

VILLAGE OF DOWNERS GROVE
Report for the Village Council Meeting
6/13/2017

SUBJECT:	SUBMITTED BY:
Authorization of a Contract for an Integrated Parking Management System for Commuter Parking	Nan Newlon Director of Public Works

SYNOPSIS

A motion is requested authorizing approval of a contract through the National Cooperative Purchasing Alliance (NCPA) for an integrated parking management system for commuter parking with PassportParking, Inc.

STRATEGIC PLAN ALIGNMENT

The goals for 2015-2017 include *Exceptional Municipal Services*.

FISCAL IMPACT

Authorization of this contract will reduce the cost of providing this service.

RECOMMENDATION

Approval on the June 13, 2017 Active Agenda.

BACKGROUND

The Village provides daily fee parking spaces at each of the three commuter rail stations - Belmont, Main and Fairview. To park in these spaces commuters pay \$3.00/day, typically at one of 11 pay stations located near the stations or parking areas. In 2013 the Village added a pay-by-phone feature to this program, allowing commuters to pay for parking through a mobile app. Commuters pay a \$.50 surcharge when they use the pay-by-phone feature. Under the current agreement, the vendor Passport, retains \$.37 of the \$.50, and the Village receives \$.13, from which the Village pays credit card processing fees. Under the terms of the cooperative purchasing agreement, Passport would retain \$.25/transaction, or a reduction of \$.12/transaction, and the Village would receive \$.25/transaction. This reduction in cost will enable the Village to completely cover the costs of credit card processing. In addition to this change, the Village will also work with Passport to reduce credit card processing fees. Because Passport is the current pay-by-phone provider, the proposed change will not impact commuters.

After these changes have been implemented to the pay-by-phone feature staff will be investigating the addition of an electronic permit management system. This system will enhance service to permit parkers and reduce staff time.

ATTACHMENTS

Contract Documents

Passport



Passport

Request for Proposal for Integrated Parking Management System RFP No. 26-16

Due: November 3, 2016 at 2:00PM CST

For:

Region 14 Education Service Center

1850 Highway 351

Abilene, Texas 79601

From:

Passport

427 Tatnall Street, Suite 27927

Wilmington, DE 19801-2230

USA

(704)-837-8066

Cover Letter

PassportParking, Inc. ("Passport") is pleased to present a proposal for a pay by phone application for the National Cooperative Purchasing Alliance, Region 14 Education Service Center. Passport provides an unparalleled software and management experience to both parking customers and municipalities across North America. While others have taken the approach of a one-size-fits-all solution, Passport recognizes the significant nuances of individual cities and environments. In 2014, Passport developed and deployed the first ever private label mobile payment for parking application, ParkOmaha. Since launching ParkOmaha, Passport has taken the approach of offering a custom configured application with the ease of an off the shelf solution.

Passport currently serves over 250 clients, including Boston, Toronto, and Chicago. Every client has access to the same features as every other client and may choose to turn features on or off depending on that city's unique needs. In its experience working with so many cities, Passport has a complete understanding of the entire value chain of parking, from session initiation to citation payment, and will guide the city to the best suited feature set. Passport's applications, leadership team, implementation process, and programming architecture reflect a continued commitment to specialized support for each parking operation.

Passport's technological superiority and attentiveness to customer service has yielded a 100% municipal client retention rate while maintaining 95% of its contracts on a month to month basis. Passport's clients stick with Passport because of its commitment to creating a memorable user experience and constantly seeking and incorporating client feedback into the product.

Passport is thrilled to have the opportunity to partner with the NCPA and deliver its world-class product to the Region 14 Education Service Center. Please review the following proposal and do not hesitate to reach out to me with any questions or clarifications related to this proposal.

Best Wishes,



Khristian Gutierrez
CBDO, Passport
Khristian.Gutierrez@passportinc.com


TABLE OF CONTENTS**PAGE**

Signature Form	2
NCPA Administration Agreement	3
Vendor Questionnaire	7
Vendor Profile	10
Products and Services/Scope	23
References	75
Pricing	80
Value Added Products and Services	83
Required Documents	87
Passport in the News	100
Training Materials	103

Signature Form

The undersigned further certifies that he/she is an officer of the company and has authority to negotiate and bind the company named below and has not prepared this bid in collusion with any other Respondent and that the contents of this proposal as to prices, terms or conditions of said bid have not been communicated by the undersigned nor by any employee or agent to any person engaged in this type of business prior to the official opening of this proposal.

Prices are guaranteed: **120 days**

Company name	PassportParking, Inc.
Address	427 Tatnall Street, Ste. 27927
City/State/Zip	Wilmington, DE 19801
Telephone No.	(302) 543-2882
Fax No.	(888) 804-1783
Email address	RFP@Passportinc.com
Printed name	Khristian Gutierrez
Position with company	Chief Business Development Officer
Authorized signature	

NCPA Administration Agreement

Tab 2 – NCPA Administration Agreement

This Administration Agreement is made as of November 14, 2016, by and between National Cooperative Purchasing Alliance (“NCPA”) and PassportParking, Inc. (“Vendor”).

Recitals

WHEREAS, Region 14 ESC has entered into a certain Master Agreement dated November 14, 2016 referenced as Contract Number 05-20, by and between Region 14 ESC and Vendor, as may be amended from time to time in accordance with the terms thereof (the “Master Agreement”), for the purchase of Integrated Parking Management System;

WHEREAS, said Master Agreement provides that any state, city, special district, local government, school district, private K-12 school, technical or vocational school, higher education institution, other government agency or nonprofit organization (hereinafter referred to as “public agency” or collectively, “public agencies”) may purchase products and services at the prices indicated in the Master Agreement;

WHEREAS, NCPA has the administrative and legal capacity to administer purchases under the Master Agreement to public agencies;

WHEREAS, NCPA serves as the administrative agent for Region 14 ESC in connection with other master agreements offered by NCPA

WHEREAS, Region 14 ESC desires NCPA to proceed with administration of the Master Agreement;

WHEREAS, NCPA and Vendor desire to enter into this Agreement to make available the Master Agreement to public agencies on a national basis;

NOW, THEREFORE, in consideration of the payments to be made hereunder and the mutual covenants contained in this Agreement, NCPA and Vendor hereby agree as follows:

- ◆ General Terms and Conditions
 - The Master Agreement, attached hereto as Tab 1 and incorporated herein by reference as though fully set forth herein, and the terms and conditions contained therein shall apply to this Agreement except as expressly changed or modified by this Agreement.
 - NCPA shall be afforded all of the rights, privileges and indemnifications afforded to Region 14 ESC under the Master Agreement, and such rights, privileges and indemnifications shall accrue and apply with equal effect to NCPA under this Agreement including, but not limited to, the Vendor’s obligation to provide appropriate insurance and certain indemnifications to Region 14 ESC.
 - Vendor shall perform all duties, responsibilities and obligations required under the Master Agreement in the time and manner specified by the Master Agreement.
 - NCPA shall perform all of its duties, responsibilities, and obligations as administrator of purchases under the Master Agreement as set forth herein, and Vendor acknowledges that NCPA shall act in the capacity of administrator of purchases under the Master Agreement.
 - With respect to any purchases made by Region 14 ESC or any Public Agency pursuant to the Master Agreement, NCPA (a) shall not be construed as a dealer, re-marketer, representative, partner, or agent of any type of Vendor, Region 14 ESC, or such Public Agency, (b) shall not be obligated, liable or responsible (i) for any orders made by Region

14 ESC, any Public Agency or any employee of Region 14 ESC or Public Agency under the Master Agreement, or (ii) for any payments required to be made with respect to such order, and (c) shall not be obligated, liable or responsible for any failure by the Public Agency to (i) comply with procedures or requirements of applicable law, or (ii) obtain the due authorization and approval necessary to purchase under the Master Agreement. NCPA makes no representations or guaranties with respect to any minimum purchases required to be made by Region 14 ESC, any Public Agency, or any employee of Region 14 ESC or Public Agency under this Agreement or the Master Agreement.

- The Public Agency participating in the NCPA contract and Vendor may enter into a separate supplemental agreement to further define the level of service requirements over and above the minimum defined in this contract i.e. invoice requirements, ordering requirements, specialized delivery, etc. Any supplemental agreement developed as a result of this contract is exclusively between the Public Agency and Vendor. NCPA, its agents, members and employees shall not be made party to any claim for breach of such agreement.

◆ Term of Agreement

- This Agreement shall be in effect so long as the Master Agreement remains in effect, provided, however, that the obligation to pay all amounts owed by Vendor to NCPA through the termination of this Agreement and all indemnifications afforded by Vendor to NCPA shall survive the term of this Agreement.

◆ Fees and Reporting

- The awarded vendor shall electronically provide NCPA with a detailed monthly or quarterly report showing the dollar volume of all sales under the contract for the previous month or quarter. Reports shall be sent via e-mail to NCPA offices at reporting@ncpa.us. Reports are due on the fifteenth (15th) day after the close of the previous month or quarter. It is the responsibility of the awarded vendor to collect and compile all sales under the contract from participating members and submit one (1) report. The report shall include at least the following information as listed in the example below:

Entity Name	Zip Code	State	PO or Job #	Sale Amount

Total _____

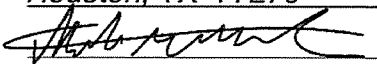
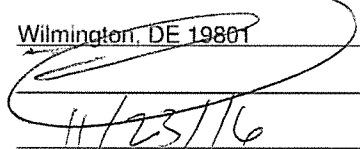
- Each quarter NCPA will invoice the vendor based on the total of sale amount(s) reported. From the invoice the vendor shall pay to NCPA an administrative fee based upon the tiered fee schedule below. Vendor’s annual sales shall be measured on a calendar year basis. Deadline for term of payment will be included in the invoice NCPA provides.

<u>Annual Sales Through Contract</u>	<u>Administrative Fee</u>
0 - \$30,000,000	2%
\$30,000,001 - \$50,000,000	1.5%
\$50,000,001+	1%

- Supplier shall maintain an accounting of all purchases made by Public Agencies under the Master Agreement. NCPA and Region 14 ESC reserve the right to audit the accounting for a period of four (4) years from the date NCPA receives the accounting. In the event of such an audit, the requested materials shall be provided at the location designated by Region 14 ESC or NCPA. In the event such audit reveals an underreporting of Contract Sales and a resulting underpayment of administrative fees, Vendor shall promptly pay NCPA the amount of such underpayment, together with interest on such amount and shall be obligated to reimburse NCPA's costs and expenses for such audit.

◆ General Provisions

- This Agreement supersedes any and all other agreements, either oral or in writing, between the parties hereto with respect to the subject matter hereof, and no other agreement, statement, or promise relating to the subject matter of this Agreement which is not contained herein shall be valid or binding.
- Awarded vendor agrees to allow NCPA to use their name and logo within website, marketing materials and advertisement. Any use of NCPA name and logo or any form of publicity regarding this contract by awarded vendor must have prior approval from NCPA.
- If any action at law or in equity is brought to enforce or interpret the provisions of this Agreement or to recover any administrative fee and accrued interest, the prevailing party shall be entitled to reasonable attorney's fees and costs in addition to any other relief to which such party may be entitled.
- Neither this Agreement nor any rights or obligations hereunder shall be assignable by Vendor without prior written consent of NCPA. Any assignment without such consent will be void.
- This Agreement and NCPA's rights and obligations hereunder may be assigned at NCPA's sole discretion, to an existing or newly established legal entity that has the authority and capacity to perform NCPA's obligations hereunder
- All written communications given hereunder shall be delivered to the addresses as set forth below.

National Cooperative Purchasing Alliance:	Vendor:	<u>PassportParking, Inc.</u>
Name: <u>Matthew Mackel</u>	Name: <u>Khristian Gutierrez</u>	
Title: <u>Director, Business Development</u>	Title: <u>Chief Business Development Officer</u>	
Address: <u>PO Box 701273</u>	Address: <u>427 Tatnall Street, Ste. 27927</u>	
		<u>Wilmington, DE 19801</u>
Signature: 	Signature: 	
Date: <u>November 14, 2016</u>	Date: <u>11/23/16</u>	

Vendor Questionnaire

Tab 3 – Vendor Questionnaire

Please provide responses to the following questions that address your company's operations, organization, structure, and processes for providing products and services.

◆ States Covered

➤ Bidder must indicate any and all states where products and services can be offered.

➤ Please indicate the price co-efficient for each state if it varies.

50 States & District of Columbia (Selecting this box is equal to checking all boxes below)

- | | | |
|---|---|---|
| <input type="checkbox"/> Alabama | <input type="checkbox"/> Maryland | <input type="checkbox"/> South Carolina |
| <input type="checkbox"/> Alaska | <input type="checkbox"/> Massachusetts | <input type="checkbox"/> South Dakota |
| <input type="checkbox"/> Arizona | <input type="checkbox"/> Michigan | <input type="checkbox"/> Tennessee |
| <input type="checkbox"/> Arkansas | <input type="checkbox"/> Minnesota | <input type="checkbox"/> Texas |
| <input type="checkbox"/> California | <input type="checkbox"/> Mississippi | <input type="checkbox"/> Utah |
| <input type="checkbox"/> Colorado | <input type="checkbox"/> Missouri | <input type="checkbox"/> Vermont |
| <input type="checkbox"/> Connecticut | <input type="checkbox"/> Montana | <input type="checkbox"/> Virginia |
| <input type="checkbox"/> Delaware | <input type="checkbox"/> Nebraska | <input type="checkbox"/> Washington |
| <input type="checkbox"/> District of Columbia | <input type="checkbox"/> Nevada | <input type="checkbox"/> West Virginia |
| <input type="checkbox"/> Florida | <input type="checkbox"/> New Hampshire | <input type="checkbox"/> Wisconsin |
| <input type="checkbox"/> Georgia | <input type="checkbox"/> New Jersey | <input type="checkbox"/> Wyoming |
| <input type="checkbox"/> Hawaii | <input type="checkbox"/> New Mexico | |
| <input type="checkbox"/> Idaho | <input type="checkbox"/> New York | |
| <input type="checkbox"/> Illinois | <input type="checkbox"/> North Carolina | |
| <input type="checkbox"/> Indiana | <input type="checkbox"/> North Dakota | |
| <input type="checkbox"/> Iowa | <input type="checkbox"/> Ohio | |
| <input type="checkbox"/> Kansas | <input type="checkbox"/> Oklahoma | |
| <input type="checkbox"/> Kentucky | <input type="checkbox"/> Oregon | |
| <input type="checkbox"/> Louisiana | <input type="checkbox"/> Pennsylvania | |
| <input type="checkbox"/> Maine | <input type="checkbox"/> Rhode Island | |

All US Territories and Outlying Areas (Selecting this box is equal to checking all boxes below)

- | | |
|---|---|
| <input type="checkbox"/> American Samoa | <input type="checkbox"/> Northern Marina Islands |
| <input type="checkbox"/> Federated States of Micronesia | <input checked="" type="checkbox"/> Puerto Rico |
| <input type="checkbox"/> Guam | <input checked="" type="checkbox"/> U.S. Virgin Islands |
| <input type="checkbox"/> Midway Islands | |

- ◆ **Minority and Women Business Enterprise (MWBE) and (HUB) Participation**
 - It is the policy of some entities participating in NCPA to involve minority and women business enterprises (MWBE) and historically underutilized businesses (HUB) in the purchase of goods and services. Respondents shall indicate below whether or not they are an M/WBE or HUB certified.
 - **Minority / Women Business Enterprise**
 - Respondent Certifies that this firm is a M/WBE
 - **Historically Underutilized Business**
 - Respondent Certifies that this firm is a HUB
- ◆ **Residency**
 - Responding Company's principal place of business is in the city of Charlotte, State of NC
- ◆ **Felony Conviction Notice**
 - Please Check Applicable Box;
 - A publically held corporation; therefore, this reporting requirement is not applicable.
 - Is not owned or operated by anyone who has been convicted of a felony.
 - Is owned or operated by the following individual(s) who has/have been convicted of a felony
 - If the 3rd box is checked, a detailed explanation of the names and convictions must be attached.
- ◆ **Distribution Channel**
 - Which best describes your company's position in the distribution channel:
 - Manufacturer Direct Certified education/government reseller
 - Authorized Distributor Manufacturer marketing through reseller
 - Value-added reseller Other: _____
- ◆ **Processing Information**
 - Provide company contact information for the following:
 - **Sales Reports / Accounts Payable**
 Contact Person: Xue Liu
 Title: Account Manager
 Company: PassportParking, Inc.
 Address: 427 Tatnall Street, Ste. 27927
 City: Wilmington State: Delaware Zip: 19801
 Phone: (302) 543-2882 Email: Xue@Passportinc.com

- Purchase Orders
 - Contact Person: Xue Liu
 - Title: Account Manager
 - Company: PassportParking, Inc.
 - Address: 427 Tatnall Street, Ste. 27927
 - City: Wilmington State: Delaware Zip: 19801
 - Phone: (302) 543-2882 Email: Xue@passportinc.com
- Sales and Marketing
 - Contact Person: Daniel Bliley
 - Title: VP of Marketing
 - Company: PassportParking, Inc.
 - Address: 427 Tatnall Street, Ste. 27927
 - City: Wilmington State: Delaware Zip: 19801
 - Phone: (302) 543-2882 Email: Daniel.Bliley@passportinc.com

◆ Pricing Information

- In addition to the current typical unit pricing furnished herein, the Vendor agrees to offer all future product introductions at prices that are proportionate to Contract Pricing.
 - If answer is no, attach a statement detailing how pricing for NCPA participants would be calculated for future product introductions.
 - Yes No
- Pricing submitted includes the required NCPA administrative fee. The NCPA fee is calculated based on the invoice price to the customer.
 - Yes No
- Vendor will provide additional discounts for purchase of a guaranteed quantity.
 - Yes No

◆ Cooperatives

- List any other cooperative or state contracts currently held or in the process of securing.

Cooperative/State Agency	Discount Offered	Expires	Annual Sales Volume

Vendor Profile

PassportParking, Inc. est. 2011

Passport's founding was the culmination of the lifelong entrepreneurial aspiration of Bob Youakim. After college, Bob was working with Wells Fargo in Charlotte, NC where he had daily interaction (and headaches) with the bank's parking payment stations. Bob also realized the inefficiencies of the parking industry given that he was able to get away without paying for his parking for weeks at a time. Upon discussion with people in the parking industry, Bob quickly realized that the industry was ripe for disruption and that there were ways to incentivize both the client and end user to drive the industry forward.

In the summer of 2011, Khristian Gutierrez, a co-worker of Bob's at Wells Fargo's New York office, left the bank to join Bob as a managing partner at Passport. Together, they noticed that the field of mobile payments software applications had only two main competitors and that the applications were often unattractive, plagued with errors, and not well received by any users. It was at this time that Passport changed its focus from providing parking hardware to building sleek, scalable, and user-friendly mobile payments software for the parking industry.

Passport launched its first product, an Interactive Voice Response ("IVR") mobile payment application on NCDOT property, where it was beta tested under the name Alliance Parking. The success of this prototype resulted in the formation of Passport's dedicated software engineering team and the hiring of Brad Powers, CTO. Passport made its official debut in February 2012 at Startup Riot in Atlanta, GA.

In 2012 Passport won a Mobile Payments contract for the entire city of Asheville, NC. Throughout meetings with the city managers, Passport discovered that there was a strong demand for city-branded municipal applications. The idea of private label mobile payment applications came to fruition and is still a big driver for clients to use Passport's applications across the nation.

In January 2013, Passport closed a deal with the city of Omaha, NE to implement a citation enforcement solution and create the base of Passport's current Citation Management Platform. However, by marketing its Private Label capabilities, Passport was also able to secure a deal to provide private label mobile payments for the entire city of Omaha. "Park Omaha" was born, paving the way for the Private Label Payments product. With a fully formed product in the marketplace, Passport filed for incorporation in the state of Delaware.

In the fourth quarter of 2013, Passport signed a deal with Chicago Parking Meters to provide a private label mobile payments platform for the entire city of Chicago. With this deal also came Passport's Series A funding round of \$6MM dollars from Relevance Capital and Grotech Ventures.

Following the launch of Chicago, Passport continued to win cities across North America, including the largest parking environment on the continent, Toronto, Canada (Green P). Passport's products continue to evolve with the needs and desires of its clients and Passport's suite now includes Mobile Payments for Parking, Citation Management, Digital Permitting, and Mobile Ticketing for Transit.

Passport closed its Series B funding round in 2016, receiving an additional \$8MM from MK Capital in Chicago. With that money, Passport will continue to innovate its current products and break into new markets and new verticals to give cities a sole source product for all parking and transportation needs. Passport currently employs a team of 58 people, performing all engineering in house, and paving the way for the future of parking and transit.

DUNS Number:	72254770
Corporate Office Location:	Wilmington, Delaware
Number of Sales Offices:	1
Main Point of Contact:	Khristian Gutierrez, CBDO 427 Tatnall Street, Ste. 27927 Wilmington, DE 19801 (302) 543-2882 Khristian.Gutierrez@PassportInc.com
Standard Terms of Payment:	Net 30
Competitors:	PayByPhone and ParkMobile
Annual Sales in Last 3 Years:	
Cities/Counties:	\$7,500,000.00
K-12:	0
Higher Education:	\$150,000.00
Other Gov. Agencies:	\$200,000.00



Passport Dedicated Team

Brad Powers CTO	Bob Youakim CEO	Khristian Gutierrez CBDO	
Mike Hulthen VP, Engineering	Brandon Rivard VP, Client Success	Michael Rafferty VP, EIT	Drew Myers VP, Project Mgmt.

Software Development

Product & QA		Parking		Infrastructure/Ops	
David Kim	Marcus Wu	Andrew Gerst	Chris Roberts		
Giridhar Venkataraman	Anand Ravi	Kenny Higginbotham	Sean Moriarty	Steven Shelby	Shannon Craven
	Brahma Chilakala	Lucky Narayanan			Sai Jonnala
	Nigilan Palanisamy				

Passport

What differentiates your company from competitors?

Through this procurement, the cities in Region 14 Education Service Center are not just hiring a vendor, but rather are selecting a technology partner; they are determining who will best represent, launch, and accommodate their city as it exists today and in the future. Partnering with Passport means access to a team of 30+ in-house engineers, all of whom ensure that the cities' systems will always be at the cutting edge of technology. It also means that the city will have an active voice in the development of its own product; providing feedback to the current product and working with their own dedicated Client Success Manager to ideate innovative new features. Passport is uniquely positioned to best represent the NCPA and Region 14 for the following reasons:



Built to Scale

Passport believes in the lean methodologies, building products to best accommodate the users and pivoting as necessary with changing and growing demand. In order to be successful in that endeavor, Passport has built its product, its team, and its processes to scale accordingly.

Product

Passport's system processes more than \$85MM annually and is built to successfully manage more than 2 Billion transactions per year. As the City grows, Passport's system will grow along side of it, preventing any lag in the service offering.

Process

Passport has fine-tuned its team and processes to handle the growth of the company and the City's parking operations. These scalable processes are largely responsible for Passport's seamless implementations in the largest parking environments in North America: Chicago (36,000 spaces) and Toronto (55,000 spaces).



