may be undertaken simultaneously.
- Periodic reports will be made to the senior leadership of Spare to ensure risks are being mitigated appropriately, and in accordance with business priorities and objectives.

Risk Acceptance Levels

Aa Role	≡ Responsibility
<u>CEO</u>	Ultimately responsible party for the acceptance and/or treatment of any risks to the organization.
<u>CTO (VP of Engineering)</u>	Can approve the avoidance, remediation, transference, or acceptance of any risk cited in the Risk Register. This person shall be responsible for communicating risks to top management and the board and adopting risk treatments in accordance with executive direction.
<u>CTO (IT Manager)</u>	Shall be responsible for adherence to this policy.

Amendment & Termination of this Policy

Spare reserves the right to modify, amend or terminate this policy at any time.

Exceptions

Requests for an exception to this Policy must be submitted to the CTO for approval.

Violations & Enforcement

Any known violations of this policy should be reported to the CTO. Violations of this policy can result in immediate withdrawal or suspension of system and network privileges and/or disciplinary action in accordance with company procedures up to and including termination of employment.

Versions

 Version	 Description	 Date	 Author	 Approved by	 Attachment
<u>1</u>	First Version	@February 1, 2021	Alexey Indeev	Alexey Indeev	Risk_Management_Policy.pdf
<u>2</u>	No changes	@March 22, 2022	Alexey Indeev	Alexey Indeev	
<u>3</u>	Renewed	@April 4, 2023	Alexey Indeev	Alexey Indeev	



Secure Development Policy

Policy Owner: 🧑 Alexey Indeev

Effective Date: April 4, 2023

Purpose

To ensure that information security is designed and implemented within the development lifecycle for applications and information systems.

Scope

All Spare applications and information systems that are business critical and/or process, store, or transmit Confidential data. This policy applies to all internal and external engineers and developers of Spare software and infrastructure.

Policy

This policy describes the rules for the acquisition and development of software and systems that shall be applied to developments within the Spare organization.

System Change Control Procedures

Changes to systems within the development lifecycle shall be controlled by the use of formal change control procedures. Change control procedures and requirements are described in the Spare Operations Security Policy.

Significant code changes must be reviewed and approved by software engineer before being merged into any production branch in accordance with the Code Review guidelines found here: 🧑 [Code review guidelines](#)

Software Version Control

All Spare software is version controlled and synced between contributors (developers). Access to the central repository is restricted based on an employee's role. All code is written, tested, and saved in a local repository before being synced to the origin repository.

Technical Review of Applications after Operating Platform Changes

When operating platforms are changed, business critical applications shall be reviewed and tested to ensure that there is no adverse impact on organizational operations or security.

Restrictions on Changes to Software Packages

Modifications to third-party business application packages shall be discouraged, limited to necessary changes and all changes shall be strictly controlled.

Secure System Engineering Principles

Principles for engineering secure systems shall be established, documented, maintained and applied to any information system implementation efforts.

Engineering style guides and technical references can be found in the Engineering Guidelines here:  [Engineering_guidelines](#)

Software developers are expected to adhere to Spare's coding standards throughout the development cycle, including standards for quality, commenting, and security.

Secure Development Environment

Spare shall establish and appropriately protect secure development environments for system development and integration efforts that cover the entire system development life cycle.

Outsourced Development

Spare shall supervise and monitor the activity of outsourced system development. Outsourced development shall adhere to all Spare standards and policies.

System Security Testing

Testing of security functionality shall be carried out during development. No code shall be deployed to Spare production systems without documented, successful test results.

System Acceptance Testing

Acceptance testing programs and related criteria shall be established for new information systems, upgrades and new versions.

Prior to deploying code, automated tests must have succeeded and any relevant manual release test plans must be completed which show the completion of all tests.

Protection of Test Data

Test data shall be selected carefully, protected and controlled. Confidential customer data shall be protected in accordance with all contracts and commitments. Customer data shall not be used for testing purposes without the explicit permission of the data owner and the CTO.

Acquisition of Third-Party Systems and Software

The acquisition of third-party systems and software shall be done in accordance with the requirements of the Spare Third-Party Management Policy.

Exceptions

Requests for an exception to this Policy must be submitted to the CTO for approval.