Market Leadership

Passport is the only mobile payments company to offer top-of-the line platforms across every facet of the parking and transportation industries. In addition to a Mobile Payment for Parking solution, Passport has developed Citation Management, Digital Permitting, and Mobile Ticketing platforms. Because of Passport's experience developing these platforms, it has a better understanding of the nuances of the parking industry than any other mobile payment provider. When Passport integrates with other enforcement providers, it knows first hand what information will be the most pertinent to the officer, it also knows what data to pull that will be most beneficial for the City to have access to in Passport's backend management portal. This

breadth and depth of experience in the market is unparalleled and is integral to a successful technology partnership.

True Private Label



Passport is the only provider in the market that can provide a true private label solution to the participants in Region 14. While most competitors provide a skinned application with the City's colors and logo, Passport's private label application has a unique name, application in the Google Play and Apple App stores, dedicated website, colors, logos, and is fully customizable. Passport was the first mobile payment provider to deliver a true private label application, ParkOmaha in 2013. Since then, Passport has delivered this service to municipalities and universities of all different sizes and has even created a private label application for a region, including two cities and a state university. Even if the City doesn't opt for a private label application, due to the flexibility of Passport's system, that City will receive a custom configured application tailored to their unique needs and wants, without being burdened with unnecessary functionality.

Robust Back Office



Implementing a mobile payment for parking solution is more than just providing a means for parkers to pay, it is providing data and transparency to improve the City's parking operations. To aid in that, Passport's platform includes a robust back office management and reporting tool that gives the City all the necessary tools and data to manage the entire parking ecosystem.

Management

Passport's backend management tool, Operator Management ("OpsMan") is the brain of Passport's suite of products. From OpsMan, the City will have complete access to their parking rates, event changes, live monitoring of transactions, extensive reporting, and all integrations. If the City wants to add or change a rate or implement a temporary event rate, they can do all of that directly within OpsMan.

Reporting

OpsMan will aggregate all data from the mobile payment system, integrated meters, enforcement, and LPR technology. With all of this data in one warehouse, the City will be able to run a myriad of reports on everything from daily revenue from transactions to the number of unique users on any given day. Every report in OpsMan can be scheduled to run on a recurring basis, set as specifically as one day or as broad as all time, and can be exported to Excel. If there is a report

that the City needs that isn't included in OpsMan already, Passport will work with the City to develop an ad hoc report.



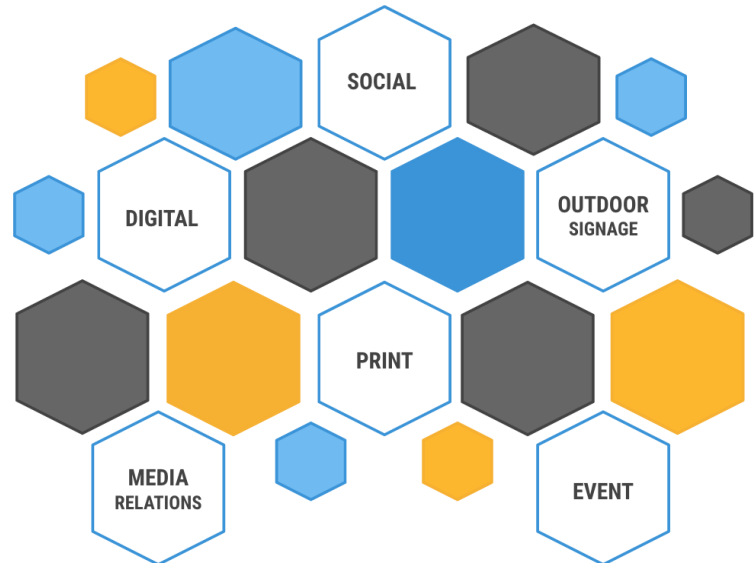
Enhanced Merchant Experience

Paid parking is critical to create turnover, which helps businesses thrive, but residents who frequent these local businesses often voice their concerns over paying frequently to support these businesses. Passport includes local businesses in the parking process by allowing them to pay for their customers' parking. This creates a win-win-win dynamic for all parties involved: the City increases parking revenue, the parker is incentivised to shop locally, and the business gains another opportunity to reward loyal customers.

Describe how your company will market this contract if awarded.

Marketing Campaign

During the implementation process, Passport's marketing team will work closely with the City to develop a marketing campaign to increase utilization of the new parking app. The marketing team will begin by gathering information related to key demographics and channel options. Once that information is gathered, Passport will deploy **one of three advertising options below** to accommodate the launch of the mobile application, generating maximum market exposure for the agency and mobile pay for parking application.



Packages

LAUNCH BURST

The first package is designed to get exposure to the application at the time of launch. This campaign comes with a three week advertising and public relations campaign designed specifically for the City. Most of the advertising will be digital and geared towards early adopters and trendsetters. Depending on the unique demographics of the City, Passport will specifically select distribution channels to maximize awareness and utilization. Depending on the market size, passport will reach 1 million impressions during this time.

SUSTAINED LAUNCH

The second package will extend beyond the launch date and drive adoption and utilization. This campaign is a five week advertising and public relations campaign with both digital advertising and street team involvement. A street team will physically walk the streets of the City and help parkers download and use the app to pay for parking. This boots-on-the-ground tactic will help attract parkers who may be hesitant to learn a new application. Similar to the other packages, Passport will select distribution channels to maximize awareness and utilization throughout the City. During these five weeks, passport will deliver 2 million impressions, depending on market size.

LAUNCH PLUS UTILIZATION

The final package is very similar to the Sustained Launch package, but this package includes a follow up campaign. The initial campaign is five weeks with digital advertising and street team involvement, just like with the Sustained Launch package. However, this package has an additional three week utilization flight that will occur about six weeks after the initial five week flight ends. This package will deliver 5 million impressions, depending on market size.

Advertising Channel Components

Signs

Passport will provide the City with one street sign for every block. The street signs will direct the parker on how to download the app, pay via SMS message, call an IVR number, or call for customer support. If the City desires, the signage will also include the City's logo at no extra charge. Passport can also customize the signs in the City's colors at an additional cost.

Decals

Every meter head and pay station will have a decal on it with directions on how to download the app, the zone number, and the space number (where applicable). These are the necessary data that the parker will have to enter in order to initiate a parking session and will be provided to the City for free.

Digital Advertising

The digital advertising in each package will consist of blog articles placed in native advertising and geo-targeted ads running through digital ad networks. The advertising will be split 80/20 with a concentration on mobile advertising. Passport will also target social media users with 2 posts per week, a promoted post, and geo-targeted install advertising on Twitter and Facebook.

Traditional Advertising

Passport will also reach parkers through traditional advertising, such as information and educational flyers. Passport will place local



newspaper and magazine ads as well, but studies show that digital advertising is a better channel to reach early adopters of a mobile application, so any print advertising will be at an additional charge.



Describe how you intend to introduce NCPA to your company.

To introduce NCPA, Passport will create a custom landing page just for NCPA Region 14 Education Services Center affiliates. From this page, any City looking to implement the mobile payment for parking application will have full access to Passport's product portfolio, including case studies, documentation, and training materials. Cities will also be able to schedule demo's with Passport's sales team to learn more about the product and how it can be configured for that City. Additionally, Passport will host multiple webinars on its product and partnership with NCPA and send out mailers and case studies to all NCPA Region 14 Education Services Center members.

Describe your firm's capabilities and functionality of your on-line catalog/ordering website.

Passport's Mobile Payment for Parking platform is available in three possible tiers: base model, skinned, and true private label. The differences between the tiers centers on the front-end design, specifically the name, colors, and URL. All three tiers offer the same functionality, which is fully configurable to each unique client. From Passport's website (www.passportinc.com), any potential client will gain a complete understanding of Passport's base model product offering. If a City within Region 14 wishes to purchase

Passport's product, or learn more about the different tiers available, they will can either schedule a demo from the website or contact Passport's sales team directly. The Sales team will walk the City through the sales process and will send a contract over to the City the same day, if desirable. Once a contract is signed, the City will be assigned a Client Success Team made up of a Client Success Manager, Project Manager, and Product Support Specialist and begin to implement the product.

Describe your company's Customer Service Department.

A pillar of the Passport philosophy is to provide excellent and continued support and service to its clients. That belief is ingrained in every detail of the partnership between Passport and the City, from developing all software in-house, to creating a dedicated team to meet the needs of each client for the duration of the relationship. The City's dedicated Client Success Manager (the "CSM") will be responsible for training and handling enterprise questions for the City. The CSM will also train all City administrators on how to use the system, how to answer commonly asked questions, how to report issues, and how to get the most out of this partnership. After the product launches, the CSM will be the main point of contact for the City, sitting on the intersection of operations and software development. Throughout the partnership, if there is any feedback that the City wishes to deliver, the CSM will be the appropriate channel.

After launch, the CSM will speak with the City on a monthly basis, at a minimum, to fully understand the state of affairs. During these calls, the CSM will also impart any roadmap updates or new features that may be beneficial to the City. Once a quarter, the CSM will conduct a system review with the City to ensure that the product meets or exceeds the needs of the City. Passport positions its CSMs to be the best resource for any City not only on all things Passport, but all things related to enforcement.

To address any critical problems or triaging any issues, the City will also have access to a dedicated Product Support Specialist (the "PSS"). The PSS is trained in solving most technical problems that the City may encounter and for any problem that is outside the scope of their training, the PSS will liaise with the software engineer that built the system. Any issues will be addressed immediately and should be resolved within 24 hours of notice.

Parker Support

Passport supplies a variety of support through the application, website, and and telephone support. Parkers will have unlimited access to parking history and self help in the form of FAQs through the website and application. Additionally, Passport will provide live agent support from 8am-9pm EST Monday-Saturday and 12pm-9pm EST on Sundays. Outside of those hours, the parker will be able to call a dedicated call center, which will answer basic questions related to the application and flag any more serious issues to be handled by a Passport Customer Support representative the next day.

Passport strives to create an intuitive application that ought to reduce the number of technical support representatives required. As an example, Passport technical support has fielded only 75 calls for the City of Victoria, B.C. in the first 10 months of deployment. While Passport is able to handle multiple calls at once, this is rarely necessary.

Green Initiatives

As our business grows, we want to make sure we minimize our impact on the Earth's climate. We are taking every step we can to implement innovative and responsible environmental practices throughout NCPA to reduce our carbon footprint, reduce waste, energy conservation, ensure efficient computing and much more. To that effort we ask respondents to provide their company's environmental policy and/or green initiative.

Passport's solution is a cloud-hosted SaaS product, which requires no infrastructure to function properly. However, Passport understands that most cities are not yet ready to switch to a "mobile only environment," so Passport's solution is typically implemented in conjunction with existing infrastructure. Using both a traditional payment option, such as a meter or kiosk, in addition to Passport's mobile payment solution lessens the amount of wear and tear on the Agency's current infrastructure, extending the time between replacing hardware. Implementing mobile payments for parking also cuts out the need for paper receipts from kiosks, by pushing all parking data in real time to parking enforcement officers and also capturing it in the backend system for future use by Agency administrators.

All receipts and documentation are provided electronically, as emails or within the application for review. All agency reporting is also provided in OpsMan, as digital reporting, using email updates and pushing information between devices. The Agency will not require the use of any paper or related resources to gain the full benefit of this system.

Passport was recently featured in Forbes's "Clean Technology is Good Business" article (see pg. 100). The article looked at the need for businesses and municipalities to focus on promoting clean energy solutions as a strategy for growth and providing sustainable options to consumers. Passport is committed to providing solutions which create a more sustainable mobility environment, while delivering a best in class solution.

Additionally, Passport is committed to improving the world we live in. As such, it incorporates environmentally safe practices into its daily operations. Passport maintains a recycling program of office paper, hard and soft plastic, glass containers, cardboard boxes, and aluminum cans.

Vendor Certifications



PAYMENT CARD INDUSTRY DATA SECURITY STANDARD

Compliance Certificate

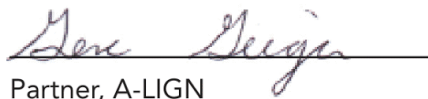
This is to certify that A-LIGN has validated Passport Parking, Inc.'s compliance with the Payment Card Industry Data Security Standard ("PCI DSS") version 3.1.

On-site testing was performed in accordance with the guidance provided by the Payment Card Industry Security Standards Council ("PCI SSC") to determine that payment card data stored, processed or transmitted by Passport Parking, Inc. was secured in accordance with the requirements of PCI DSS.

ROC date: September 28, 2016

AOC date: September 28, 2016

Issued by:


Partner, A-LIGN

Conditions of Use:

- This certificate is evidence of work performed by A-LIGN for the certificate holder and was not created by or required by the PCI SSC.
- This certificate is valid for one year from the Compliance Date.
- This certificate was issued at a point in time and does not guarantee or represent future compliance with the PCI DSS or the security of payment card data.
- This certificate does not warrant or guarantee to any party that the certificate holder is not susceptible to a data breach that may impact the security, confidentiality and integrity of the payment card data. As such, A-LIGN will not be liable to any party in the event of a breach.

Passport

November 2, 2016

Re: PassportParking, Inc. SSAE 16 Examination

To Whom It May Concern:

PassportParking, Inc., is subject to an SSAE examination annually. Passport's last complete examination was performed for the period of January 2015- November 2015. A-LIGN, an independent accounting and auditing firm performed the examination in compliance with SSAE 16 principles.

On October 15, 2016, A-LIGN began their auditing process for the previous 12 months. As of today's date, to the best of our knowledge, there have been no significant changes in the internal controls of PassportParking, Inc., which were described in the previous SSAE 16 report that could adversely affect such internal controls. Additionally, there have not been any significant deficiencies or material weaknesses in such internal controls that management is aware of.

This letter relates solely to the Client and may not be relied upon by any other entity.

Sincerely,



Brad Powers
CTO
Passport Parking, Inc.

1300 South Mint Street, Suite 200
Charlotte, NC 28203
Tel: 704.837.8066 Fax: 888.804.1783
www.passportinc.com

* Please see the appendix for an attached copy of Passport's most recent SSAE 16 Report.

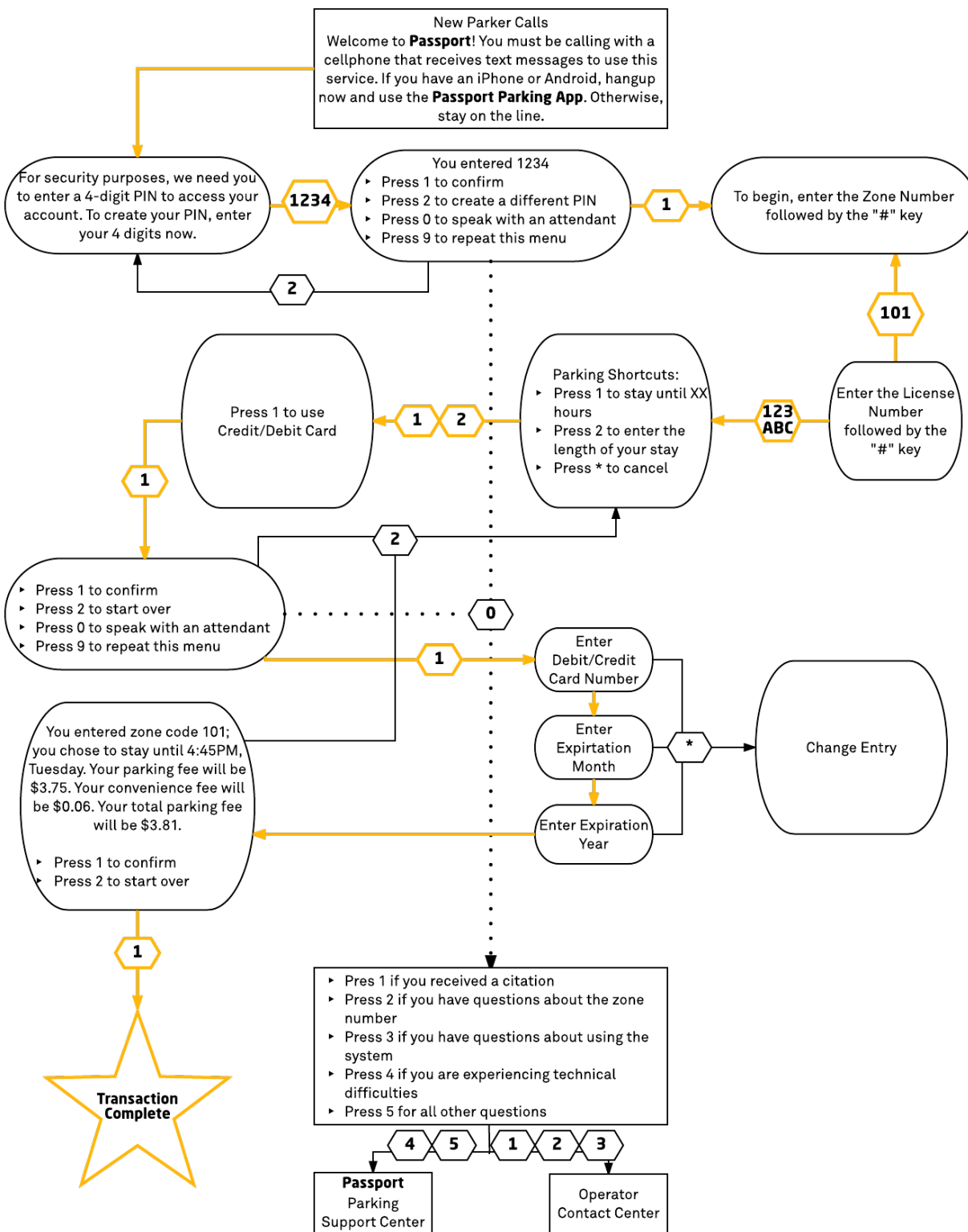
Products and Services/Scope

Respondent shall perform and provide these products and/or services under the terms of this agreement. The supplier shall assist the end user with making a determination of their individual needs.

The following is a list of suggested (but not limited to) categories. List all categories along with manufacturer that you are responding with:

- **Payment Options - The mobile payment for parking system must have the following payment options:**
 - Mobile Payment System (IVR) *Comply.*
 - Pay by mobile application *Comply.*
 - Pay by web *Comply.*
- **Mobile Payment for Parking System (IVR) - The vendor must provide an IVR system with the following requirements:**
 - Users can call a toll free or local number. *Comply.*
 - The system recognizes the user (account) based on the incoming number. *Comply.*
 - One account can be associated with multiple landline or cellular phone numbers. *Comply.*
 - The IVR system must recognize use inputs by touch tones and speech. *Comply.*
 - The IVR system must have menu options and dialog, including:
 - **Begin parking - One account can hold multiple vehicles (license plate numbers). The system must allow the user to choose a vehicle if multiple vehicles are on the account. *Comply.***
 - **Extend parking - The system must have the ability to restrict extensions that are beyond the maximum length of stay. The system must have the ability to reject purchases on the same block for a set amount of time after a maximum purchase. *Comply.***
 - **Sign up as a new user. *Comply.***
 - If the user selects the option to begin parking, the system must:
 - **Prompt for a meter/block/zone ID. *Comply.***
 - **Query the parking system inventory to confirm that parking is permitted at the current time. *Comply.***
 - **Prompt for the time to park - The system must have the ability to impose a minimum time purchase. The system must have the ability to restrict purchases to increments of time. The system must reject an entry greater than the length of stay. *Comply.***
 - **Confirm that the purchase is complete. *Comply.***
 - **Prompt whether to remind the user that the parking session is set to expire with an automated SMS or email. *Comply.***
 - **Prompt the number of minutes before the expiration to send the reminder. *Comply.***

- If the user selects the option to extend parking, the system must:
 - Verify that there is a currently active parking session. **Comply.**
 - Prompt for the time to extend. **Comply.**
 - Confirm that the extension is complete. **Comply.**



- **Pay by Mobile Application - The vendor must provide smart phone applications with the following requirements:**
 - **Mobile applications need to support existing and new Android, iOS, BlackBerry, and Windows Mobile 7 versions, in addition to a browser version. *Comply.***
 - **Applications can be downloaded from the Android Marketplace or Apple Store, or equivalent. *Comply.***
 - **Applications can be downloaded or redirected from the vendor's website. *Comply.***
 - **Applications can be downloaded or redirected from NCPA's website. *Comply.***
 - **When a user launches an application, it must:**
 - **Prompt the username and password (for registered users). The application must have the ability to save the username and password to expedite future logins. *Comply.***
 - **Provide an interface to sign up as a new user. *Comply.***
 - **When logging in, the application must have the following options, with identical functionality to that of the IVR system:**
 - **Begin parking via GPS, QR Code, NFC, or manual entry. *Comply.***
 - **Extend parking. *Comply.***
 - **Check account balance. *Comply.***
 - **Recharge account with credit card on file. *Comply.***
 - **In addition, the application must also have the following functionality:**
 - **Manage account: add, remove, or edit a credit card. *Comply.***
 - **Manage account: add, remove, or edit a vehicle. *Comply.***
 - **Manage account: select a primary vehicle. *Comply.***
 - **Manage account: add funds to the account from a credit card. *Comply.***
 - **Transaction history showing all paid parking sessions by: Date and time, Duration, Rate, Total amount, payment method, License plate number, Meter/block/zone ID. *Comply.***
 - **For new or extended parking sessions, the application must:**
 - **Remind the customer that the session is about to expire with a push notification on the phone. The user must be able to turn this feature on or off. *Comply.***
 - **The application must have industry-level standards to encrypt and secure credit card and other personal data. *Comply.***

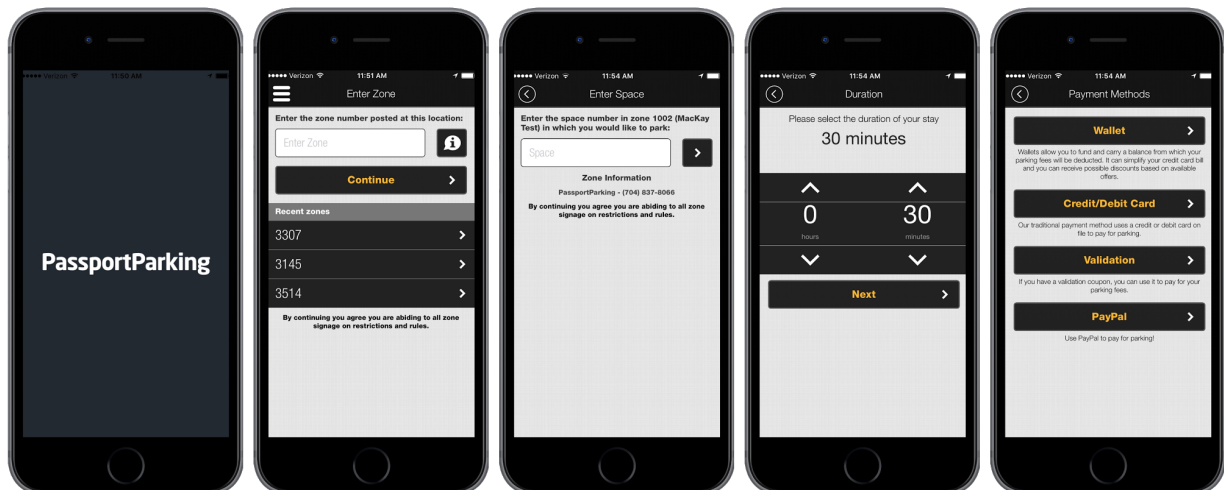
Passport will provide a mobile parking application to pay for and extend parking sessions for the City. This native application will be available on all Android and iOS smartphones. Passport's app is not supported by Windows or Blackberry operating systems as they only account for 3% of the smartphones in the US. However, Blackberry's newer models do support Android applications and are able to run Passport's applications.