Violations & Enforcement

Any known violations of this policy should be reported to the CTO. Violations of this policy can result in immediate withdrawal or suspension of system and network privileges and/or disciplinary action in accordance with company procedures up to and including termination of employment.

Versions

Aa Version	Description	Date	Author	Approved by	Attachment
<u>1</u>	First Version	@February 1, 2021	Alexey Indeev	Alexey Indeev	Secure_Development_Policy.pdf
<u>2</u>	No changes	@March 22, 2022	Alexey Indeev	Alexey Indeev	
<u>3</u>	Renewed	@April 4, 2023	Alexey Indeev	Alexey Indeev	



System Access Control Policy HIPAA Addendum

Policy Owner: 🧑 Alexey Indeev

Effective Date: April 4, 2023

Purpose

This HIPAA policy addendum outlines Spare's approach to access authorization and management to ensure confidentiality and integrity of ePHI within the company systems and networks. Spare is committed to mitigating the risk of unauthorized access to ePHI. This policy outlines Spare's commitment to the unique user identification and password, emergency access, automatic logoff, encryption and decryption, firewall, and remote and wireless access procedures that will apply to electronic information systems that maintain ePHI. This addendum seeks to satisfy requirements of HIPAA, the Privacy Rule, and the Security Rule including, Title 45, §§

- 164.308(a)(1)(ii)(D)
- 164.308(a)(4)(ii)(A)
- 164.308(a)(4)(ii)(B)
- 164.308(a)(4)(ii)(C)
- 164.312(a)(1)
- 164.312(b)
- 164.312(d) of the Code of Federal Regulations ("CFR").

Definitions

Capitalized terms used in this document and not otherwise defined herein shall have the meanings set forth in the Privacy Rule and the Security Rule, which definitions are incorporated in this document by reference. Protected Health Information (PHI) and electronic Protected Health Information (ePHI) when referred to in this document is defined in 45 CFR § 160.103.

Security of ePHI Transmission

All encryption mechanisms implemented to comply with this policy must adhere to the encryption standard minimums as stated in Spare's Cryptography Policy. When transmitting ePHI electronically, regardless of the transmission system being used, users must take reasonable precautions to ensure

that the receiving party is who they claim to be (must be authenticated) and has a legitimate need for the ePHI requested. All transmissions of ePHI should include only the minimum amount of ePHI as required. Transmitting ePHI via removable media such as a flash drive or removable hard drive requires the files to be password protected in accordance with Spare's Cryptography Policy.

Unique User Identification and Password

Any user that requires access to any network, system, or application that accesses, transmits, receives, or stores ePHI, must be provided with a unique username and must use this username when accessing any network or system that handles ePHI. Each username account must have a password that meets the minimum requirements as outlined in Spare's Password Policy. Each user must ensure that their assigned username is appropriately protected and only used for legitimate access to Spare's networks, systems, or applications. If a user believes their username or password has been compromised, they must report this to their manager and the HIPAA Security Officer immediately.

Encryption and Decryption

All ePHI will be encrypted, whether at rest or in transmission, where a risk analysis indicates that such encryption is necessary to protect the security of ePHI. Such risk analysis will consider the probability and impact of these risks to Spare's security.

Emergency Access

To ensure that access to critical ePHI is maintained during an emergency situation, Spare's will establish and implement procedures to ensure that access to company systems is maintained where required. This plan is outlined in the Spare's Disaster Recovery Plan.

Automatic Logoff

Servers, workstations, or other computer systems that access, transmit, receive, or store ePHI must employ automatic logoff mechanisms. These logoff systems must terminate a user session in accordance with Spare's Asset Management Policy. Before leaving any server, workstation, or other computer systems unattended, users must lock or activate the system's automatic logoff mechanism or logout of all applications and database systems containing ePHI.

Firewall Use

All networks that handle ePHI data must be appropriately secured in accordance with Spare's System Access Policy.

Remote Access

All remote access mechanisms that would expose or grant users access to ePHI must be configured in accordance with Spare's System Access Policy. All remote portable devices and users of those

devices must comply with Spare's Asset Management Policy and be authorized for use. Confirmation of compliance with this policy by the HIPAA Security Officer is required before access can be granted.

Wireless Access

To ensure that all networks that contain ePHI based systems and applications are appropriately secured, Spare must configure all wireless access points in accordance with Spare's System Access Policy.

Violations

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. Violation may also result in civil and criminal penalties to Spare as determined by federal and state laws and regulations related to loss of data.

Responsibilities

The HIPAA Security Officer is responsible for ensuring this policy is followed.

Versions

 Version	 Description	 Date	 Author	 Approved by	 Attachment
<u>1</u>	First Version	@February 1, 2021	Alexey Indeev	Alexey Indeev	<u>Access_Control_Policy_HIPAA_Addendum.pdf</u>
<u>2</u>	Minor updates	@March 22, 2022	Alexey Indeev	Alexey Indeev	
<u>3</u>	Renewed	@April 4, 2023	Alexey Indeev	Alexey Indeev	



Third-Party Management Policy

Policy Owner: 🧑 Alexey Indeev

Effective Date: April 4, 2023

Purpose

To ensure protection of the organization's data and assets that are shared with, accessible to, or managed by suppliers, including external parties or third-party organizations such as service providers, vendors, and customers, and to maintain an agreed level of information security and service delivery in line with supplier agreements.

This document outlines a baseline of security controls that Spare expects partners and other third-party companies to meet when interacting with Spare Confidential data.

Scope

All data and information systems owned or used by Spare that are business critical and/or process, store, or transmit Confidential data. This policy applies to all employees of Spare and to all external parties, including but not limited to Spare consultants, contractors, business partners, vendors, suppliers, partners, outsourced service providers, and other third-party entities with access to Spare data, systems, networks, or system resources.

Policy

Information security requirements for mitigating the risks associated with supplier's access to the organization's assets shall be agreed with the supplier and documented.

For all service providers who may access Spare Confidential data, systems, or networks, proper due diligence shall be performed prior to provisioning access or engaging in processing activities. Information shall be maintained regarding which regulatory or

certification requirements are managed by or impacted by each service provider, and which are managed by Spare as required. Applicable regulatory or certification requirements may include ISO 27001, SOC 2, PCI-DSS, CCPA, GDPR or other frameworks or regulations.

Submit third party vendors for review using the following procedure:  [Third-Party Vendor Management Procedure](#)

Information Security in Third-Party Relationships

Addressing Security in Agreements

Relevant information security requirements shall be established and agreed with each supplier that may access, process, store, or transmit Confidential data, or provide physical or virtual IT infrastructure components for Spare.

For all service providers who may access Spare production systems, or who may impact the security of the Spare production environment, written agreements shall be maintained that include the service provider's acknowledgment of their responsibilities for the confidentiality of company and customer data, and any commitments regarding the integrity, availability, and/or privacy controls that they manage in order to meet the standards and requirements that Spare has established in accordance with Spare's information security program or any relevant framework.

Technology Supply Chain

Spare will consider and assess risk associated with suppliers and the technology supply chain. Where warranted, agreements with suppliers shall include requirements to address the relevant information security risks associated with information and communications technology services and the product supply chain.

Third-Party Service Delivery Management

Monitoring & Review of Third-Party Services

Spare shall regularly monitor, review, and audit supplier service delivery. Supplier security and service delivery performance shall be reviewed at least annually.

Management of Changes to Third-Party Services

Changes to the provision of services by suppliers, including changes to agreements, services, technology, policies, procedures, or controls, shall be managed, taking account of the criticality of the business information, systems, and processes involved. Spare shall assess the risk of any material changes made by suppliers and make appropriate modifications to agreements and services accordingly.

Third-Party Risk Management

Spare will ensure that potential risks posed by sharing Confidential data are identified, documented and addressed according to this policy. Risk management plays an integral part in the governance and management of the organization at a strategic and operational level. The purpose of a partner and third-party security policy is to ensure that partnerships and services achieve their business plan aims and objectives, and are consistent with Spare's requirements for information security.

Spare shall not share or transmit Confidential data to a third-party without first performing a third-party risk assessment and fully executing a written contract, statement of work or service agreement which describes expected service levels and any specific information security requirements.

Third-Party Security Standards

All third-parties must maintain reasonable organizational and technical controls as assessed by Spare.