To account for those parkers who do not own an Android or Apple device, Passport's Mobile Payment for Parking platform ("MPP") is also available as a web app. The web app is accessible by any device that has access to the internet. To enhance this experience, the web application and the payment webpage are both optimized for mobile use.

Passport is currently available in both English and Spanish. Passport's system will automatically detect the language settings on the parker's phone and automatically select to run the corresponding version of the application. If the phone's language is set to something other than English or Spanish, the application will default to English.

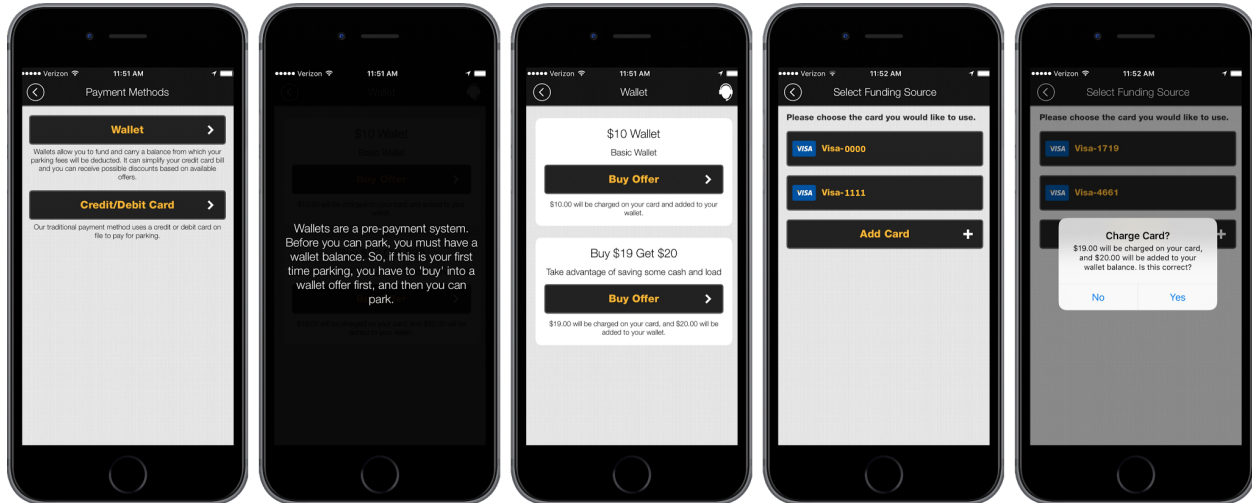
Passport's mobile payment platform is the simplest, most robust mobile payment solution on the market. As the only provider using progressive profiling for registration, parkers register using only information needed at that specific point in the process, in contrast to populating an entire profile at sign up. For example, Passport's platform only requires one piece of identifying information (phone number, email, or public Facebook profile) and a valid credit or debit card to pay for parking; payment card information is only requested once a transaction is initiated, in an effort to streamline the registration and avoid 'hang ups.'

Passport understands that most adopters of the system do so as they are about to purchase their first parking session, as opposed to planning in advance; therefore, Passport focused on making the registration process as quick and easy as possible. With just two clicks, Parkers can create their account using their public information on Facebook. Facebook login does not give Passport access to any other information or let Passport post to a parker's Facebook account. If a parker registers the first time they use Passport, each subsequent session will only require they enter a four digit pin.

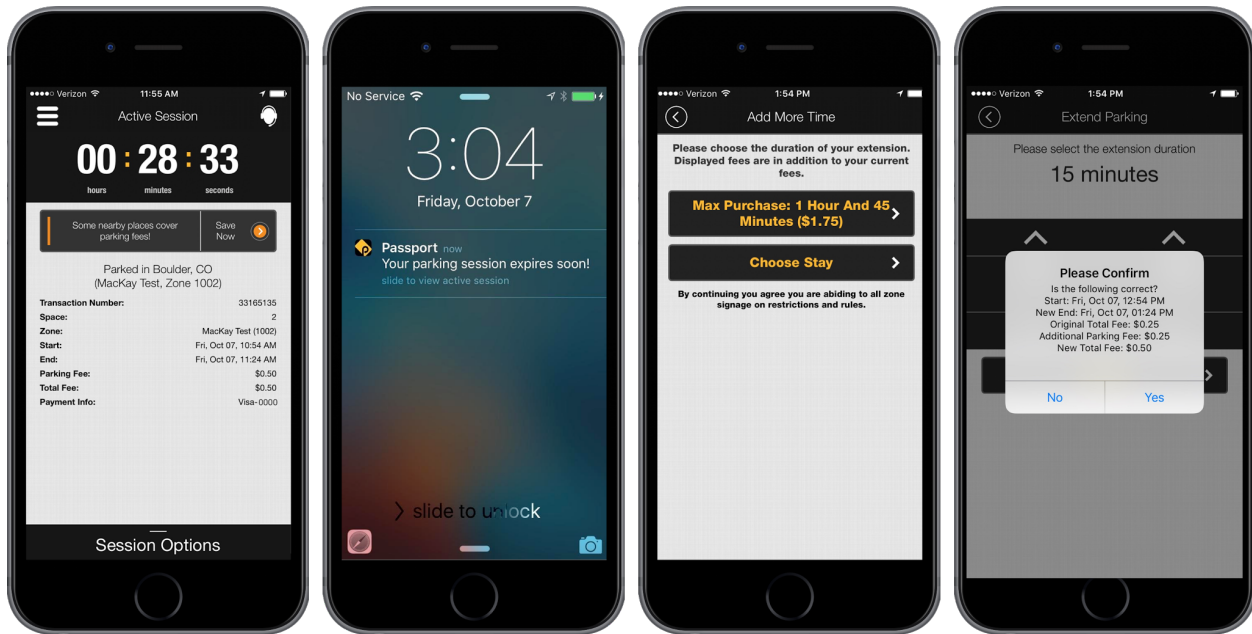


Passport provides parkers with more options to pay for parking than traditional meters, which only accept coins, or even smart meters, which only accept credit cards and coins. Passport accepts payment in the form of debit and credit cards, a digital wallet, PayPal

accounts (including ACH payments), merchant validation, and corporate accounts. Passport makes it easy for parkers to use its system, regardless of their current financial situation. Additionally, by adding merchant validation to the system, the City is able to incorporate local businesses to the parking initiative, further strengthening the community.

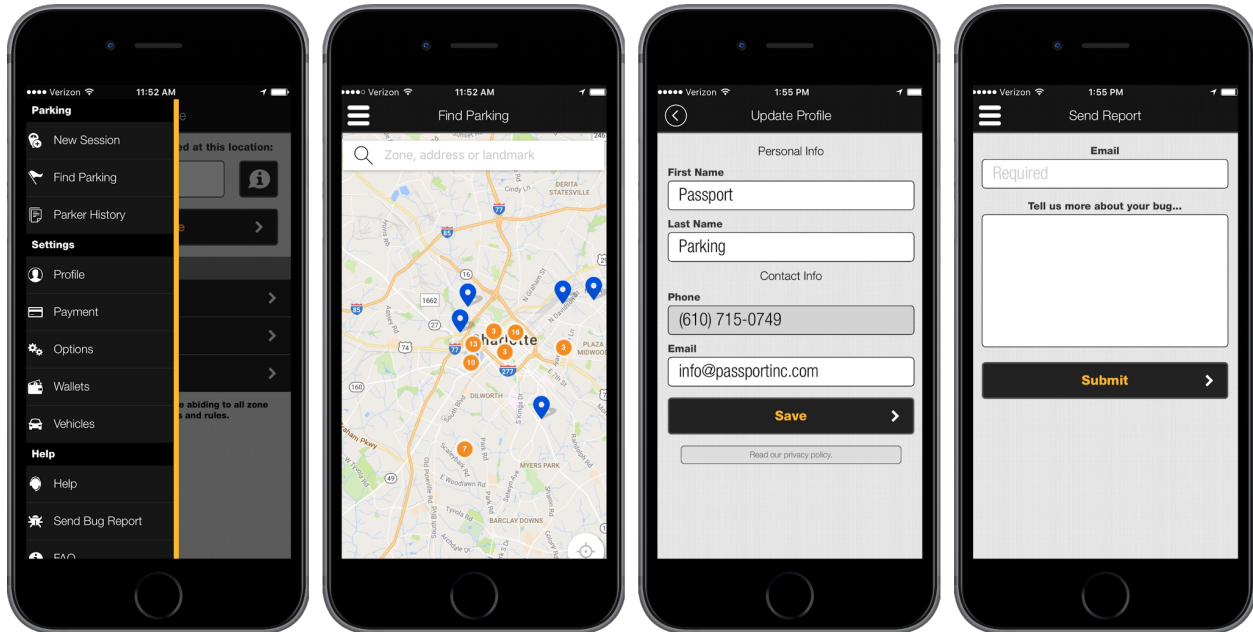


After initiating a parking session, the parker is free to go about their day without concern for their parking session. When the session is 15 minutes away from expiring, the parker will be notified by their phone. Upon receiving this notification the parker has three options: (1) return to their car, (2) ignore the notification and risk a ticket, or (3) extend their parking remotely. Using the same method that the parker used to initiate the session, the parker may easily extend their parking session. The City can control how many times and for how long the parker may extend their time, ensuring that this convenience is not abused. The parker's credit or debit card is not charged until the end of the session, meaning that **extending a parking session only incurs a single charge** for the parker and a single merchant processing fee for the City.



Credit card numbers are encrypted with AES-256 with a rotating encryption key. All information is stored in an isolated card storage database per best practices. All transactions are tokenized at the point of transaction, meaning that credit card information is encrypted from the time a user inputs data into the system. Passport's server then reads the tokenized information and sends the proper data to the merchant processor. Tokenization reduces the risk of credit card fraud in the event of a breach since there are no actual credit card numbers every stored or transferred in the system.

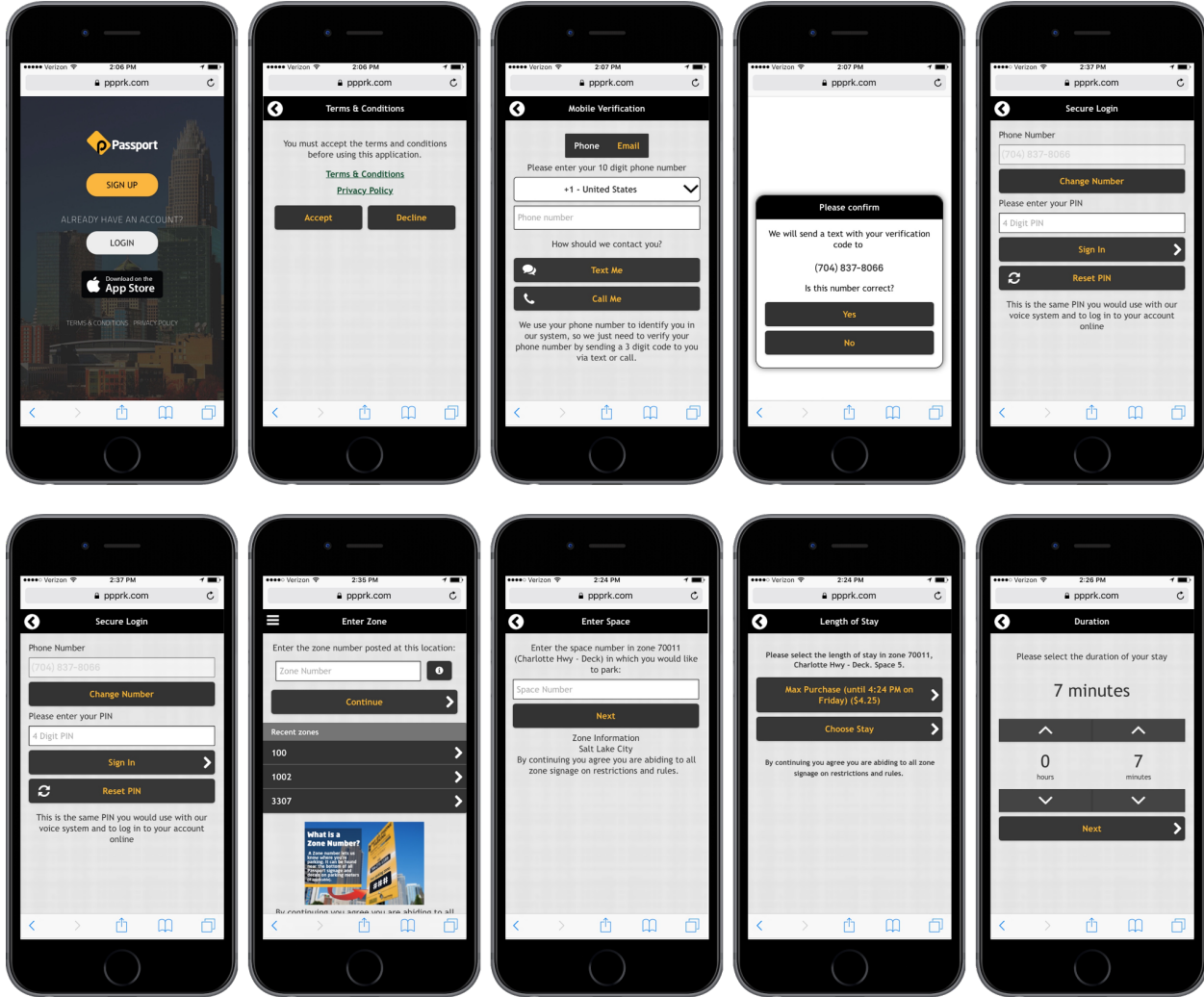
Registered parkers will be able to manage their entire account from either the mobile application or the Passport website. Passport's database is housed in a cloud, meaning that the parker will have real-time access to their account, regardless of whether they access it from the website or application. The parker will log into their account with their phone number, email address, or Facebook profile and the 4-digit PIN created at registration. Once they have accessed their account, the parker will be able to see their full parking history, email receipts to themselves or third parties, change their vehicle, update their payment methods, and delete their account.



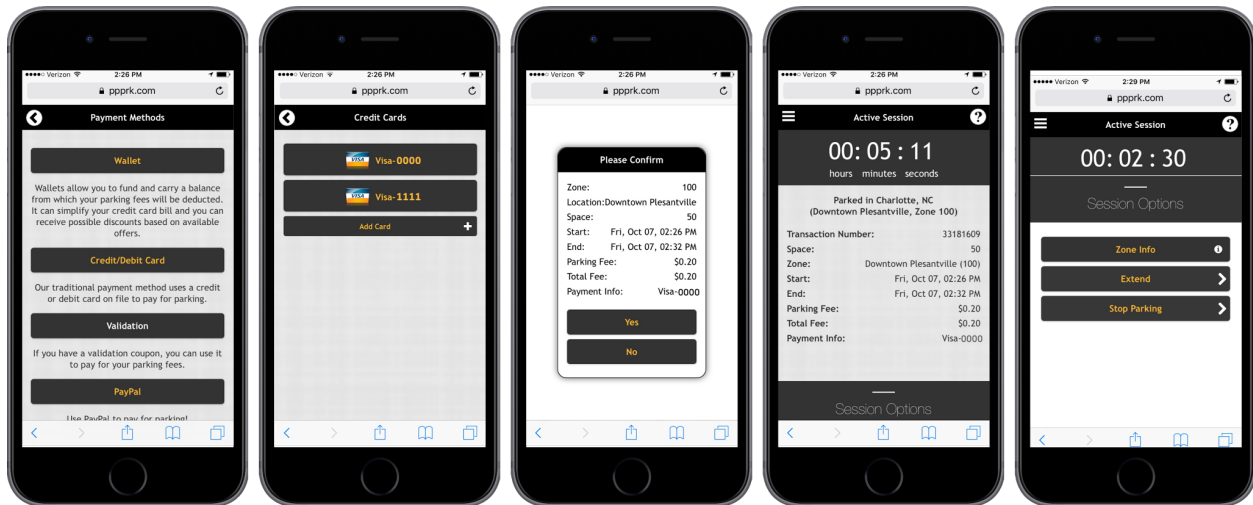
- **Pay by Web - The System must provide a website with the following requirements:**
 - **Participant must have the option to have a customized website (e.g., <http://www...com/NCPA>) or use the participant's standard website. **Comply.****
 - **Support desktop and mobile browsers. **Comply.****
 - **When a user launches the website, it must:**
 - **Prompt for the username and password (for registered users). The website must have the ability to save the username and password locally on the device (PC or phone) to expedite future logins. **Comply.****
 - **Provide an interface to sign up as a new users. **Comply.****
 - **Upon logging in, the website must have the following options, with identical functionality to that of the mobile application:**
 - **Begin parking. **Comply.****
 - **Extend parking. **Comply.****
 - **Check account balance. **Comply.****
 - **Recharge account with credit card on file. **Comply.****
 - **Manage account. **Comply.****
 - **Transaction History. **Comply.****
 - **The application must have industry-level standards to encrypt and secure credit card and other personal data. **Comply.****

Passport's service offering includes a parker-centric, mobile-optimized website, which allows registered parkers to manage their entire account and purchase parking. Passport's database is housed in a cloud, meaning that the parker will have real-time access to their account, regardless of whether they access it from the website or application. The parker

will log into their account with their phone number, email address, or Facebook profile and the 4-digit PIN created at registration. Once they have accessed their account, the parker will be able to initiate a parking session, see their full parking history, email receipts to themselves or third parties, change their vehicle, update their payment methods, and delete their account.



Credit card numbers are encrypted with AES-256 with a rotating encryption key. All information is stored in an isolated card storage database per best practices. All transactions are tokenized at the point of transaction, meaning that credit card information is encrypted from the time a user inputs data into the system. Passport's server then reads the tokenized information and sends the proper data to the merchant processor. Tokenization reduces the risk of credit card fraud in the event of a breach since there are no actual credit card numbers every stored or transferred in the system.



- **Account Management - The system must provide multiple ways for a user to manage his or her mobile payment for parking system account. This section contains the requirements for account management.**
 - All interfaces for account management must have industry-level standards to encrypt and secure credit card and other personal data. **Comply.**
 - Users must be able to create and manage accounts through a website (desktop and mobile versions), mobile applications, IVR system, and through a live customer service representative. **Comply.**
 - Users must be able to create new accounts with the following parameters:
 - Username (email). **Comply.**
 - Password. **Comply.**
 - Phone Numbers. **Comply.**
 - License Plate Numbers. **Comply.**
 - Credit Card Number. **Comply.**
 - Billing Name and Address. **Comply.**
 - Users must be able to access a history of all transactions made on an account and be able to view reports and receipts showing:
 - Date and time. **Comply.**
 - Duration. **Comply.**
 - Rate. **Comply.**
 - Total amount. **Comply.**
 - Payment method. **Comply.**
 - License Plate number. **Comply.**
 - Meter/block/zone ID. **Comply.**
 - Users must be able to configure reminders for session expirations, including the ability to:
 - Enable or disable reminders. **Comply.**
 - Configure the type of reminder (SMS or email). **Comply.**

- **When funding an account, the system must have the ability to impose a minimum charge/recharge amount.** *Comply.*
- **The system must have the ability to automatically notify a user and/or recharge the account if the account balance falls below a certain amount.** *Comply.*
- **The system must be able to support both pay per transaction and pay out of a "mobile wallet" models.** *Comply.*
 - **The participant must explain any difference in cost between these two models.** *Confirmed.*

Passport's Mobile Payment for Parking platform ("MPP") will provide the parker with an intuitive user experience, which will significantly improve the parking experience. MPP is a native application, which is accessible on all Android and iOS smartphones. Other smartphone operating systems, such as Windows and older Blackberry models only account for 3% of smartphones in the US and do not support MPP.

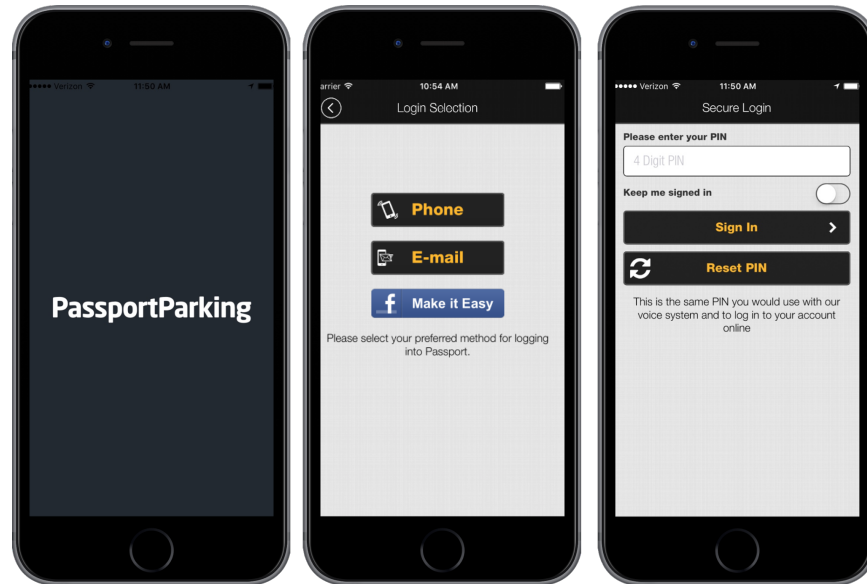
To account for those parkers who do not own an Android or Apple device, MPP also available via the web app, which is accessible by any device that has access to the internet. To enhance this experience, the web application and the payment webpage are both optimized for mobile use.

In addition to the application and mobile-optimized website, Passport offers an IVR and SMS system to enable mobile payment of parking. With IVR, parkers will call a local number and respond to commands using touch tone prompts. The very first session started by a parker will end with a prompt to create a PIN. Thereafter, the system will recognize the phone number and request the PIN, thereby recalling all payment and vehicle information. Similar to the IVR system, parkers can register for and begin parking sessions via SMS (text) messages. The parker will respond to prompts via SMS, including zone and space numbers, as well as payment information.