Assessment of third-parties which receive, process, or store Confidential data shall consider the following controls as applicable based on the service provided and the sensitivity of data stored, processed or exchanged.

Information Security Policy

Third-parties maintain information security policies supported by their executive management, which are regularly reviewed.

Risk Assessment & Treatment

Third-parties maintain programs that assess, evaluate, and manage information and technology risks.

Operations Security

Third-parties implement commercially reasonable practices and procedures designed, as appropriate, to maintain operations security. Protections may include:

- Technical testing
- Protection against malicious software
- Network protection and management
- Technical vulnerability management
- Logging and monitoring
- Incident response
- Business continuity planning

Access Control

Third-parties maintain a technical access control program.

Secure System Development

Third-parties maintain a secure development program consistent with industry software and systems development best practices including risk assessment, formal change management, code standards, code review and testing.

Physical & Environmental Security

If third-parties are storing or processing confidential data, their physical and environmental security controls should meet the requirements of the Spare Physical Security Policy.

Human Resources

Third-parties maintain human resource policies and processes which include criminal background checks for any employees or contractors who access Spare Confidential information.

Compliance & Legal

Spare shall consider all applicable regulations and laws when evaluating suppliers and third parties who will access, store, process or transmit Spare Confidential data. Third-party assessments should consider the following criteria:

- Protection of customer data, organizational records, and records retention and disposition
- Privacy of Personally Identifiable Information (PII)

Exceptions

Requests for an exception to this Policy must be submitted to the CTO (IT Manager) for approval.

Violations & Enforcement

Any known violations of this policy should be reported to the CTO (IT Manager).

Violations of this policy can result in immediate withdrawal or suspension of system and network privileges and/or disciplinary action in accordance with company procedures up to and including termination of employment.

Versions

 Version	 Description	 Date	 Author	 Approved by	 Attachment
<u>1</u>	First Version	@February 1, 2021	Alexey Indeev	Alexey Indeev	<u>Third-Party_Management_Policy.pdf</u>

Aa Version	Description	Date	Author	Approved by	Attachment
<u>2</u>	Minor changes in vendor request process	@March 22, 2022	Alexey Indeev	Alexey Indeev	
<u>3</u>	Renewed	@April 4, 2023	Alexey Indeev	Alexey Indeev	

NORTH CAROLINA DEPARTMENT OF INFORMATION TECHNOLOGY – TRANSPORTATION



Application / Service Resiliency Signoff (ARS)

This Demand Response Scheduling service has been determined to be **Statewide Critical**. Offerors are therefore required to provide the **Maximum Tolerable Downtime (MTD)**, and a **Recovery Point Objective (RPO)** with a bid submission. *Use hours. As one day may mean 8 hours & or 24 hours, etc.*

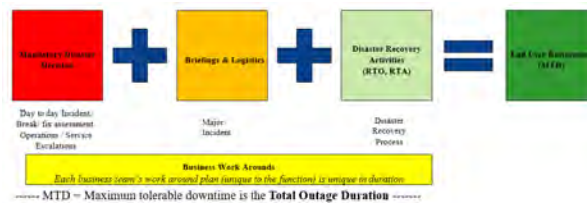
Disaster Recovery requirements are:	
Criticality level	Statewide
Maximum Tolerable Downtime (MTD)	xx hours
Recovery Point Objective (RPO)	xx hours
Offeror Signature: 	

Definitions;

Statewide Critical: From an information technology perspective, in the agency's opinion, the loss of this application/ service will have a direct impact to statewide core functions, processes and/or activities. The loss may also impact a large portion of the State's population).