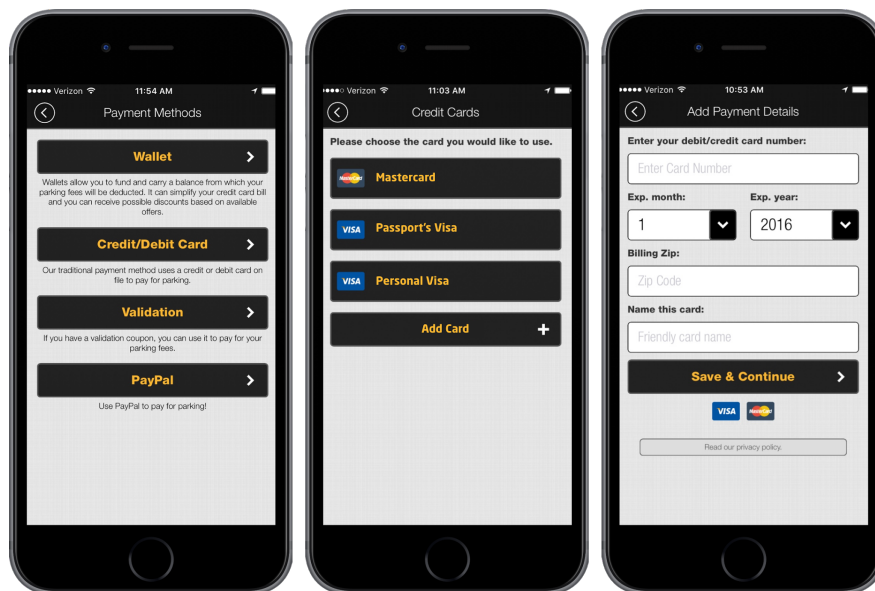
Passport's mobile payment platform is the simplest, most robust mobile payment solution on the market. As the only provider using progressive profiling for registration, parkers register using only information needed at that specific point in the process, in contrast to populating an entire profile at sign up. For example, Passport's platform only requires one piece of identifying information (phone number, email, or public Facebook profile) and a valid credit or debit card to pay for parking; payment card information is only requested once a transaction is initiated, in an effort to streamline the registration and avoid 'hang ups.'

Passport understands that most adopters of the system do so as they are about to purchase their first parking session, as opposed to planning in advance; therefore, Passport focused on making the registration process as quick and easy as possible. With just two clicks, Parkers can create their account using their public information on Facebook. Facebook login does not give Passport access to any other information or let Passport post to a parker's

Facebook account. If a parker registers the first time they use Passport, each subsequent session will only require they enter a four digit pin.

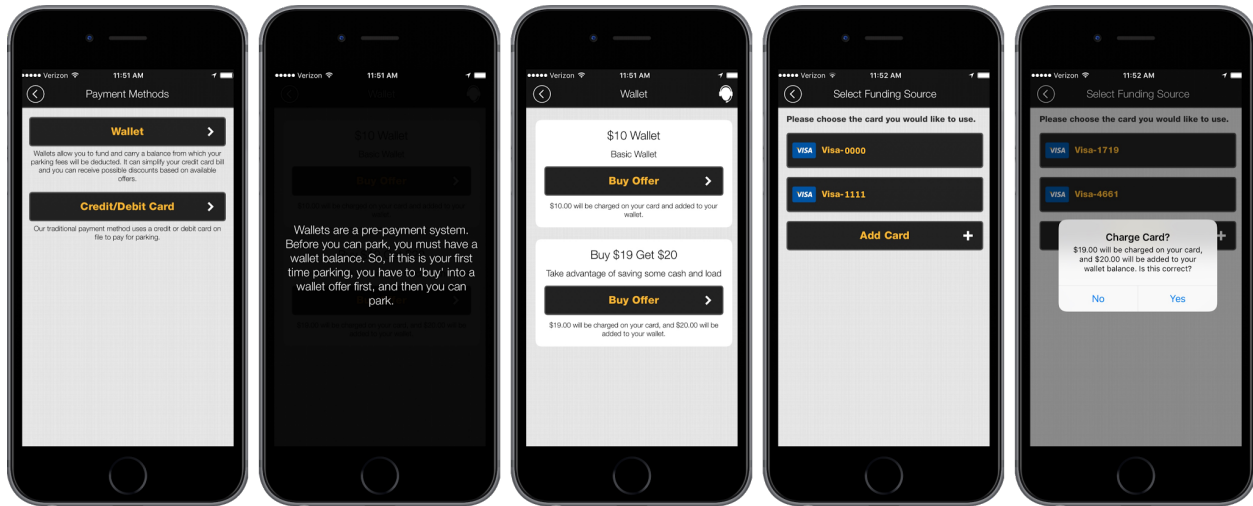


Passport provides parkers with more options to pay for parking than traditional meters, which only accept coins, or even smart meters, which only accept credit cards and coins. Passport accepts payment in the form of debit and credit cards, a digital wallet, PayPal accounts (including ACH payments), merchant validation, and corporate accounts. Passport makes it easy for parkers to use its system, regardless of their current financial situation. Additionally, by adding merchant validation to the system, the City is able to incorporate local businesses to the parking initiative, further strengthening the community.



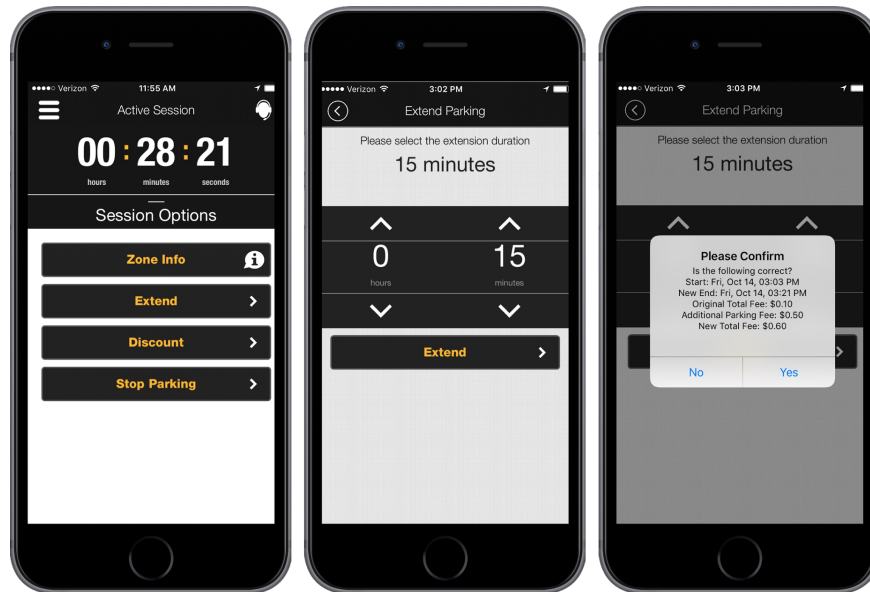
Passport's Digital Wallet allows parkers to pre-load a larger sum of money onto their account, which will then be debited against every time the parker pays for a transaction. The

Digital Wallet is dually advantageous as it saves the City money on merchant processing fees and it allows the parker to avoid multiple small transactions for parking sessions. The City can choose to offer the wallet as an option or may require one. By requiring a wallet with a minimum, the City will realize increased savings in merchant processing fees almost immediately.



In cities where there is a wallet option, Passport has seen a utilization split as high as 71% favoring the wallet to individual credit card transactions. With that many parkers choosing to use the wallet, it is reasonable for a city to require a wallet without damaging the public's adoption of the app. Several cities have taken this approach, including Chicago, which has realized more than \$2,000,000 in savings since deploying the wallet-only feature.

After initiating a parking session, the parker is free to go about their day without concern for their parking session. When the session is 15 minutes away from expiring, the parker will be notified by their phone. Upon receiving this notification the parker has three options: (1) return to their car, (2) ignore the notification and risk a ticket, or (3) extend their parking remotely. Using the same method that the parker used to initiate the session, the parker may easily extend their parking session. The City can control how many times and for how long the parker may extend their time, ensuring that this convenience is not abused. The parker's credit or debit card is not charged until the end of the session, meaning that extending a parking session only incurs a single charge for the parker and a single merchant processing fee for the City.



Passport's service offering includes a parker-centric, mobile-optimized website, which allows registered parkers to manage their entire account and purchase parking. Passport's database is housed in a cloud, meaning that the parker will have real-time access to their account, regardless of whether they access it from the website or application. The parker will log into their account with their phone number, email address, or Facebook profile and the 4-digit PIN created at registration. Once they have accessed their account, the parker will be able to initiate a parking session, see their full parking history, email receipts to themselves or third parties, change their vehicle, update their payment methods, and delete their account.

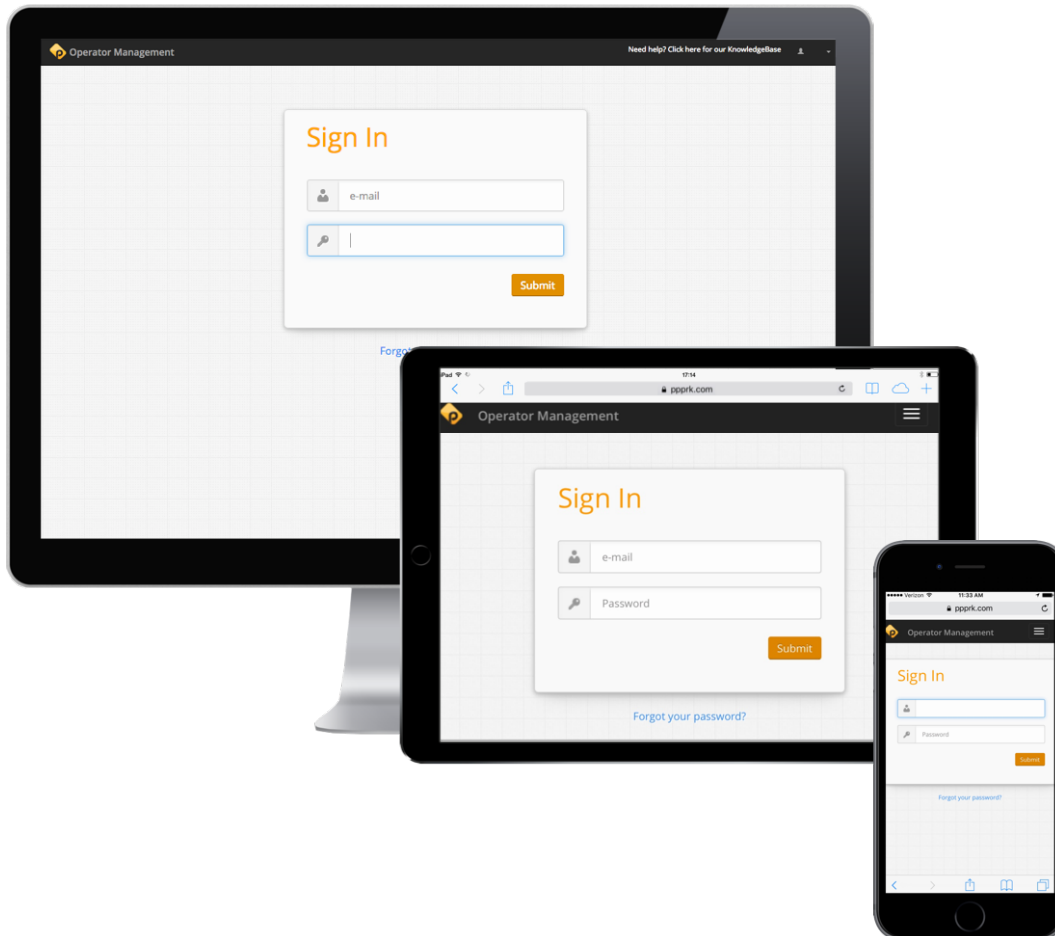
Administrator Requirements

- **Administrator Portal - The system must provide a website accessible only to designed system administrators. *Comply.***
 - **Customer service representatives must be able to create and manage user accounts. *Comply.***
 - **Customer service representatives must be able to activate or deactivate mobile payment system user accounts. *Comply.***
 - **Administrators must be able to run reports on transactions and accounts. *Comply.***

- Administrators must have an interface to query transactions for ticket adjudication purposes. **Comply.**
- Reporting - The system must provide reporting functionality to designated administrators of the system. These reports must include data on:
 - Transactions made by:
 - License plate number. **Comply.**
 - Phone number. **Comply.**
 - Username/account number. **Comply.**
 - Date and time. **Comply.**
 - Duration. **Comply.**
 - Rate. **Comply.**
 - Total amount. **Comply.**
 - Payment method. **Comply.**
 - License Plate number. **Comply.**
 - meter/block/zone ID. **Comply.**
 - Account sign ups. **Comply.**
 - Account charges/recharges. **Comply.**
 - The system must allow reports to be exported to:
 - Microsoft Excel. **Comply.**
 - Text Files. **Comply.**
 - Database flat files. **Comply.**
 - Direct connection with another database. **Comply.**
 - Reports must be available for viewing or downloaded within reasonable time. The participant must provide performance metrics on its reporting tool, with scenarios such as:
 - Number of new accounts per week. **Comply.**
 - Amount of transactions per day by meter/block/zone ID. **Comply.**
 - All transactions in a calendar year. **Comply.**
- Parking System Inventory - The system must have the option for a web-based tool to manage the inventory of the parking system. This section describes the requirements of the inventory management tool.
 - The inventory must hold information on each meter/block/zone, including its:
 - ID. **Comply.**
 - Address. **Comply.**
 - Status (active or inactive). **Comply.**
 - Rate. **Comply.**
 - Hours of operation. **Comply.**
 - Hours of restrictions. **Comply.**
 - Maximum length of stay. **Comply.**
 - Once a change is made to the inventory, the system must be either updated immediately or queued for update at a set time. **Comply.**

- **An administrator must be able to use the tool to manually update the attributes of a single meter/block/zone. *Comply.***
- **An administrator must be able to import a file to update the entire inventory. *Comply.***

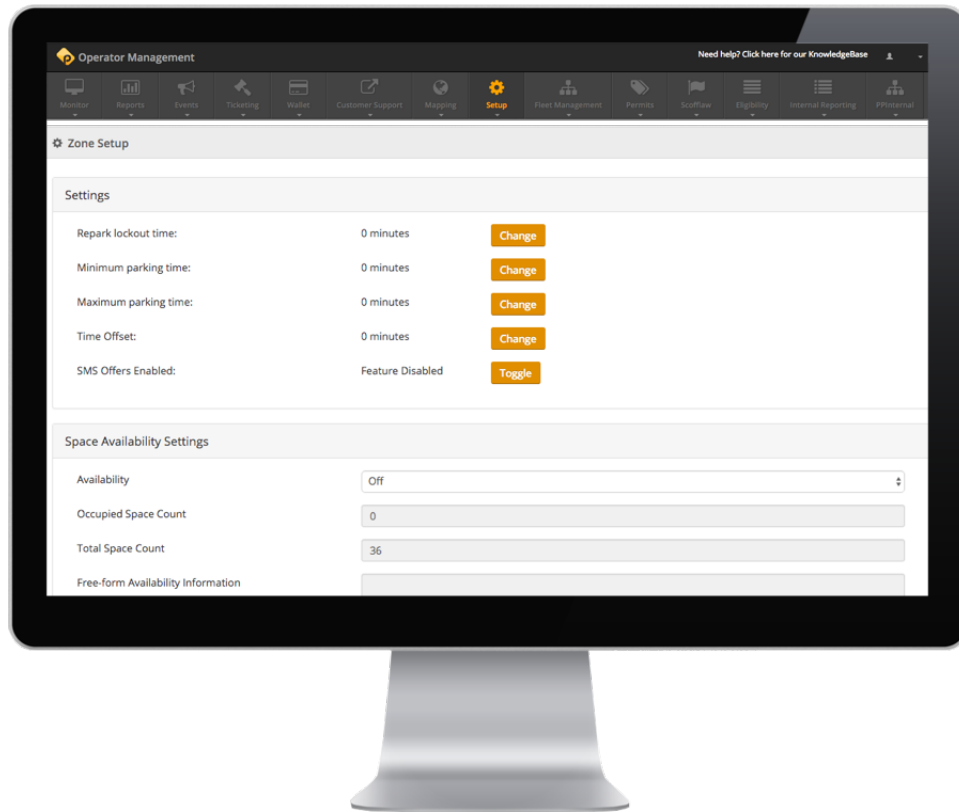
The brain of Passport's suit of products is its backend system, Operator Management ("OpsMan"). OpsMan puts all management and analytics tools into the hands of the the City administrator. OpsMan is accessible on any internet-connected device, is mobile-optimized for use on smartphones or tablets, and allows for an unlimited number of administrators.



System Configuration

Zone and Space Setup

During the implementation process, Passport will fully configure the City to have defined zones and spaces. During this process, the City's dedicated project manager will divide the City into zones, assign a unique number to each zone, and number the parking spaces (if space based).



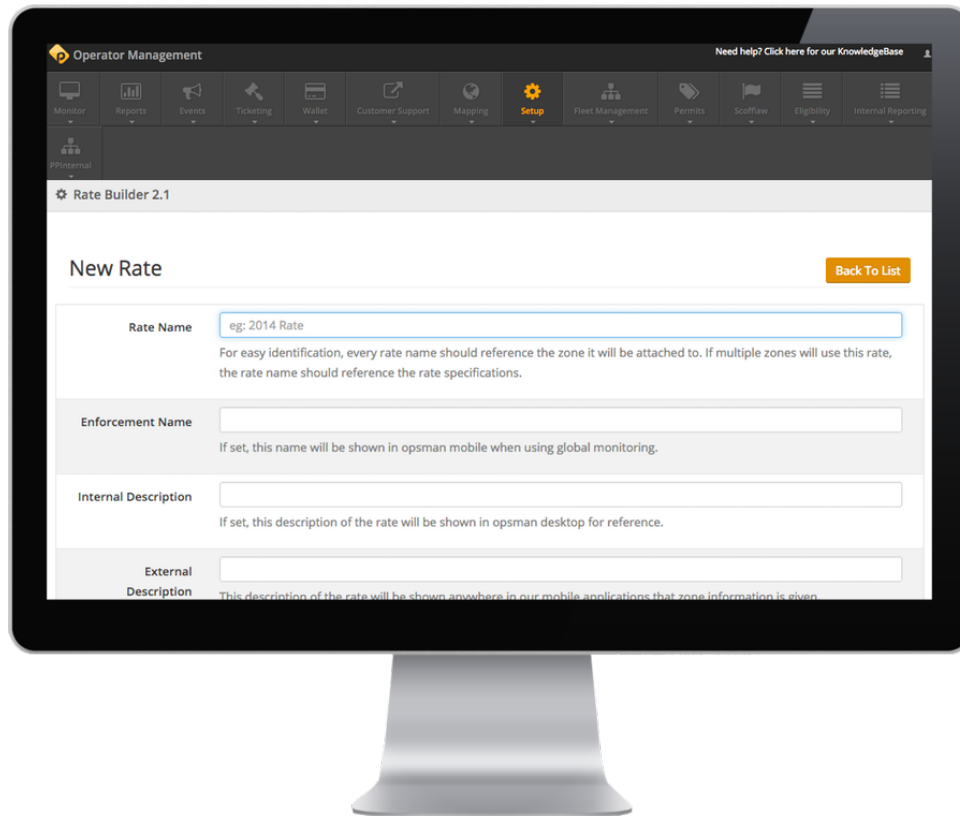
Integrations

Passport operates an open Application Programming Interface ("API"), which makes it much easier to integrate with other software providers. While Passport is implementing its product, it will also integrate with other necessary software to provide a seamless transition.

Rate Setup

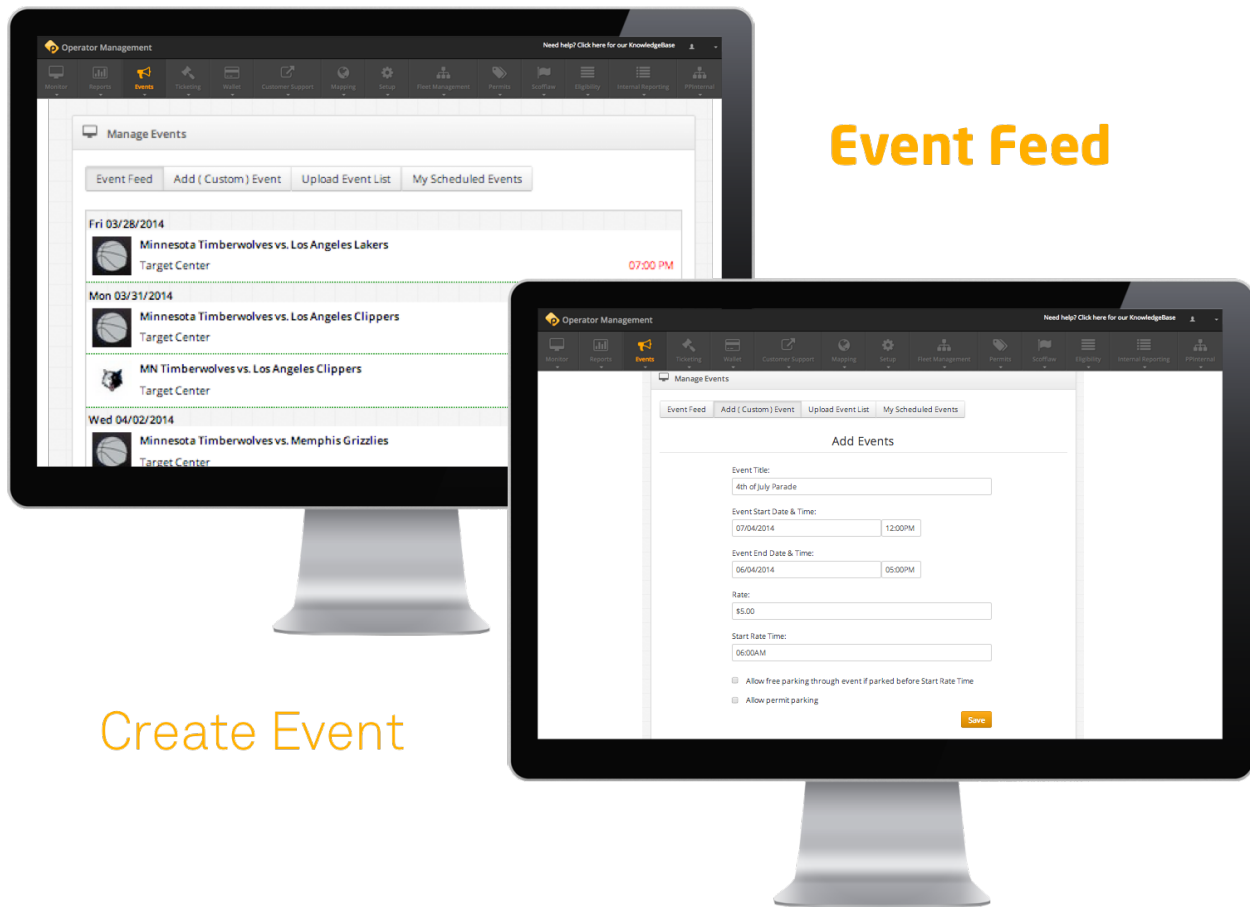
Initially, Passport will configure all rates within the City prior to launch. These rates will match what the City currently has in place. However, after launch, the City will be able to fully control the rate structure.

In OpsMan, the City administrator responsible for setting rates will navigate to the "Setup" tab and then select "Rates" from the dropdown menu. From here, the administrator will be able to add a new rate, delete a rate, or modify an existing rate. These changes can be set to either take effect immediately or at a scheduled time.



Event Rates

If there is a special event in the City, the City will be able to set special rates for specific lots. From the OpsMan dashboard, the administrator will navigate to the "Events" tab and select either "Manage Venues" or "Manage Rates." From this screen, the City will input information related to the event, including starting and ending date and time. The City will also have the option of make certain zones free during this time or accepting permits during the event. This information will update in real time to the Passport Mobile Payment app and OpsMan, giving all parkers and parking enforcement officers access to the most recent rates.



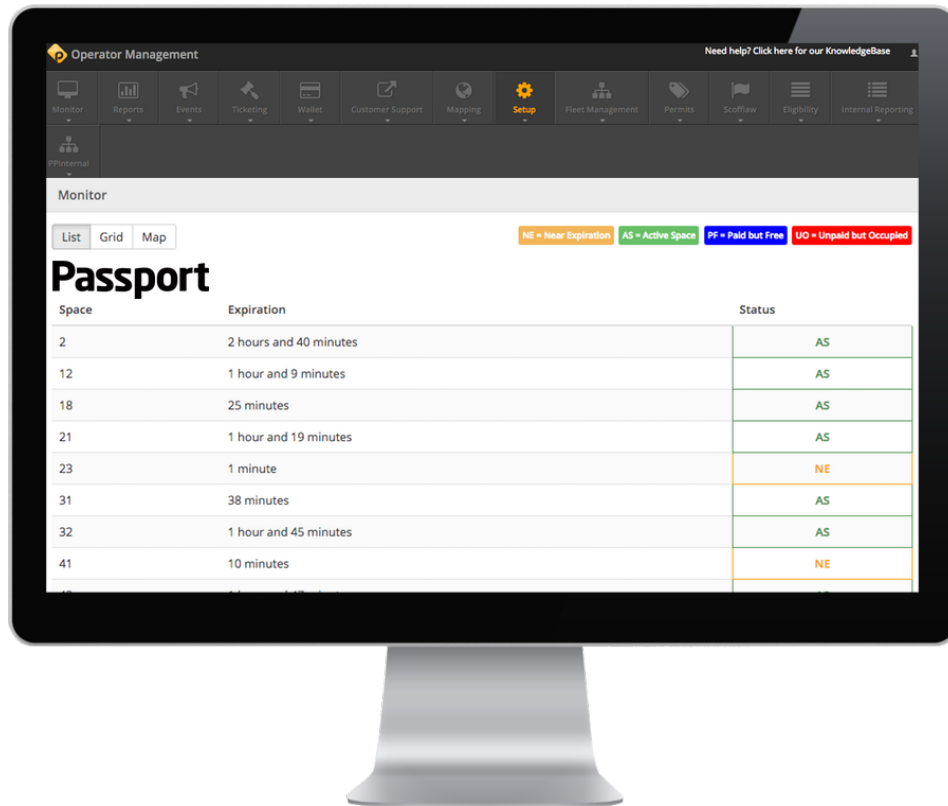
Event Feed

Create Event

System Transparency

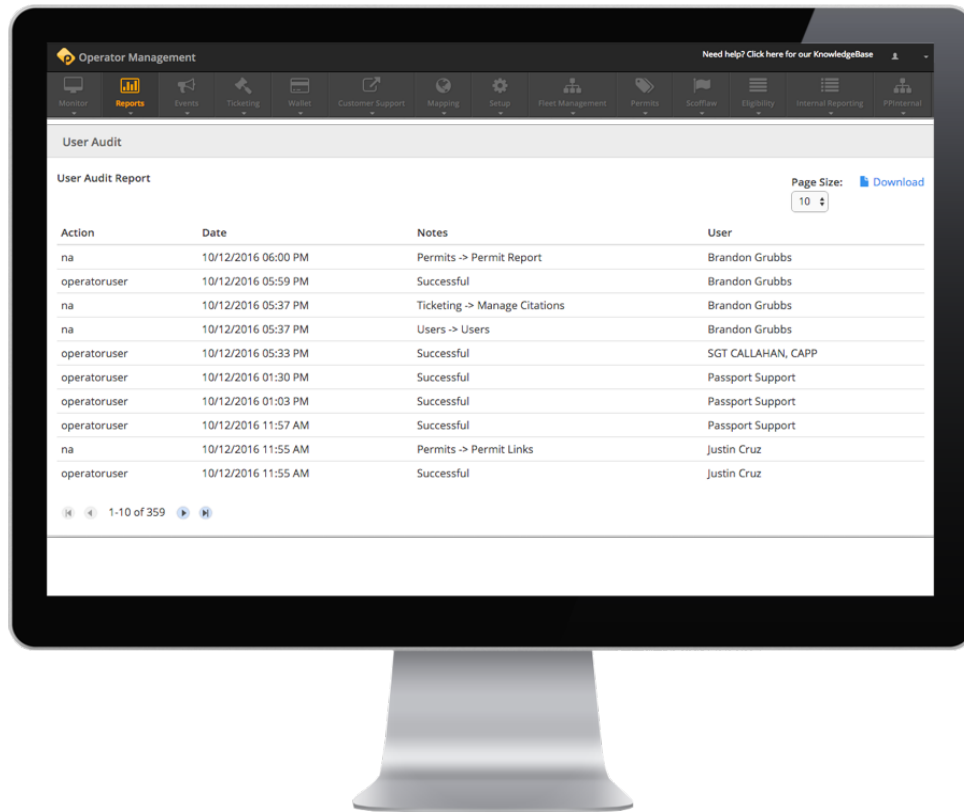
Live Monitoring

OpsMan gives the City complete insight into the entire parking system. An administrator will be able to watch a Live Feed of all transactions. Using the monitor feature, City administrators can see how many parking sessions are active, which sessions are about to expire, whether a space is occupied in a "free" zone, and whether a space is already expired.



Complete Control

OpsMan puts all of the control into the hands of the City. For all platforms, administrators will have the ability to update information including names, vehicle information, and LPNs. As an added layer of transparency, every adjustment made in OpsMan is time stamped with the username of the administrator making the adjustment as well a date and time.



Reporting

OpsMan aggregates data from all other platforms (Passport app, OpsMan Mobile, and RMCPay), allowing City administrators to access and analyze data in real time. OpsMan comes with certain predefined reports, but all data may be exported to Excel, giving the City even more control over management of the system. All reports can be manually run or scheduled to run in the future. Pre-scheduled reports can be set to run on a recurring or one-time basis.

Predefined Reports

OpsMan is configured to run reports on a myriad of topics and facets related to the entirety of the City's parking environment. In running these reports, the City may choose the time frame, being as broad as total transactions and as a specific as a given day. OpsMan will come with the following reports ready to be run on the following topics:

Mobile Payments for Parking

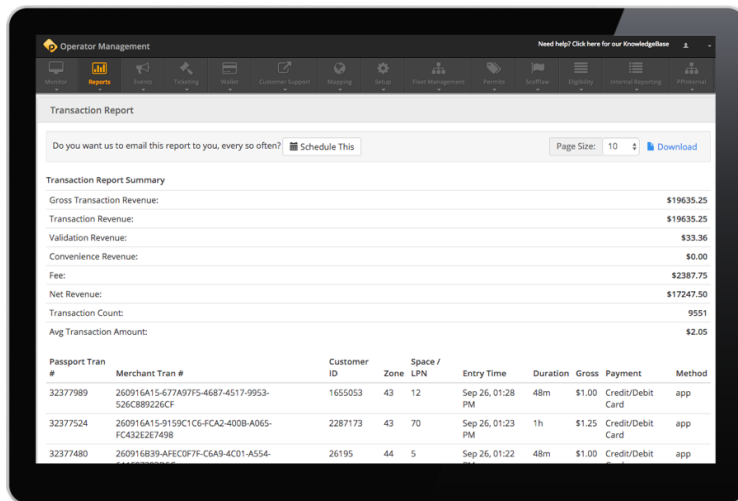
- | | | |
|----------------------------|---|---------------------|
| Financial Reporting | → | Transaction Report |
| | → | Daily Total Revenue |
| | → | Summary By Zone |
| | → | Wallet Summary |
| | → | Merchant Report |

- Void/Refund Report
- Declined Card Transactions
- Many more!

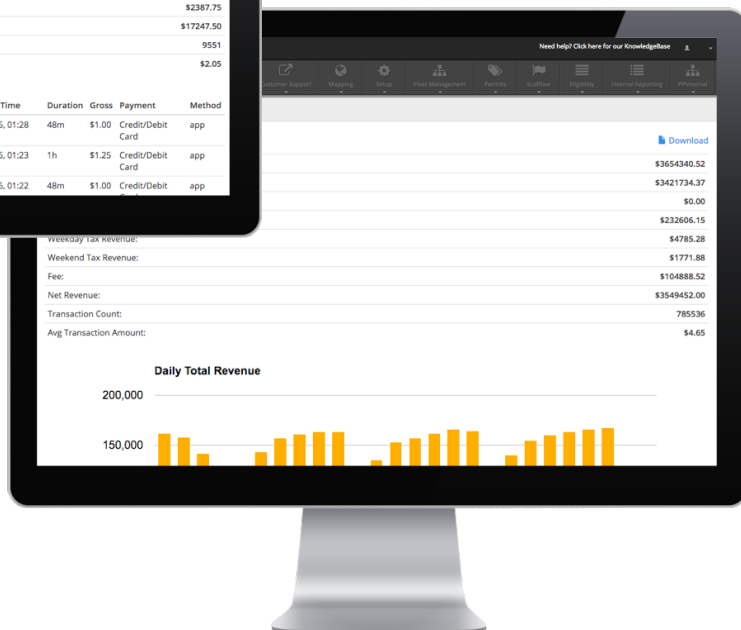
- Customer Reporting**
 - Individual Customer Report
 - Utilization by Space Number
 - User Report

- Events Reporting**
 - Events Summary

- Administrative Reporting**
 - Audit Reports
 - Suspended Account Attempts



Transaction Report



Daily Summary

Ad Hoc Reports

Aside from the predefined reporting, Passport will also work with the City to create custom reports. Whenever a custom report is generated for a specific City, that same report will be made available to all other clients. The following are the current custom reporting available in OpsMan:

- Payment Rates by Month,
- Payments by Platform,
- Suspended Parkers;
- Online Payments by Source, and

→ Passport continues to add to these reports.

Operator Management

Need help? Click here for our KnowledgeBase

Suspended Parkers

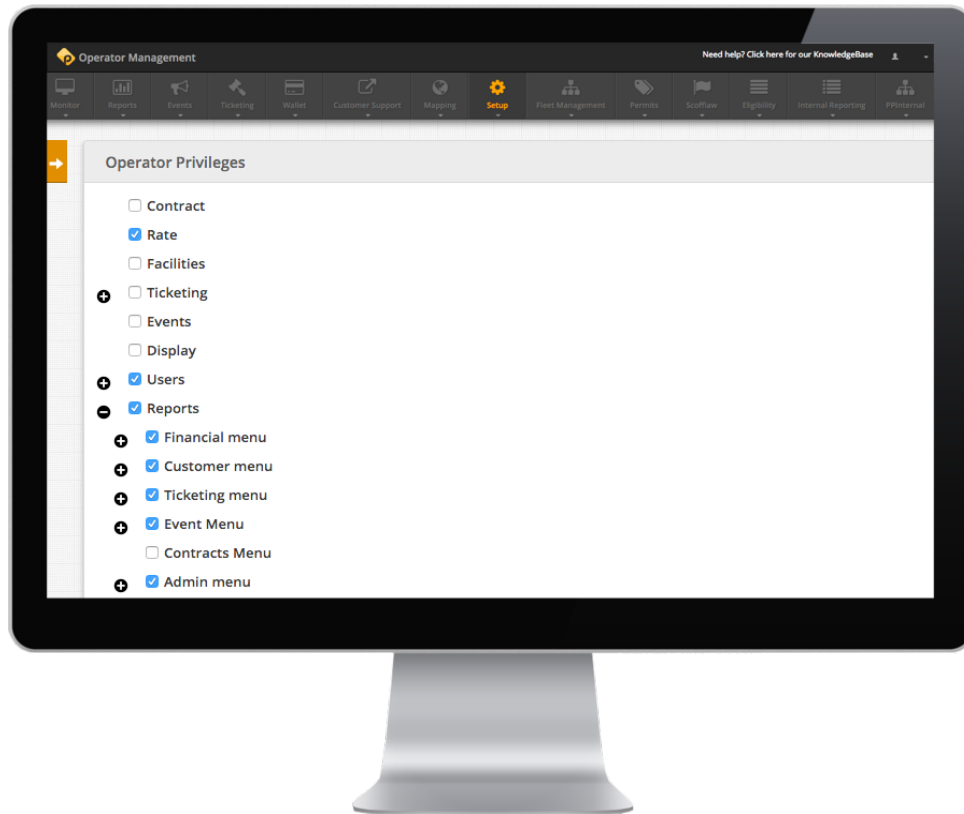
Report Details [Download](#) Page Size: 25

Id	Name	Phone	Balance	Suspended	Reason	Officer
169501	Mike Powers	(123) 456 - 7890	\$30.37	2014-06-27 13:15:01	Last \$50 wallet load was charged back to company as fraudulent transaction with a notation that the account was closed.	null
122185	Tom Danko	(123) 456 - 7890	\$102.17	2014-07-03 14:34:21	\$100 charge from 5/20/14 that was chargebacked and reversed was chargebacked again on 7/3/2014.	null
148723	Tiffany Weise	(123) 456 - 7890	\$16.42	2014-07-07 15:02:59	Charge from 6/6/14 charged back as fraudulent. Message from issuing bank says that account is closed.	null
168517	Lars Olivo	(123) 456 - 7890	\$12.00	2014-07-16 14:50:32	\$20 charge on 6/28/2014 was returned as fraudulent.	null
185702	Moyo Gutierrez	(123) 456 - 7890	\$25.72	2014-07-21 15:09:57	\$20 wallet load on 6/28/14 was charged back as fraudulent, no cardholder authorization.	null
145565	Nate Kim	(123) 456 - 7890	\$14.37	2014-07-24 13:31:10	Cardholder claims this is a fraudulent transaction even though she acknowledged to me on the phone that it was her card. She just doesn't like the wallet policy.	null
184548	Molly Mohler	(123) 456 - 7890	\$28.00	2014-08-04 13:46:37	Charge returned as fraudulent, no cardholder authorization.	null
177582	Mark Weber	(123) 456 - 7890	\$12.52	2014-08-05 12:30:54	\$20 wallet load on Visa 8377 charged back as fraudulent	null
124132	Kelsey	(123) 456 - 7890	\$18.25	2014-08-13	A \$60 wallet load on 5/20/14 was charged back as fraudulent.	null

The City will be able to export all data to Excel and run whatever queries they would like.

Limited Administrative Access

Knowing that different roles and administrators have different data needs, Passport created OpsMan to easily limit access. The main City administrator will have access to all data and be able to easily manage different access levels. These levels can range from having access just to financial information for the City's accountants, to giving the parking management office access to every aspect of the system. All of this is possible in OpsMan and is within the full control of the main City administrator.



Customer Support

Live Chat Support

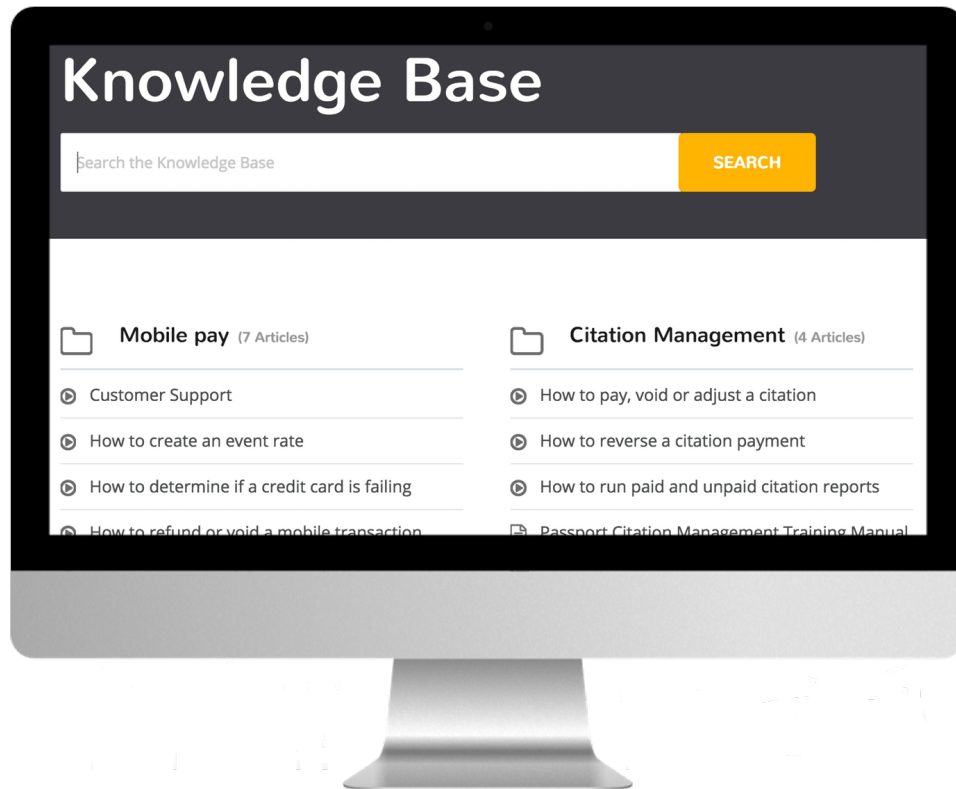
Passport will offer live support, via the telephone, for any technical issues that the parker may encounter. However, when the parker has questions or issues with the actual parking structure, they will be directed to contact the City. To manage this influx of calls, Passport created a live chat support function between the parkers' app and OpsMan. City administrators will be able to speak directly to parkers and solve problems, from any location with internet access. This improves the parker's experience using the application and it releases the City from tying customer service to a particular call-center location.

Client Success

Knowledge Base

Knowledge Base is an online repository of training videos, online forums, and training materials, all of which are updated along with the software. Using Knowledge Base, City administrators will be able to chat with other OpsMan administrators in other cities to work through common problems; watch short training videos on new and old functionality; and access training manuals for each of Passport's products.

Passport's Client Success Managers ensure that this information is updated regularly. If, for whatever reason, Knowledge Base does not address the City's concern, the Client Success Manager is always on hand to resolve issues as needed.



Client Support

After contract execution, the City will be managed by Passport's Client Success team. This team is made up of the Client Success Manager and a Product Support Specialist. The Product Support Specialist is devoted solely to the technical support of the City. Having a dedicated technical support line and representative ensures that the City receives the best service in a timely manner.

The City will be able to contact the Product Support Specialist 24 hours a day, 7 days a week via email and during regular business hours via phone. Regardless of method of communication, all issues will be resolved in accordance with Passport's backup procedures, which prioritizes problems by the impact of the issue. The Product Support Specialist will be in constant contact with the City throughout the resolution of the problem.

All technical and operational support items should follow the outlined procedure:

- a. Email: help@passportinc.com Include the nature of the issue and any background that would be helpful in resolving the identified item.
- b. Phone: Immediately call 980-939-0990
- c. The on-call team will respond to inquiries and take appropriate action

Other Technical Requirements

- **Data Security - The system must exercise industry standard protocols to ensure the protection of any data stored and transmitted in the system, including:**
 - **Securing physical servers, storage, etc.** *Comply.*
 - **Firewalls to protect against unauthorized access.** *Comply.*
 - **SSL encryption on websites.** *Comply.*
 - **PCI PA_DDS level 1 compliant on all applicable data.** *Comply.*
 - **SAS 70 Type II certified before the Notice of Award.** *Comply.*
 - **The participant must minimize NCPA's exposure to sensitive data, such as:**
 - **Credit card numbers.** *Comply.*
 - **Personal information of users.** *Comply.*
 - **The participant must describe its data security plan and disclose any breaches of security.** *Comply.*

At its base, Passport is a payments processing company. In order to do this effectively, security is the number one concern of everyone at Passport. Passport goes above and beyond required security measures to provide peace of mind to cities, parkers, violators, permit holders, and riders.

PCI-DSS Compliance

Any merchant that stores, processes, or transmits cardholder data is required to maintain payment security of that information. PCI security standards lay out the technical and operational requirements for software developers and manufacturers of applications and devices used in payment transactions. PCI Data Security Standards (PCI-DSS) provide actionable framework for developing a robust payment card data security process -- including prevention, detection, and appropriate reaction to security incidents.



Passport maintains PCI-DSS Version 3.1 compliance. No sensitive information is stored or transferred on the Passport database. The only information stored on the database are names, phone numbers, and email addresses. All credit card information is stored in an isolated card storage database. That data is encrypted and tokenized to reduce the risk of credit card fraud in the event of a breach. Please see page 21 for Passport's Compliance Certificate.

SSAE-16

The Statement of Standards for Attestation Engagements (SSAE) No. 16 is the authoritative guide for reporting on service organizations. Using these standards, Passport is audited by an Independent Auditing Firm, which issues a Service Auditor's Report. The Report outlines the chain of control and risk associated



with internal operations. Passport completes SSAE-16 audits annually for its mobile payment transactions.

PriceWaterhouse Coopers

In addition to other security standards and audits that Passport regularly engages in, Pricewaterhouse Coopers conducts ethical hacking on Passport's system yearly. PwC hackers attempt to break Passport's system, searching specifically for security flaws. Any issues that arise from this exercise are immediately relayed to Passport and fixed.



A-LIGN

Passport hires A-LIGN to assist in meeting specific auditing and security assessment needs. A-LIGN helps navigate security standards for credit card transactions and ensures that Passport continually meets and exceeds those standards.



Secure Socket Layer

Passport utilizes Secure Socket Layer (SSL) to securely transfer sensitive data between the application and servers. SSL is the standard security technology for establishing an encrypted link between a web server and a browser. This link ensures that all data passed between the web server and browsers remain private and integral.

Passport only stores the name and email address of the parker, violator, permit holder, or rider on the application while all other sensitive data is stored on a secured, firewall protected server.

Gateway Provider

Passport is listed as a certified gateway provider on both Visa and Mastercard's national registries. Additionally, Passport is recognized as a sponsored service provider for both companies as well.

OpsMan

Internal security standards are managed through Passport's backend system, Operator Management ("OpsMan"). OpsMan restricts access to data via permissions defined by the City for the administrators. Roles can be created such that specific titles correspond to specific access permissions. Passport will only have access to the username (either email or phone number) of administrators for troubleshooting and customer support.

- **System Availability - The system must provide redundant/failsafe servers which ensure at least 99.9% uptime of all components of the system, including:**
 - **IVR, including the availability of live customer service representatives.**
- Comply.

- **Mobile applications.** *Comply.*
- **User and administrator websites.** *Comply.*
- **Integration with existing multi-space meters (only for the integration part for which the participant is responsible).** *Comply.*
- **Integration with existing enforcement systems (only for the integration part for which the participant is responsible).** *Comply.*
- **The proposed system must be able to handle up to 50 million mobile payment transactions per year, including up to 12,000 transactions per hour.** *Comply.*
- **The system must provide system uptime reports from the past 4 years and also provide a plan to scale the system to support additional users and transactions.** *Comply.*

Passport's servers are hosted by Amazon Web Services ("AWS"), a secure cloud services platform that stores databases and delivers content and functionality to its clients. Part of AWS's service offering is the implementation and maintenance of virus and security software. Using AWS and its suite of products, Passport is able to offer peace of mind to the City.

Database Storage

Amazon Relational Database Services ("RDS") houses Passport's database. RDS provides multiple advantages to Passport such as provisioning, patching, backup, recovery, failure detection, and repair. Using AWS and RDS, Passport is able to scale easily, which means that every one of Passport's clients' utilization can grow quickly and all at the same time without affecting the efficacy of the database.