MTD: The maximum number of hours for which it is acceptable that a function can be interrupted following a continuity event. (FEMA See, Recovery Time Objective; Maximum Acceptable Outage)

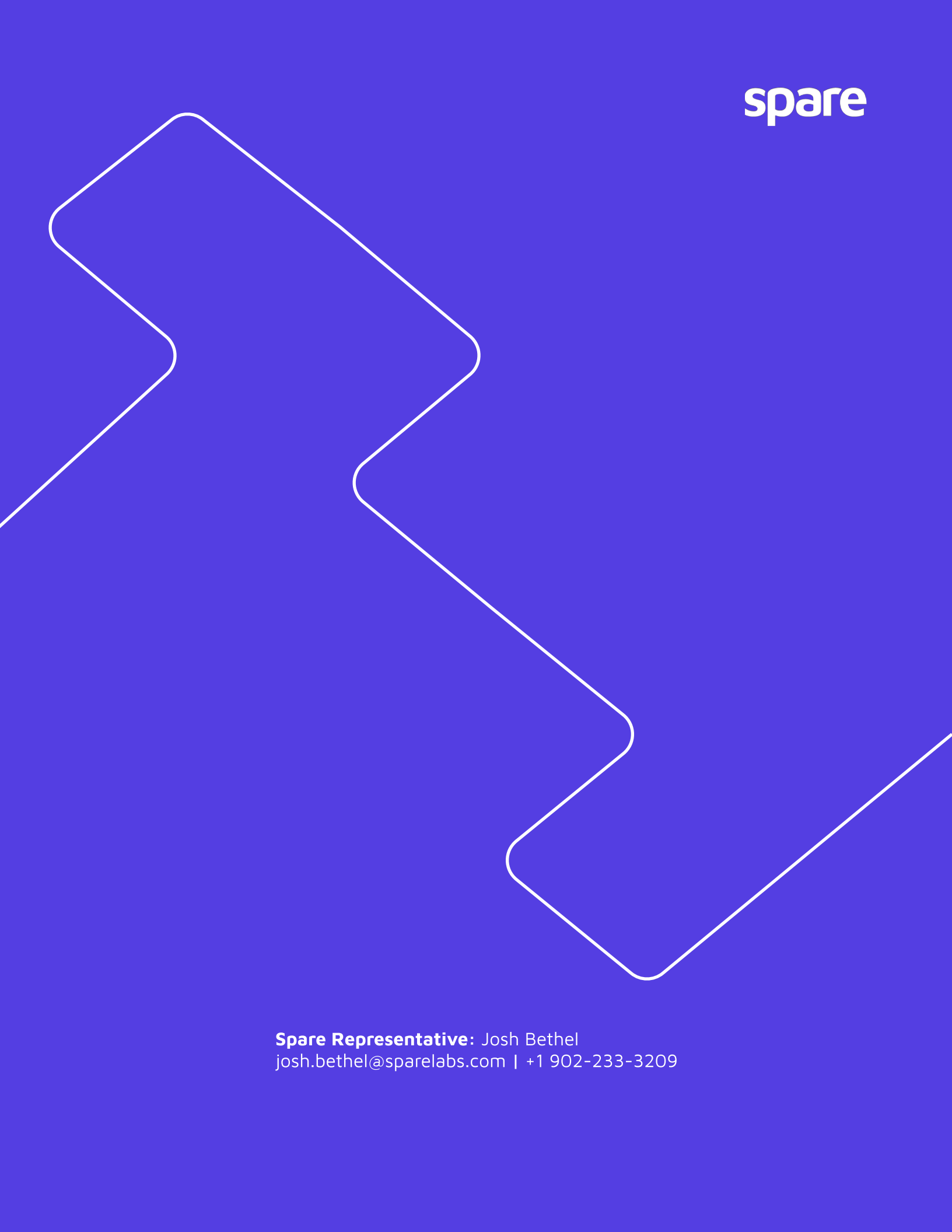
MTD Clarification; Represents the total amount of time leadership are willing to accept for a mission/business process outage or disruption including all impact considerations. Further, while RTO - Recovery Time Objective is required to recover the IT Application / system, MTD includes RTO plus (if) business work arounds exist that would apply in the early stages of an outage prior to a disaster declaration.



MTD is made up of 2 components, RTO plus business work arounds.

RPO: Recovery Point Objective = The point in time to which systems and data must be recovered following an adverse event, e.g. the last completed transaction or the point immediately before the last backup commences. Also known as the Critical Data Point.

RPO Clarification: Age of the data to be restored to, once the application / system is recovered in the DR environment & made available to the business. For example, 8 hours, means the data is "8 hours older than the time the incident occurred.



spare

Spare Representative: Josh Bethel
josh.bethel@sparelabs.com | +1 902-233-3209