Elastic Load Balancing

Multiple servers exist within the system, each with the capacity to host the entire system. Amazon RDS automatically creates a primary database instance, which is simultaneously replicated to a standby instance in a different Availability Zone ("AZ"). Each AZ runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable.

If a server becomes overloaded or fails, RDS performs an automatic failover to the standby instance. This means that the application can resume database operation without the need for manual intervention. Essentially, RDS protects the system from failure and the only potential lag time would be the amount of time it takes for the system to failover from one AZ to the next.

Database Backup

RDS offers automated backup, which allows for point-in-time recovery of Passport's database instance. RDS backs up the database and transaction logs and stores both for a specified retention period, meaning that Passport can restore its database instance to any second during the retention period, up to the last five minutes. Passport's entire database is

backed up daily between 3:00-3:30AM EST, capturing all transaction logs. Each backup is saved for seven (7) days. Thus, if there is ever a failure of the server, Passport will be able to recover all data and transaction logs up to the morning of the failure.

Database Snapshots

Amazon's Simple Storage Services ("S3") takes and stores database snapshots of the entire system. The snapshots are kept until explicitly deleted and are incredibly durable, allowing Passport to create a new instance of the database from the snapshot whenever needed or desired. These snapshots can be stored in separate AZs, giving an additional protection against any potential system failure or overload. Daily offsite snapshots are taken of the entire Passport database.

Passport guarantees that its solution will have a 99.9% uptime.

Integrations

- **Multispace Meters - The system must be able to communicate with the back office system of the existing multi-space meters. The system must have the following requirements:**
 - **Send each transaction to the existing back office system or a 3d party system as it happens in real time.** *Comply.*
 - **Accept transactions sent from the back office system or a 3d party system.** *Comply.*
 - **The participant must provide examples of data formats and delivery methods used to communicate transactions to and from external systems.** *Comply.*
- **Enforcement - The system must be able to communicate with any enforcement system. The system must have the following requirements:**
 - **Allow a device to query the payment status of a vehicle through its license plate number using an API provided by the vendor that is compatible with:**
 - **Android.** *Comply.*
 - **iOS.** *Comply.*
 - **Blackberry.** *Comply.*
 - **Windows Mobile.** *Comply.*
 - **A platform agnostic web service.** *Comply.*
 - **Allow a device to query a list of paid vehicles through a meter/block/zone ID.** *Comply.*
 - **Allow a license plate recognition system to query the payment status of a vehicle through its license plate number.** *Comply.*
 - **Pull or receive a list of license plate numbers flagged by law enforcement.** *Comply.*
 - **The system must be able to send an alert when a matching vehicle makes a parking transaction.** *Comply.*

- **The participant must provide examples of their enforcement integration models with other clients. Comply.**

Passport is a leader in integrated technology software for parking due to an open API, which integrates with all other providers in the City's ecosystem. Passport's solution uses a caching system that ensures the fastest transfer of data and system performance between providers, including Digital Payment Technologies, IPS, and CALE. Passport has the ability to push information to the meters meters, however, many meter providers charge per transaction for pushing data. To save the City money, Passport bypasses this step and pushes data directly to the citation enforcement issuance provider.

Passport recommends using its Citation Management Platform for the best quality service, but if the City has a different provider, Passport will work with that provider to deliver a seamlessly integrated experience. Passport is currently integrated with the following citation management software: Xerox, T2, Duncan Solutions, CivicSmart, Kelly & Ryan Associates, AIMS, UP Safety, Clancy Systems, Complus Data, Quatred, and VATS. If parking enforcement officers are not all equipped with an internet-connected issuance device, Passport will provide the City with its Park Monitor solution, which tracks all active parking sessions and is available via any Android device.



Enforcement Integration Examples

Example: Genetec Integration

Passport maintains an existing integration with Genetec for LPR enforcement. With this integration, when a parker pays with the Passport app, parking rights are automatically synchronized with AutoVu mobile ALPR enforcement units. All information is passed in real-time, thereby decreasing the number of parking ticket disputes and increasing compliance in payment from parkers. Passport is able to meet this level of integration with other LPR technology providers with which the City already works.

Example: TurboData Integration

Passport maintains an active integration with TurboData whereby Passport sends real-time parking session data to the Android and Dolphin 99EX Honeywell handhelds and to the TurboData system for real-time monitoring of all parking session statuses. By pushing this information in real-time, TurboData the City will be able to monitor all parking sessions throughout the City.

Example: T2 Flex Integration

The Passport/T2 integration pushes all parking session statuses in real-time to T2 issuance devices. So long as the issuance device is connected to the internet or cellular data, it will receive parking session data immediately. The City's parking enforcement officers will be able to see whether a parking session is active or inactive and take the appropriate action. As it is not necessary for accurate enforcement, Passport does not push any monetary information to the T2 system.

Marketing

The vendor must provide examples of marketing plans used in other cities or markets. In addition:

- **The vendor must provide an initial marketing plan to promote the use of the system, including details on the message, medium, location, and frequency of marketing. *Comply.***
- **The vendor must provide a comprehensive recurring marketing plan. *Comply.***
- **The vendor must supply all promotional and operational graphics, excluding the street signage used to identify meter/block/zone IDs. *Comply.***

All marketing plans and materials shall be approved by NCPA prior to implementation. *Confirmed.*

Passport will work closely with the NCPA and the Region 14 City to develop a marketing plan, starting with an initial questionnaire to identify key demographic information and channel options. Upon completion, Passport will deploy ***one of three advertising options below***, selected by the City, to accommodate the launch of the mobile application, generating maximum market exposure of the mobile pay for parking application.

-
- **Included (\$0)**
 - Press release
 - Digital ad creation for City's distribution channels
 - Promo code handout (promo discount to be matched by City's investment)
 - iOS App Store Search Ads
 - Google Play Search Ads
 - Geo Targeted social media posts
 - Advertising design for local print and digital publications (placement not included)

- **Launch Burst (\$2,000)**
 - 3 week advertising and public relation campaign
 - Mainly digital advertising
 - Selected distribution channels to maximize awareness and utilization
 - 1 million total delivered impressions (dependent on market size)
- **Sustained Launch (\$5,000)**
 - 6 week advertising and public relation campaign
 - Digital + Street Team Involvement
 - Rose Bowl Flea Market, Noon Year's Eve at Kidspace Museum, etc.
 - Selected distribution channels to maximize awareness and utilization
 - 2 million total delivered impressions (dependent on market size)
- **Launch + Utilization Package (\$7,500)**
 - 12 week advertising and public relation campaign
 - Digital + Street Team Involvement
 - Rose Bowl Flea Market, Noon Year's Eve at Kidspace Museum, etc.
 - Selected distribution channels to maximize awareness and utilization
 - Additional 3 week utilization flight (1 to 2 months after initial 12 week flight ends)
 - 5 million total delivered impressions (dependent on market size)

Marketing Channel Tactical Components

Passport will build an omni channel advertising package that will consist of the below options, based on availability and agreement between Passport and Pasadena. *Items highlighted in yellow are considered premium services and may require additional costs*

Out of Home (OOH)

- On/Off Street Signage
- Meter decals
- Downtown banners / posters (if applicable)
- Shopping mall / retail space kiosk posters (if applicable)

Digital / Web Advertising

- Blog Article Placed in Native Advertising
 - 21 day run
- Geo-targeted ads ran through digital ad networks
 - 80/20 mobile concentration



- 1 month flight
- ❑ Google Adword Keyword Ad Targets
- ❑ iOS App Store Search Ads

Social Media Advertising

- ❑ 2x Social Posts per week for 1 month
 - Facebook
 - Twitter
- ❑ 1x promoted post
 - Facebook
 - Twitter
- ❑ Twitter Mobile App Install Ad
 - Geo targeted and defined demographics
- ❑ Facebook Mobile App Install Ad
 - Geo targeted and defined demographic

Traditional Advertising

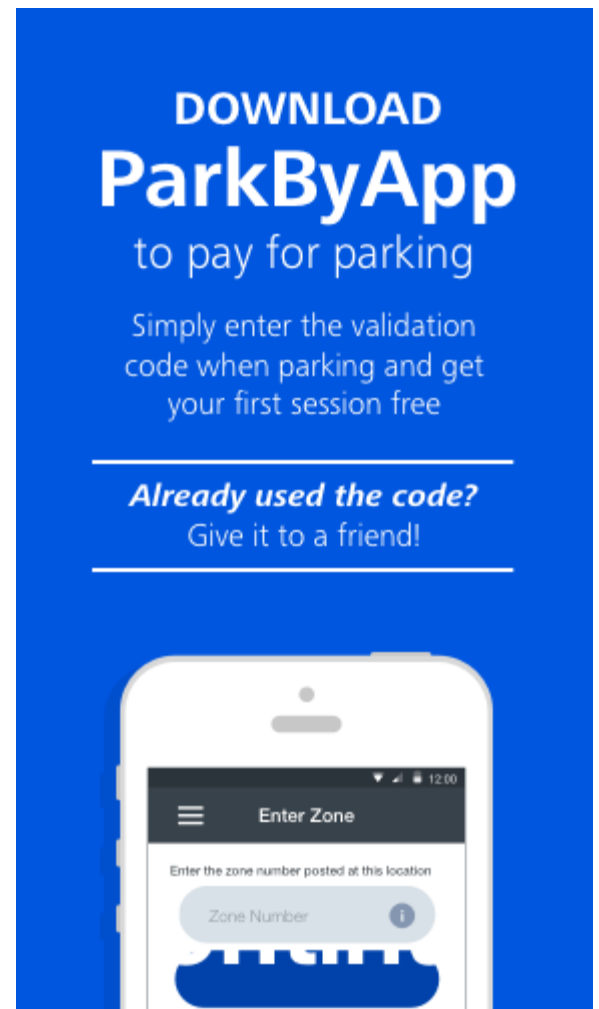
- ❑ Informational Handouts
 - 10,000 provided
 - Additional upon request
- ❑ Parking Validation Code Card Handouts
 - 1,000 provided
 - Additional upon request
- ❑ Educational flyers
 - 5,000 provided
- ❑ Local magazine / newspaper ads
- ❑ Direct Mail to defined zip codes
 - Quantity to be determined by demographic count

Experiential Marketing

- ❑ Street Team
 - Team of 4 - 4 days per week, 4 hours per day
 - Email collection for future fare promos / codes
- ❑ Sidewalk chalk / street decals at high traffic parking areas
- ❑ Window clings at local merchants
- ❑ Collaboration with local sports / events
- ❑ Local coffee shop cup sleeve advertising

Media Relations

- ❑ Drafted launch press release



- National news wire release
- ❑ Special event, status, feature, update press releases (as needed)
- ❑ Coordinated press launch event
- ❑ *(all repurposed and republished on LinkedIn, Facebook, and Twitter)*
- ❑ Retweet and share other news outlet stories
- ❑ **Blogger outreach**
 - **Identified through local social and web sites**

Additional Services

- ❑ **Marketing Management Services**
- ❑ **Demographic research (if not currently provided)**
- ❑ **SMS Sign-Up Page for Fare Coupon Promotions**
- ❑ **How-To Use Video**

Customer Service

- **End User Customer Service - The vendor must provide the following customer service to end users:**
 - **Live operators available 24/7 to create accounts and resolve issues.**
Comply.
 - **Language support for:**
 - **English.** *Comply.*
 - **Spanish (if available).** *Comply.*
 - **Customers looking to establish contact with a live operator must be provided the option at the start of a parking action.** *Comply.*
 - **Callers seeking a live operator must not be on hold for longer than 2 minutes.** *Comply.*
 - **Music and updated messaging must be provided during calls on hold.**
Comply.
 - **Customers looking to find parking must be provided a web-based or mobile app based map, or other method of locating metered parking.**
Comply.

The vendor must provide a customer support plan that includes projected call volumes and number of support staff available. *Comply.*

Passport supplies a variety of support through the application, website, and and telephone support. Parkers will have unlimited access to parking history and self help in the form of FAQs through the website and application. Additionally, Passport will provide live agent support from 8am-9pm EST Monday-Saturday and 12pm-9pm EST on Sundays. Outside of those hours, the parker will be able to call a dedicated call center, which will answer basic questions related to the application and flag any more serious issues to be handled by a Passport Customer Support representative the next day.

The extent of Passport's support will be limited to questions related to the application itself. Passport will not answer questions related to the City's parking operations and will direct any parkers with those questions directly to the City. Passport technical support will also not issue refunds, which are considered to be a business decision to be made by the City. However, Passport's technical support will void payments in truly duplicative situations, where the parker unintentionally started multiple parking sessions.

Passport strives to create an intuitive application that ought to reduce the number of technical support representatives required. As an example, Passport technical support has fielded only 75 calls for the City of Victoria, B.C. in the first 10 months of deployment. While Passport is able to handle multiple calls at once, this is rarely necessary.

- **NCPA Support - The vendor must provide the following services to NCPA:**
 - **Technical support during normal business hours of 8:30AM to 6:00PM (EST).** *Comply.*
 - **Engineering staff to perform development, testing, and deployment.** *Comply.*
 - **Response times of less than 30 minutes for urgent issues.** *Comply.*
 - **Resolution of urgent issues in less than 2 hours.** *Comply.*

The vendor must provide examples of development project plans and issue resolution processes with other clients. *Confirmed.*

After contract execution, the City will be introduced to Passport's operations team, which is comprised of Enterprise Implementation and Client Success. This team will be the liaison between the City and Passport, including all software engineers. The first call post-contract will be managed by the Regional Sales Vice President, David Singletary. David will introduce the mobile ticketing platform and the rest of the Passport team to the City's team. After this call the City's main points of contact will be its Project Manager and Client Success Manager, however, David will remain a secondary resource for the City, in the event he is needed.

After launch, the CSM will speak with the City on a monthly basis, at a minimum, to fully understand the state of affairs. During these calls, the CSM will also impart any roadmap updates or new features that may be beneficial to the City. Once a quarter, the CSM will conduct a system review with the City to ensure that the product meets or exceeds the needs of the City. Passport positions its CSMs to be the best resource for any City not only on all things Passport, but all things related to enforcement.

To address any critical problems or triaging any issues, the City will also have access to a dedicated Product Support Specialist (the "PSS"). The PSS is trained in solving most problems that the City may encounter and for any problem that is outside the scope of their training, the PSS will liaise with the software engineer that built the system. Any issues will be addressed immediately and should be resolved within 24 hours of notice. This support is available 24 hours a day, seven days a week. Depending on the severity of the issue, Passport will respond as follows:

Priority 1 – Critical Problems: If the service is experiencing problems that crash the system completely, leads to data corruption, cause major functions or features to fail to operate, or are otherwise significant, material, and substantive. Passport will provide an error notice for such problems within fifteen (15) minutes of Provider's receiving notice of such error and dedicate resources on a continual, best efforts basis to correct the problem within one (1) hour of receipt of the Error Notice. Passport will provide the City status reports every one (1) hour, or more frequently if requested by the City, until the problem has been corrected.

Priority 2 – Medium Impact Problems: If the service is experiencing problems that cause significant delays or cause minor functions or features to fail to operate that is substantive, but not material. Provider shall provide an Error Notice for such problems within one (1) hour of Provider's receiving notice and shall work during normal business hours and use reasonable commercial efforts to correct the problems within six (6) hours of receipt of the error notice. Passport will provide the City status reports every one (1) hour, or more frequently if requested by the City, until the problem has been corrected.

Priority 3 – Low Impact Problems: If the service is experiencing problems that cause minor delays, but do not inhibit the ability to use the service and are neither substantive nor material. Passport will provide an error notice for such problems within one (1) hour of Provider's receiving notice and shall work during normal business hours and use reasonable commercial efforts to correct the problems within one (1) day of receipt of the error notice. Passport will provide the City status reports every one (1) hour, or more frequently if requested by the City, until the problem has been corrected.

All technical and operational support items should follow the outlined procedure:

Phone:

- Immediately call (980) 939-0990 for Technical Product Support
 - If an email response or phone call does not occur within under 5 minutes call any of the secondary support numbers, which go directly to support engineers

Email:

- The City may email Passport at any time and will receive a response as soon as possible.
 - Parker support: support@passportinc.com

- o City support: help@passportinc.com

Training

The vendor must provide training to personnel designated by NCPA and cooperating agencies in the following areas:

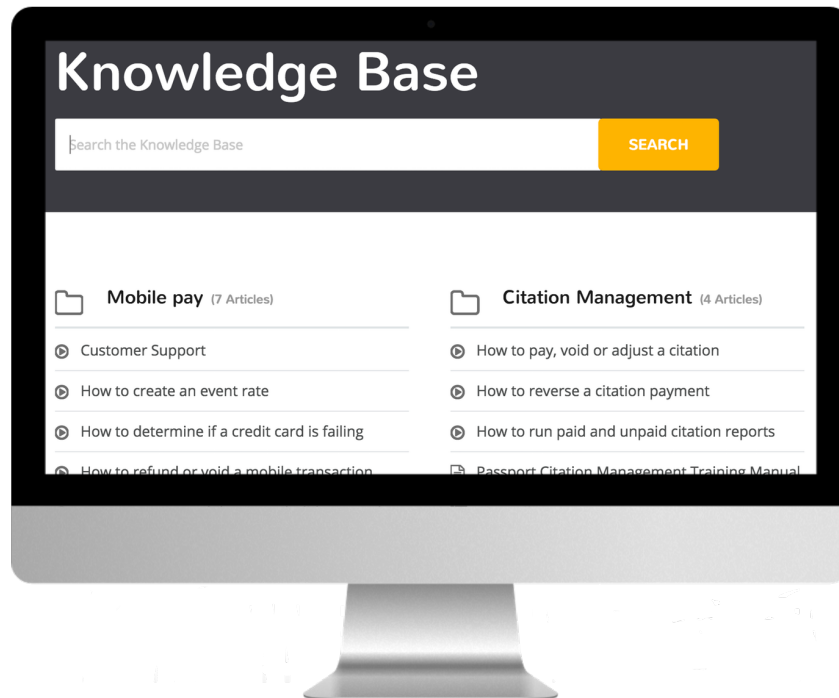
- **Use of payment methods.** *Comply.*
- **Use of any websites designed for users and administrators.** *Comply.*
- **Use of any enforcement tools.** *Comply.*

The vendor must also provide training for end users, including, but not limited to a frequently asked questions (FAQ) section and/or instructional videos on the vendor's website. *Comply.*

During implementation, Passport will train City administrators on how to best utilize the backend system, Operator Management ("OpsMan"). During that training, the City will learn all of the different ins and outs of the system and be prepared to take over operations after launch. Passport also understands that it's easy to forget things that aren't always in front of you and so it created Knowledge Base.

Knowledge Base is an online repository of training videos, online forums, and training materials, all of which are updated along with the software. Using Knowledge Base, City administrators will be able to chat with other OpsMan administrators in other cities to work through common problems; watch short training videos on new and old functionality; and access training manuals for each of Passport's products.

Passport's Client Success Managers ensure that this information is updated regularly. If, for whatever reason, Knowledge Base does not address the City's concern, the Client Success Manager is always on hand to resolve issues as needed. Please see page 103 for training materials.



Deployment

The vendor must provide examples of deployment plans with other clients that include the following:

- Development schedule.
- Testing schedule.
- Roll out schedule.
- Marketing schedule.
- Training Schedule.

The participant must provide a tentative deployment schedule for NCPA that includes all services.

PROJECT MILESTONES	DURATION (DAYS)	DAYS AWAY FROM LAUNCH
KICKOFF	10	43
review of current environment	2	43
kickoff call	0	39
request for additional information	4	38
develop project plan	2	31
distribute project schedule & documents	0	30
follow-up call if needed	0	30
SYSTEM SETUP/PROVISIONING	13	29
contact and customer support information	2	29
assign users and roles	3	25
ENVIRONMENT SETUP	12	28
complete environment and rate buildout	5	28
<i>provide testing link to client</i>	1	21
perform environment and rate testing	5	17
<i>client signoff on environment and rate testing</i>	0	11
DETERMINE IVR SETUP	4	24
establish main phone number	1	24
develop calling tree script	2	23
<i>deliver calling tree script for signoff</i>	0	22

<i>client signoff on IVR system</i>	0	21
CUSTOM INFORMATION	4	18
develop terms and conditions, privacy policy, and FAQ	4	18
custom wording for specific emails	1	18
receipts	1	18
wallet Loads	1	18
expiring credit cards	1	18
Operator Management System Setup Complete		
PARKING PAYMENT INTEGRATION	7	22
initiate contact with parking device/enforcement provider	1	22
request and receive device credentials	3	21
finalize integration setup	2	16
test parking system	1	14
<i>client sign off on parking payment system integration</i>	0	14
FINANCE	16	35
finance conversation with client	1	35
transaction voids	1	35
refunds	1	35
wallet	1	35
wallet setup	2	32
initiate contact with Merchant Processor	5	32

request gateway credentials	5	25
finalize merchant processing setup	3	18
test flow of funds to merchant account	2	15
<i>client sign off on merchant account</i>	0	14
MARKETING AND PUBLIC RELATIONS	22	32
decals and signage	21	32
discuss size and content	3	32
design decals and signage	5	29
<i>send proofs to client for approval</i>	1	22
<i>client sign off on decals and signage</i>	0	22
confirm quantity	2	21
place order	2	21
receive shipment	10	17
public relations	10	18
compile media distribution list	5	18
draft pre-launch press release	4	11
<i>client sign off on pre-launch press release</i>	0	8
distribute pre-launch press release	1	7
create launch press release	4	11
<i>client sign off on launch press release</i>	0	8

validation	14	22
validation discussion with client	1	22
create parker validation materials	4	14
develop validation codes in system	3	8
test validation system	1	3
<i>client sign off on validations</i>	0	3
handouts	17	25
design handouts for distribution	5	25
<i>send handouts to client for approval</i>	2	18
<i>client sign off on handouts</i>	0	3
receive handouts	0	3

Marketing and PR Setup Complete

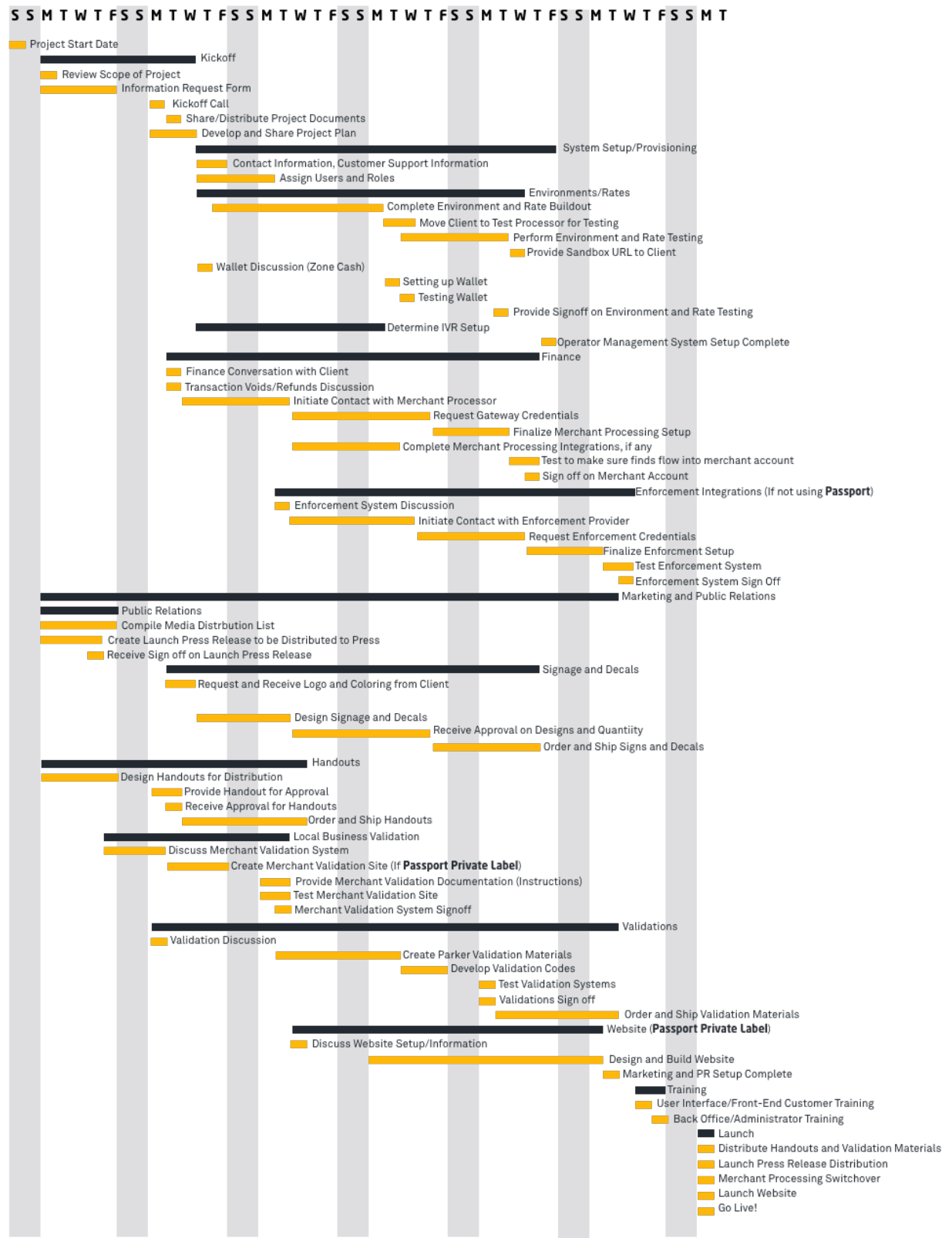
EXISTING MOBILE PAY PROVIDER	9	11
contact provider for user accounts	5	11
change any reference of existing provider	5	7
verify all information has been removed	0	0
TRAINING	2	2
move client to test merchant account for training	1	2
user interface and front end customer training	1	1
back office and administrative training	1	1

LAUNCH	3	3
distribute handouts and validation materials	1	0
distribute launch press release	1	0
merchant processing switchover	1	0
launch website	0	3

GO LIVE

POST LAUNCH FOLLOW UP	7
management checkins	7

TOTAL CALENDAR DAYS	43
TOTAL WORKING DAYS	32



Additional Integrated Services

The vendor must incorporate additional integrated services and pricing to their proposal, including but not limited to:

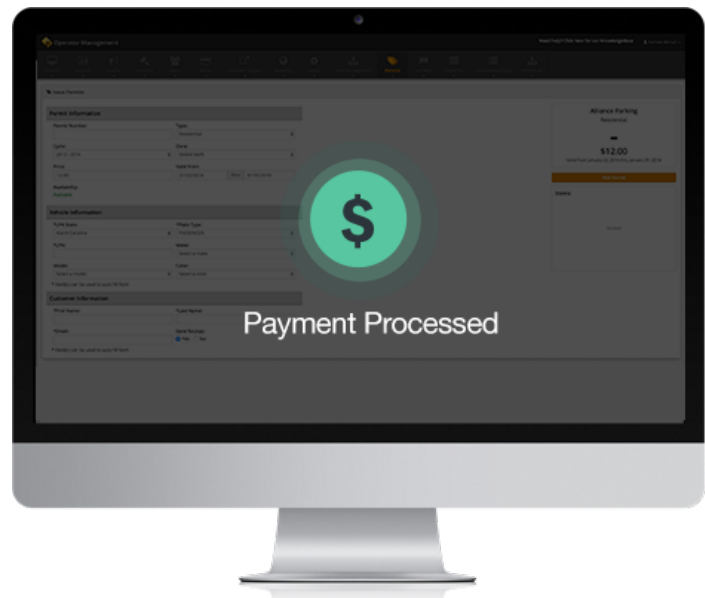
- **Digital virtual permit management system for monthly, residential, visitor, and other parking related permits:**
 - **The whole lifecycle of a permit must be automated. *Comply.***
 - **Registration, application, auto-renewal payments, approval (if applicable), and issuance must be performed online. *Comply.***
 - **Permits can be assigned to the vehicle's license plate number, send to the permit holder's smart phone or other mobile device or printed at home. *Comply.***
 - **Online personal account for permit holder to update information and manage their account. *Comply.***
 - **Waiting list and mass email functionality. *Comply.***

Passport's Digital Permit Platform ("DPP") delivers an end-to-end digital solution to manage and enforce parking permits throughout the City. DPP was built in conjunction with Passport's Citation Management Platform and informed by Passport's experience with public and private parking operations. The result is a digitally enforceable permitting system, that is able to manage the entire application process, including uploading eligibility documents and managing a wait list.

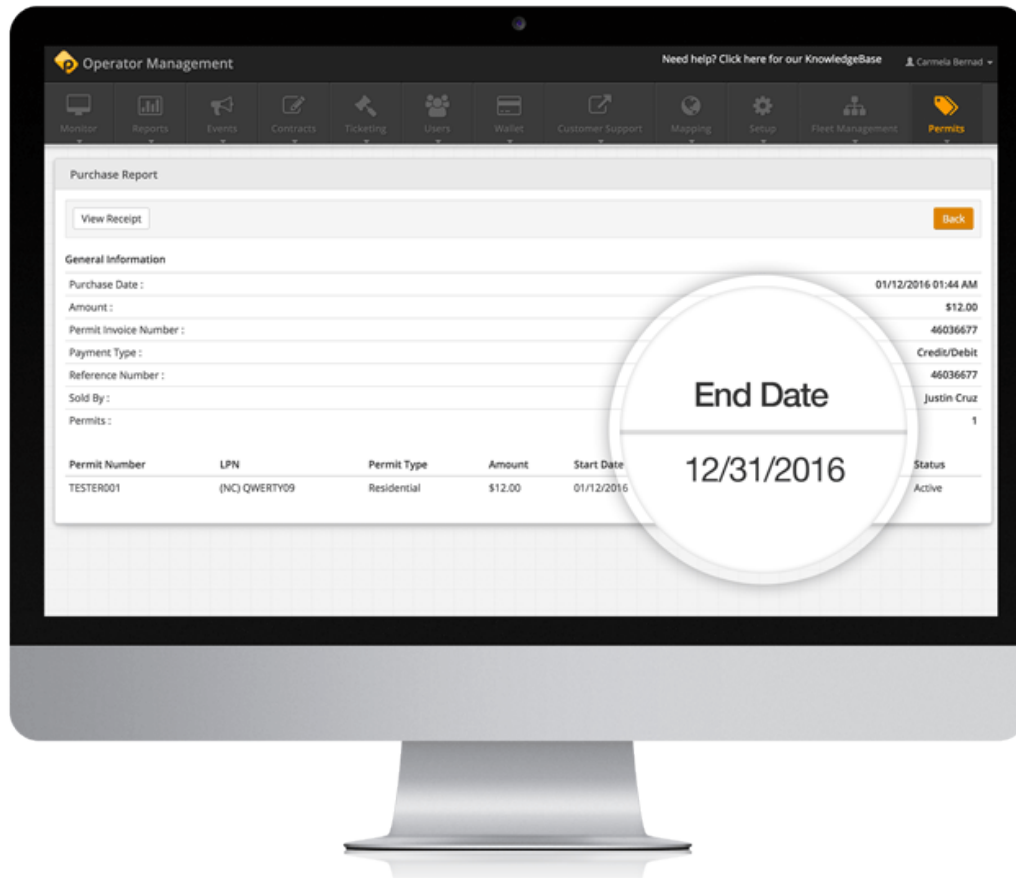
Cloud-Based Solution

Permits Built for Speed

Passport's DPP allows the City to issue, track, and manage a range of permits, including all parking permits for residents, guests, employees, and temporary one-time permits. From the backend system, Operator Management ("OpsMan"), the City will be able to control all required credentials, such as permit name, price, customer name, vehicle limit, license plate number ("LPN"), residence verification, email address, and more.



Passport's DPP solution enables cities to have a point of sale in municipal facilities or through a client-facing portal. OpsMan allows for total report generation by the City, including permit revenue, permits in use, and purchase reports. With so much data available, the City will be able to track and analyze everything from issuance to expiration dates.



Sole Sourced Solution

Passport's DPP was built along side its Mobile Payment for Parking and Citation Management platforms, giving the City a wider breadth of optionality for its permitting system. By combining Passport's private label mobile parking application and DPP, the permit application will tie into the parking application. This gives a native feel to the application that the parker is already accustomed to. Additionally, the permit applicant will have a tokenized payment record, which allows the system to pass the parker's payment credentials from the Mobile Pay application to the permitting portal.

Passport is the only digital solution on the market that allows for multi-vehicle permitting, when the City also implements Passport's Citation Management Platform. With this solution, the same family or household can register multiple vehicles for use of the same permit. Using Passport's Citation Management Platform, when a member of a household parks their car in the City, the parking enforcement officer will run the LPN against the database and mark the permit as valid and in-use. If another car from the same household parks in the City without paying for parking, the database will notify the parking enforcement officer that the permit is already in use and to issue a citation.

Powerful Features

Enforce with Accuracy

Passport partners with leading License Plate Recognition services that increase the speed and accuracy of enforcement with seamless integrations. After a permit has been issued, all relevant data will be pushed to the City's Citation Management Platform. If the City is using Passport's Citation Management Platform, a parking enforcement officer will have the benefit of a dynamic system, which allows the parking enforcement officer to easily search through the database for an LPN; because the system is dynamic, the pool of eligible vehicles becomes smaller with each additional digit. If the LPN is attached to a permit, the parking enforcement officer will be able to view the permit within the software and know that there is no violation warranting a citation.

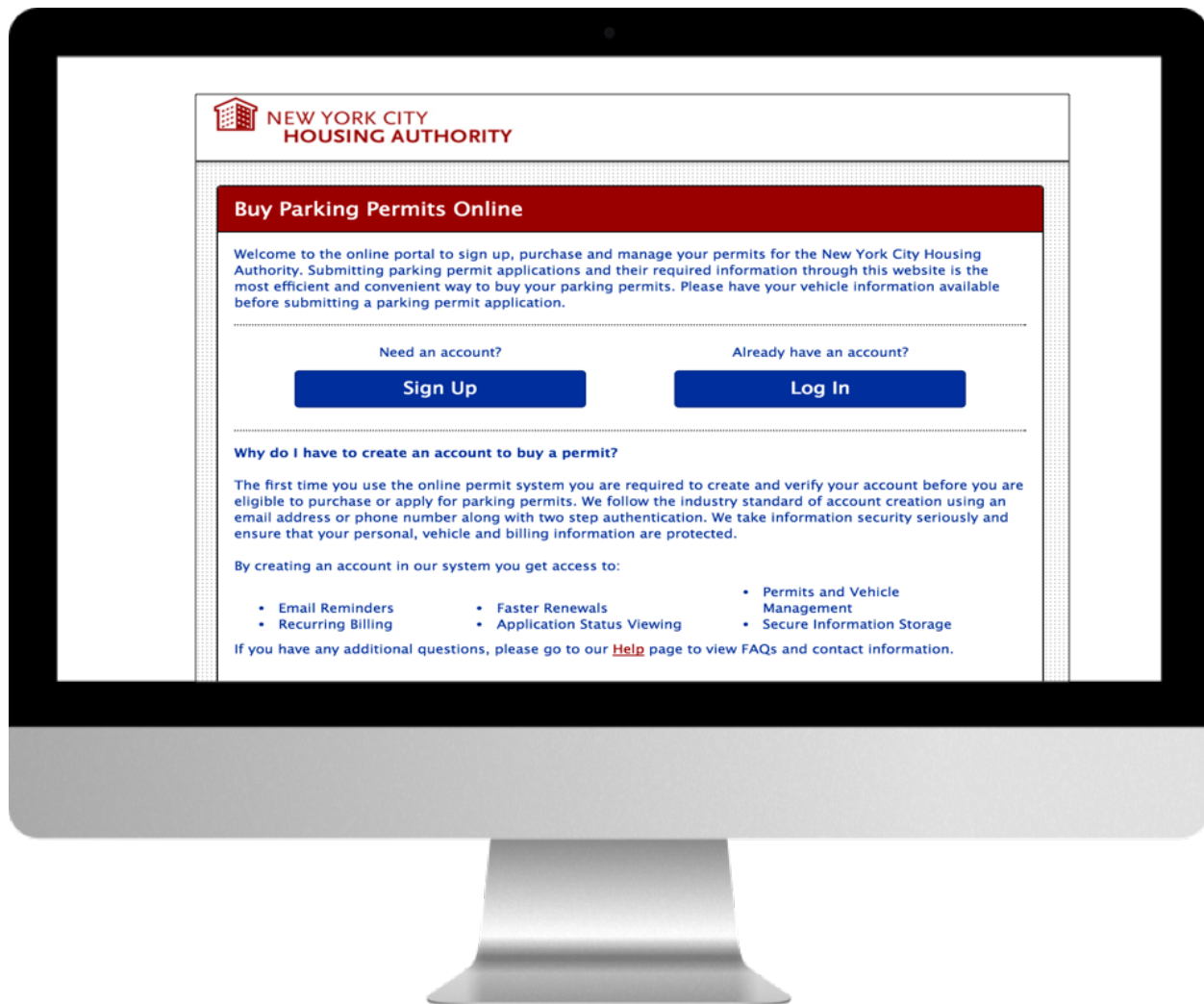
Branded Application and Payment Portal

The permit application page for DPP is a custom-branded, mobile-optimized secure payment portal, RMCPay. The City will select a custom graphic and color scheme to be used as the background of the portal and the URL will be an addition to the City's parking website. The permit applicant will login to RMCPay with the same phone number and email address they use to pay for parking through the Mobile Payment application.

RMCPay will be the applicant's dashboard to manage their permits. The permit applicant will be able to see all permit information from the portal, see how many permits are available in a given zone, apply for permits, and track their position on a wait list. When applying, the permit applicant can use that day's date or a future date. If the date is not at the beginning of a payment cycle, the City may choose to pro-rate the cost of the permit to either the day, month, or quarter.

If the permit requires proof of residency or other eligibility, the permit applicant will upload documents directly to RMCPay, which will be available for review by the City in OpsMan immediately. The permit applicant will not be required to pay for the permit until after they have been approved by the City. When a City administrator verifies the permit applicant's eligibility, they will update the permit applicant's status, which will automatically send an email notification to the applicant to return to RMCPay to complete their permit application.

If a permit applicant is wait listed for a particular zone, they will be able to monitor their status within RMCPay. The City can configure the system to determine whether the applicant can see their specific number on the list or just that they are still waitlisted. The City will also be able to manage the wait list order and override the wait list from OpsMan. Once a permit becomes available, the permit applicant will receive an email notification and direction to complete their permit. The City can configure this process to limit the amount of time that the permit applicant has to complete payment of their permit before losing the opportunity.



- **Central database repository for aggregated parking data (analysis), central enforcement and integration of several parking methods and technologies, such as much not limited to:**
 - **Mobile payments for parking system.** *Comply.*
 - **Pay by plate (multi-space meter).** *Comply.*
 - **Digital permit management system.** *Comply.*
 - **Enforcement.** *Comply.*

Passport's backend system, OpsMan, will collect all data from the Mobile Payment Platform and any other integrated system, including multi-space meters, digital permitting, and enforcement. If the City elects to implement Passport's Digital Permitting and Citation Management Platforms in conjunction with the Mobile Payment Platform, all of the data will automatically be aggregated within OpsMan from the date of launch and available for analysis and queries immediately. By implementing the enterprise suite of Passport products, the City will not only have a single backend system for its use, but it will be able to

release a single front-end application to handle parking payments, permit applications, and paying for citations. This single source application will allow the parker to use the same tokenized and stored payment method to pay for permits and citations as it does to pay for parking.

- **Access for mobile payment users to gated parking facilities via:**
 - **QR code, either via scanning within a mobile app or scanning at the gate.** **Comply.**
 - **Near Field Communication (NFC).** **Comply.**
 - **RFID or Proximity Cards.** **Comply.**
 - **License Plate Recognition (LPR).** **Comply.**

Passport is built on an open API, which allows it to seamlessly and easily integrate with any other software provider in the City's ecosystem. If the City has the hardware technology for QR Code Scanning, NFC, RFID, or LPR, Passport can integrate with those mechanisms. Additionally, Passport has created two different features that the City will have access to in parking garages. The first is a sPark and the second is Passport's

sPark

sPark is an automated parking experience for registered Passport parkers. This feature allows parkers to park in a garage without having to stop at a pay station. A registered parker's license plate number ("LPN") will be picked up by license plate recognition technology ("LPR") once they enter the garage, which will initiate the session. When the parker leaves and the LPR reader is no longer able to detect the LPN, the session will stop automatically. The parker's registered form of payment will not be charged until after the session is complete.

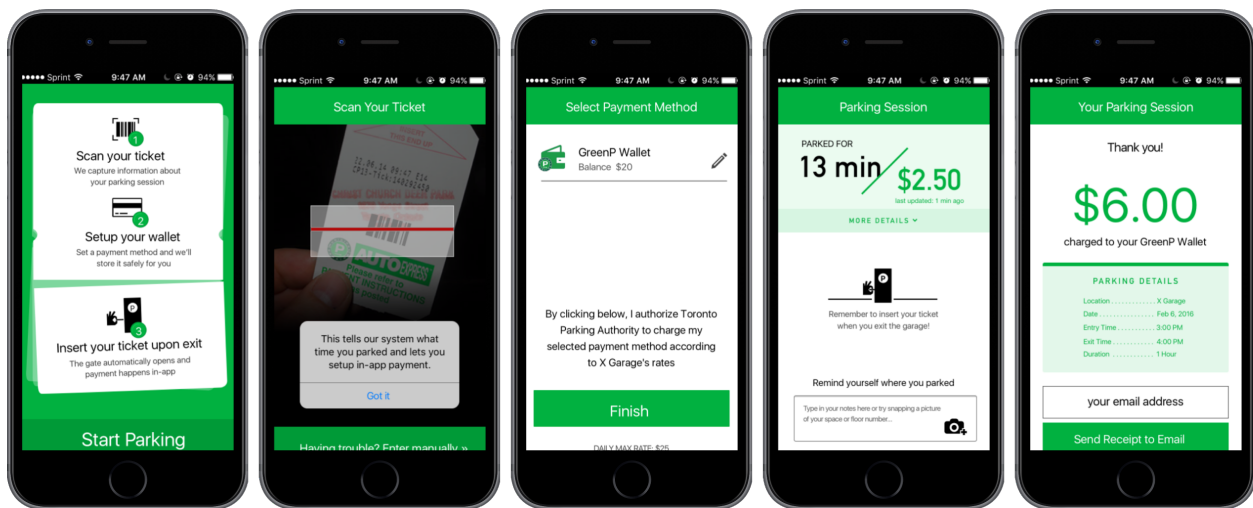
To register for this program, a parker will save vehicles to their account, by LPN, as well as select a default payment method. When the vehicle enters the garage, the LPR will scan the LPN and run the number against Passport's list of registered parkers. If the LPN is connected to a registered parker, Passport's backend system will confirm the payment method and begin the parking session. The status of this parking session will be automatically pushed to the enforcement software to ensure accurate enforcement.

To take full advantage of this feature, the City will have to install LPR cameras throughout the non-gated parking garages that it controls so that every parking bay is monitored. Passport integrates with several LPR providers already and will be happy to suggest a provider if the City wishes to purchase new LPRs.

An added bonus of this functionality is targeted enforcement. By utilizing LPR technology within an enclosed space, Passport's system is able to detect exactly where a vehicle is located within the garage. If a parker is not registered with sPark and hasn't otherwise initiated a parking session, Passport can send targeting information to the enforcement software after the City-specified grace period has expired.

Mobile Pay Station

For gated garages and surface lots, Passport has created its Mobile Pay Station function. With this feature, a parker will take a ticket to enter the lot and raise the gated arm. Once in the lot, the parker will scan the ticket using the Passport application. After the ticket is scanned, the parker then selects which payment method they would like to use to pay for parking. When the parker leaves the garage they will insert their ticket as usual, but instead of having to pay, the machine will communicate with Passport's app and charge the parker for the length of their stay. This Mobile Pay Station releases the parker from visiting a pay station before leaving or having to pull out a credit card when leaving.



- **Electrical Vehicle Charging. Comply.**

Passport's system is built on an open API, making it easy to integrate with any other software providers in the City's ecosystem. Most Electrical Vehicle Charging companies, like ChargePoint, charge for the parking session as opposed to charging for the actual charge, which would not require additional integration. However, if the City does charge the customer to use the charging station, Passport will integrate with any provider of the City's choosing.

- **Event permit system, either via mobile payments for parking system (temporary event rate override of regular parking rates). Comply.**

Within OpsMan, the City will have access to Passport's Rate Builder function. Rate Builder allows a City administrator to easily edit, add, or delete an existing rate structure as well as establish conditions for specific rates.

If there is a special event in the City, the City will be able to set special rates for specific lots. From the OpsMan dashboard, the administrator will navigate to the "Events" tab and select either "Manage Venues" or "Manage Rates." From this screen, the City will input information related to the event, including starting and ending date and time. The City will also have the option of make certain zones free during this time or accepting permits during the event.

This information will update in real time to the Passport Mobile Payment app and OpsMan, giving all parkers and parking enforcement officers access to the most recent rates.

- **Integrations with all major meter equipment, ticket software applications and sensor technology providers.** [Comply.](#)

Passport operates on an open API, meaning that it is able to integrate easily with almost any other software provider, including multi-space meters, parking enforcement, and sensor technology. Passport currently maintains integrations with more than 25 companies related to parking enforcement, LPR technology, and multi-space meters and will work with the City to add to this list. Additionally, Passport operates its own citation management solution, which the City can implement for the best experience for mobile payment and enforcement.

References



Entity Name:	Oak Park, Illinois
Contact Name and Title:	Jill Velan
City and State:	Oak Park, Illinois
Phone:	708-358-5752
Years Serviced:	October 1, 2013 - Present
Description of Services:	Mobile Payment for Parking and Special Event Passes
Annual Volume:	\$132,000.00 (Passport's annual volume of sales)



Entity Name:	Columbia, South Carolina
Contact Name and Title:	Paul Pendley
City and State:	Columbia, SC
Phone:	803-545-4015
Years Serviced:	February 23, 2015 - Present
Description of Services:	Mobile Payment for Parking
Annual Volume:	\$144,000.00 (Passport's annual volume of sales)



Entity Name: Asheville, North Carolina

Contact Name and Title: Ken Putnam

City and State: Asheville, North Carolina

Phone: 828-259-5405

Years Serviced: September 5, 2012 - Present

Description of Services: Mobile Payment for Parking

Annual Volume: \$42,000.00 (Passport's annual volume of sales)



Entity Name: University of Louisville

Contact Name and Title: Gary Becker

City and State: Louisville, KY

Phone: 502-852-7221

Years Serviced: September 10, 2013 - Present

Description of Services: Mobile Payment for Parking

Annual Volume: \$4,104.00 (Passport's annual volume of sales)



Entity Name: Newton, Massachusetts

Contact Name and Title: Jack Cowell
City and State: Newton, Massachusetts
Phone: 617-796-1082
Years Serviced: June 15, 2016 - Present
Description of Services: Mobile Payment for Parking
Annual Volume: \$48,000.00 (Passport's annual volume of sales)



Entity Name: Lincoln, Nebraska
Contact Name and Title: Wayne Mixdorff
City and State: Lincoln, Nebraska
Phone: 402-441-6097
Years Serviced: September 2, 2014 - Present
Description of Services: Mobile Payment for Parking
Annual Volume: \$27,600.00 (Passport's annual volume of sales)



Entity Name: University of Nebraska
Contact Name and Title: Dan Carpenter
City and State: Lincoln, Nebraska
Phone: 402-472-1800
Years Serviced: July 23, 2014 - Present

Description of Services: Mobile Payment for Parking
Annual Volume: \$74,400.00 (Passport's annual volume of sales)



Entity Name: Weber State University
Contact Name and Title: Crystal Taylor
City and State: Ogden, Utah
Phone: 801-626-7801
Years Serviced: June 18, 2015 - Present
Description of Services: Mobile Payment for Parking
Annual Volume: \$3,000.00 (Passport's annual volume of sales)



Entity Name: Oregon State University
Contact Name and Title: Mark Zandonella
City and State: Corvallis, Oregon
Phone: 541-737-8205
Years Serviced: August 2, 2016 - Present
Description of Services: Mobile Payment for Parking
Annual Volume: \$3,000.00 (Passport's annual volume of sales)



Entity Name: Tucson, Arizona

Contact Name and Title: Donovan Durband

City and State: Tucson, Arizona

Phone: 520-791-5071

Years Serviced: January 14, 2015 - Present

Description of Services: Mobile Payment for Parking

Annual Volume: \$48,000.00 (Passport's annual volume of sales)

Pricing

Item	Includes	Price (\$)
Per Transaction Service and License Fee	<ul style="list-style-type: none"> → Purchase of parking time, paid by the parker → Parking session extensions 	<p>List Price: \$0.35 NCPA Discount Price: \$0.25</p>
Pay by Phone Platform	<ul style="list-style-type: none"> → Android Application → iOS Application → Mobile-Optimized Pay Website → Unlimited ongoing upgrades and enhancements 	Included
System Setup and Training	<ul style="list-style-type: none"> → Zone and rate setup → Rate testing → User role creation and setup → Remote training 	Included
Access to OpsMan	<ul style="list-style-type: none"> → Real time access to active parking sessions → Access to 60+ reports → Ability to define users and roles → Unlimited Rate Builder access → Unlimited access to training videos and FAQs 	Included
Signage and Decals	<ul style="list-style-type: none"> → Aluminum signage deployed city-wide → Decals to place on existing meters and pay stations → Replacement signs → Replacement Decals 	<p>Initial round of signs and decals included</p> <p>List Price: \$35.00* and \$5.00*, respectively. NCPA Discount Price: \$30.00* and \$3.00*</p>
Activation of New Locations	<ul style="list-style-type: none"> → Passport will provide tools and assistance for location additions 	Included

API Library Access	→ Unlimited access to the 35+ active integration Passport has completed	Included
Client Technical Support & Maintenance	→ Unlimited support by email and phone	Included
Second and Third Tier User Technical Support	→ Unlimited support by email and phone	Included

* minimum order quantities apply.

Merchant Processing Costs:

Passport's platform is flexible with regards to the merchant of record ("MOR"), allowing the Client to choose any merchant processor in the market. Passport is also a registered gateway and merchant processor itself. If the Client elects to use Passport as the MOR, all parking fees will be collected by Passport and kept with Passport's merchant bank. Every 30 days, Passport will remit to the Client their portion of the parking revenue (total revenue less transaction and merchant processing costs). Passport's merchant processing rate is 2.9% + \$0.30 per transaction.

The Client may also elect to use a different MOR, in which case the Client will hold all parking fees in their merchant bank, which will be deposited daily. In this scenario, Passport would invoice the Client each month for the transaction fees (convenience fee X number of transactions) and the City would be responsible for all merchant processing fees through its third party vendor.

Custom Development:

Any system-wide improvements or modifications made by Passport to the Software platform will be promptly provided to Provider and will automatically be subject to the terms of this Agreement. The Client may request new features or functionality to be built into the system, and, to the extent that Passport plans to incorporate such requested new features or functionality into the Software, Passport will develop such features and functionality at no cost to the Client. If the Client desires to expedite such development, Passport may, at its sole discretion, charge Provider an expedite fee of two hundred dollars (\$200,00) per development hour necessary to develop the requested features or functionality. If the Client's requested features or functionality are created for the Client's use and not incorporated into the Software, Passport may, at its sole discretion, charge Provider custom development fee of two hundred and fifty dollars (\$250,00) per hour for the development of such features or functionality and a monthly maintenance fee that will be mutually agreed between the Parties and reduced to a written addendum to this Agreement that the Parties must execute.

Warranty

Passport will provide hosting for the Software in accordance with all local laws and regulations. Passport's sole and exclusive obligation in the event of an error or interruption of the Software is to use Passport's best efforts to restore or repair the Software as quickly as practicable.

Passport will provide the Software with uptime of at least ninety-nine percent (99%) calculated over a rolling six-month period ("Uptime Guarantee"). For any month during which system uptime drops below the Uptime Guarantee, Passport will provide a billing credit in an amount equal to: the percentage difference between a) the lowest uptime reached at any point during the month (calculated on a rolling six month period) and b) the Uptime Guarantee multiplied by the total fees payable to Passport for such month. For example, if during a given month the Software uptime fell as low as ninety-five percent (95%) and during that month, the fees payable to Passport were one hundred dollars (\$100.00), Passport would issue a billing credit of four dollars (\$4.00). For the purposes of this Agreement, Uptime is defined as any period of time during which end users of the Software can use the Software to pay for parking, pay for mobile tickets, or issue parking citations, as applicable.

Value Added Products and Services

Citation Management Platform

Passport's Citation Management Platform ("CMP") delivers a flexible and dynamic solution to your parking system. Built on Passport's industry-leading enterprise platform, the City can easily take advantage of cloud-based software technology to streamline services, reduce time and cost, and increase collection rates.

Parking enforcement officers are able to see real-time information on lightweight mobile devices that automatically send data to backend software for a complete view of operations. Passport's CMP is built on the Android operating system, which benefits the City in two ways: first, Android products are more cost effective than large, expensive handhelds or Apple products; and second, updates to the product do not require expensive hardware retrofits, nor does it take weeks for the app store to approve each update as Apple does. Passport's commitment to continuous innovation leads to frequent enhancements and upgrades, pushing each update to the system in a matter of hours or days, depending on the needs of the City.

Automated Process

Ticket Issuance

Passport's ticket issuance software, OpsMan Mobile, is build on the Android Operating System. Parking enforcement officers are able to take advantage of lightweight mobile devices that are connected in real-time to the backend management portal. Each parking enforcement officer can have their own account and ticket flow can be configured to meet the specifications of the City.

More than Just Issuance

Passport's Citation Management Platform offers both flexibility and efficiency to the City's operations. No two operations are the same, so Passport designed its platform to adapt to each city's unique requirements. The CMP offers the following robust feature set to help improve the City's operations:

- Monitoring and electronic chalking
- Issuance flow and data collection
- Reporting incidents in the field
- Adding custom notes and pictures to violations
- Formatting and content of printed violations
- Real time notifications for scofflaw, boot, and tow eligibility
- Reprinting tickets in the field
- Automatic generation of delinquency notifications
- A Mobile friendly payment portal
- A complete appeals process

Flawless Integration

Passport seamlessly integrates with a variety of systems and fully supports the implementation process with a dedicated expert team of engineers. Using real-time and batching capabilities, Passport's CMP integrates easily with other systems to allow for continuous development of new integrations and to meet the future needs of the City's operations.

Increase Collection Yield

Real Time Data

All parking data housed in the Passport system is available in real time, giving the City complete confidence in monitoring mobile and meter payments and dramatically reducing the time it takes to manage handwritten processes.

Once a violation is issued, all information is uploaded immediately and made available for payment. This means that violators are able to view and pay their violations quickly. Ease of payment means more violations are paid in a timely, efficient manner.

Data Analytics

With a cloud-based backend system, the City gets full access to the wealth of data generated when issuing citations. Reports can be run giving a 50,000 foot view of all transactions in the last year or drilling down to a single parking enforcement officer's activities in a particular lot on a particular day. The reports can be scheduled to run daily, weekly, or monthly, giving the City a constant view of the current state of operations. With all of this data at your fingertips, the City can make decisions backed by a wealth of data and analytics.

Mobile Payment for Transit

Passport's mobile ticketing solution is an enterprise platform providing agencies with mobile technology that improves the rider experience, allowing riders to plan, track, and pay for their trip in one simple, secure app. Eliminate the need for costly hardware and gain deep insights into rider patterns with data analytics. Transit agencies can choose between visual inspection of rider's tickets or Passport can easily integrate with a variety of hardware partners.

Mobile Ticketing for Smart Cities

The Agency's point of sale is now everywhere riders are. Mobile ticketing is a cost effective solution that brings speed and efficiency to the system, while delivering easy and simple solutions customers have come to expect in a mobile world.

Plan. Track. Pay.

With Passport's mobile ticketing technology, the entire transportation experience is at each rider's fingertips. Riders can plan their trip, track their travel options in real time, and complete ticket purchases all from their smartphone.

When a rider first opens the app, they will be greeted with a native map that is designed to help those riders that are in a rush, need help finding the best route to their destination, or don't want to register with the app immediately. The following is a walkthrough on how Passport has addressed the needs of riders:

Plan: Passport is integrated with Google Transit, whereby the rider will enter their start and end destination and Google Directions will return available route options. Riders will then plan their route, including walking, transit route, and travel time to meet their individual needs.

Track: Passport integrates with your system's pre-existing real-time feed to provide a real-time bus location overlay on top of Google Maps. Riders will use this information to determine where their bus is currently and when it will arrive at their destination.

Pay: Once the rider has planned and tracked their mode of transportation, they will also be able to purchase the ticket directly from their smartphone. The tickets will be stored in the rider's "Ticket Manager" until they are used or expire. Once the ticket is validated by the transit agency or expires, the ticket will no longer be available in the Ticket Manager.

Registration

All Passport solutions are configured so that the user receives all pertinent information prior to purchasing anything. Potential riders are able to plan and track their trip before they are ever prompted to pay. When a rider decides to purchase a ticket using the Passport app, they will be asked to enter payment information. This information will be tokenized and encrypted for security purposes, but will remain associated with the account, allowing the rider to have a seamless experience the next time they opt to purchase a ticket through the app.

Ticket Manager

After a ticket is purchased, it will be accessible in Ticket Manager along with all other active tickets. Each available ticket will show up in a list format. When a rider selects a ticket to use, they will be prompted to confirm that ticket, thereby reducing the number of unintentionally activated tickets. Once the ticket has been validated or time has expired, the ticket will no longer be available within Ticket Manager.

Fare Validation

Passport's Mobile Payment for Ticketing app allows for both visual and electronic validation. Each ticket will have a dynamic QR code and time and date stamps. The Agency can elect to validate tickets through visual inspection, where a fare inspector will confirm the moving QR code, the current date and time, and the fare type (i.e., student or senior citizens). If the Agency has the appropriate hardware, the Passport app is equipped with QR code, BLE, and NFC scanning capabilities. Currently, NFC scanning is only available through Android devices. The electronic validator can either be mounted or handheld, allowing the fare inspector to walk throughout the vehicle, validating individual tickets.

Passport's electronic validation has been tested and approved to perform transactions in under 500ms. Additionally, Passport's system can handle over 2 billion transactions per year, with no impact on performance. All Passport systems are designed for continuous performance, ensuring that every user has a consistently positive experience.

Eligibility Programs

Strengthen rider loyalty and grow ridership with flexible eligibility programs. Easily integrate the Agency's existing programs and offer riders only the passes they are eligible to purchase. Passport's mobile program options help reduce fraud so that riders cannot share passes. Best of all, the Agency can quickly set up programs and fare types and see data on purchase volumes by program.

Data Analytics

Through Passport's backend system, Operator Management ("OpsMan"), the Agency will have access to a powerful SaaS data and operations tool that empowers decision makers with business intelligence.

Better Communication: Send updates, notifications, schedules, and advertising to riders. Agencies can gain feedback from riders, creating a continuous feedback loop for future improvements.

Better Control: Passport's flexible platform allows the Agency to make changes in the system in real-time. Easily create and edit fare structures, eligibility programs, and manage roles from one central dashboard.


Unified View of Operations: Gain insights with accurate reporting for increased efficiency and improved ROI. Everything is in the Agency's control, including customized configurations based upon the Agency's unique policies.

Required Documents

Clean Air and Water Act & Debarment Notice

I, the Vendor, am in compliance with all applicable standards, orders or regulations issued pursuant to the Clean Air Act of 1970, as Amended (42 U.S. C. 1857 (h), Section 508 of the Clean Water Act, as amended (33 U.S.C. 1368), Executive Order 117389 and Environmental Protection Agency Regulation, 40 CFR Part 15 as required under OMB Circular A-102, Attachment O, Paragraph 14 (1) regarding reporting violations to the grantor agency and to the United States Environment Protection Agency Assistant Administrator for the enforcement.

I hereby further certify that my company has not been debarred, suspended or otherwise ineligible for participation in Federal Assistance programs under Executive Order 12549, "Debarment and Suspension", as described in the Federal Register and Rules and Regulations

Potential Vendor	PassportParking, Inc.
Print Name	Khristian Gutierrez, CBDO
Address	427 Tatnall Street, Ste 27927
City, State, Zip	Wilmington, DE 19801-2230
Authorized signature	
Date	October 27, 2016

Contractor Requirement

Contractor Certification Contractor's Employment Eligibility

By entering the contract, Contractor warrants compliance with the Federal Immigration and Nationality Act (FINA), and all other federal and state immigration laws and regulations. The Contractor further warrants that it is in compliance with the various state statues of the states it is will operate this contract in.

Participating Government Entities including School Districts may request verification of compliance from any Contractor or subcontractor performing work under this Contract. These Entities reserve the right to confirm compliance in accordance with applicable laws.

Should the Participating Entities suspect or find that the Contractor or any of its subcontractors are not in compliance, they may pursue any and all remedies allowed by law, including, but not limited to: suspension of work, termination of the Contract for default, and suspension and/or debarment of the Contractor. All costs necessary to verify compliance are the responsibility of the Contractor.

The offeror complies and maintains compliance with the appropriate statutes which requires compliance with federal immigration laws by State employers, State contractors and State subcontractors in accordance with the E-Verify Employee Eligibility Verification Program.

Contractor shall comply with governing board policy of the NCPA Participating entities in which work is being performed

Fingerprint & Background Checks

If required to provide services on school district property at least five (5) times during a month, contractor shall submit a full set of fingerprints to the school district if requested of each person or employee who may provide such service. Alternately, the school district may fingerprint those persons or employees. An exception to this requirement may be made as authorized in Governing Board policy. The district shall conduct a fingerprint check in accordance with the appropriate state and federal laws of all contractors, subcontractors or vendors and their employees for which fingerprints are submitted to the district. Contractor, subcontractors, vendors and their employees shall not provide services on school district properties until authorized by the District.

The offeror shall comply with fingerprinting requirements in accordance with appropriate statutes in the state in which the work is being performed unless otherwise exempted.

Contractor shall comply with governing board policy in the school district or Participating Entity in which work is being performed

Business Operations in Sudan, Iran

In accordance with A.R.S. 35-391 and A.R.S. 35-393, the Contractor hereby certifies that the contractor does not have scrutinized business operations in Sudan and/or Iran.

Authorized signature



Date

October 27, 2016

Antitrust Certification Statements (Tex. Government Code § 2155.005)

I affirm under penalty of perjury of the laws of the State of Texas that:

- (4) I am duly authorized to execute this contract on my own behalf or on behalf of the company, corporation, firm, partnership or individual (Company) listed below;
- (2) In connection with this bid, neither I nor any representative of the Company has violated any provision of the Texas Free Enterprise and Antitrust Act, Tex. Bus. & Comm. Code Chapter 15;
- (3) In connection with this bid, neither I nor any representative of the Company has violated any federal antitrust law; and
- (4) Neither I nor any representative of the Company has directly or indirectly communicated any of the contents of this bid to a competitor of the Company or any other company, corporation, firm, partnership or individual engaged in the same line of business as the Company.

Company name	PassportParking, Inc.
Address	427 Tatnall Street, Ste. 27927
City/State/Zip	Wilmington, DE 19801-2230
Telephone No.	(302) 543-2882
Fax No.	(888) 804-1783
Email address	rfp@passportinc.com
Printed name	Khristian.Gutierrez@passportinc.com
Position with company	Chief Business Development Officer
Authorized signature	

FEMA Standard Terms and Conditions Addendum for Contracts and Grants

If any purchase made under the Master Agreement is funded in whole or in part by Federal Emergency Management Agency ("FEMA") grants, Contractor shall comply with all federal laws and regulations applicable to the receipt of FEMA grants, including, but not limited to the contractual procedures set forth in Title 44 of the Code of Federal Regulations, Part 13 ("44 CFR 13").

In addition, Contractor agrees to the following specific provisions:

- 1) Pursuant to 44 CFR 13.36(i)(1), University is entitled to exercise all administrative, contractual, or other remedies permitted by law to enforce Contractor's compliance with the terms of this Master Agreement, including but not limited to those remedies set forth at 44 CFR 13.43.
- 2) Pursuant to 44 CFR 13.36(i)(2), University may terminate the Master Agreement for cause or convenience in accordance with the procedures set forth in the Master Agreement and those provided by 44 CFR 13.44.
- 3) Pursuant to 44 CFR 13.36(i)(3)-(6)(12), and (13), Contractor shall comply with the following federal laws:
 - a. Executive Order 11246 of September 24, 1965, entitled "Equal Employment Opportunity," as amended by Executive Order 11375 of October 13, 1967, and as supplemented in Department of Labor ("DOL") regulations (41 CFR Ch. 60);
 - b. Copeland "Anti-Kickback" Act (18 U.S.C. 874), as supplemented in DOL regulations (29 CFR Part 3);
 - c. Davis-Bacon Act (40 U.S.C. 276a-276a-7) as supplemented by DOL regulations (29 CFR Part 5);
 - d. Section 103 and 107 of the Contract Work Hours and Safety Standards Act (40 U.S.C. 327-30) as supplemented by DOL regulations (29 CFR Part 5);
 - e. Section 306 of the Clean Air Act (42 U.S.C. 1857(h), section 508 of the Clean Water Act (33 U.S.C. 1368), Executive Order 11738, and Environmental Protection Agency regulations (40 CFR part 15); and
 - f. Mandatory standards and policies relating to energy efficiency which are contained in the state energy conservation plan issued in compliance with the Energy Policy and Conservation Act (Pub. L.94-163, 89 Stat. 871).
- 4) Pursuant to 44 CFR 13.36(i)(7), Contractor shall comply with FEMA requirements and regulations pertaining to reporting, including but not limited to those set forth at 44 CFR 40 and 41.
- 5) Pursuant to 44 CFR 13.36(i)(8), Contractor agrees to the following provisions regarding patents:
 - a. All rights to inventions and/or discoveries that arise or are developed, in the course of or under this Agreement, shall belong to the participating agency and be disposed of in accordance with the participating agency's policy. The participating agency, at its own discretion, may file for patents in connection with all rights to any such inventions and/or discoveries.
- 6) Pursuant to 44 CFR 13.36(i)(9), Contractor agrees to the following provisions regarding copyrights:
 - a. If this Agreement results in any copyrightable material or inventions, in accordance with 44 CFR 13.34, FEMA reserves a royalty-free, nonexclusive, and irrevocable license to reproduce, publish or otherwise use, for Federal Government purposes:
 - 1) The copyright in any work developed under a grant or contract; and
 - 2) Any rights of copyright to which a grantee or a contractor purchases ownership with grant support.
- 7) Pursuant to 44 CFR 13.36(i)(10), Contractor shall maintain any books, documents, papers, and records of the Contractor which are directly pertinent to this Master Agreement. At any time during normal business hours and as often as the participating agency deems necessary, Contractor shall permit participating agency, FEMA, the Comptroller General of United States, or any of their duly authorized representatives to inspect and photocopy such records for the purpose of making audit, examination, excerpts, and transcriptions.
- 8) Pursuant to 44 CFR 13.36(i)(11), Contractor shall retain all required records for three years after FEMA or participating agency makes final payments and all other pending matters are closed. In addition, Contractor shall comply with record retention requirements set forth in 44 CFR 13.42.

Required Clauses for Federal Assistance Provided by FTA

ACCESS TO RECORDS AND REPORTS

Contractor agrees to:

- a) Maintain all books, records, accounts and reports required under this Contract for a period of not less than three (3) years after the date of termination or expiration of this Contract or any extensions thereof except in the event of litigation or settlement of claims arising from the performance of this Contract, in which case Contractor agrees to maintain same until Public Agency, the FTA Administrator, the Comptroller General, or any of their duly authorized representatives, have disposed of all such litigation, appeals, claims or exceptions related thereto.
- b) Permit any of the foregoing parties to inspect all work, materials, payrolls, and other data and records with regard to the Project, and to audit the books, records, and accounts with regard to the Project and to reproduce by any means whatsoever or to copy excerpts and transcriptions as reasonably needed for the purpose of audit and examination.

FTA does not require the inclusion of these requirements of Article 1.01 in subcontracts. Reference 49 CFR 18.39 (i)(11).

CIVIL RIGHTS / TITLE VI REQUIREMENTS

- 1) Non-discrimination. In accordance with Title VI of the Civil Rights Act of 1964, as amended, 42 U.S.C. § 2000d, Section 303 of the Age Discrimination Act of 1975, as amended, 42 U.S.C. § 6102, Section 202 of the Americans with Disabilities Act of 1990, as amended, 42 U.S.C. § 12132, and Federal Transit Law at 49 U.S.C. § 5332, Contractor or subcontractor agrees that it will not discriminate against any employee or applicant for employment because of race, color, creed, national origin, sex, marital status age, or disability. In addition, Contractor agrees to comply with applicable Federal implementing regulations and other implementing requirements FTA may issue.
- 2) Equal Employment Opportunity. The following Equal Employment Opportunity requirements apply to this Contract:
 - a. Race, Color, Creed, National Origin, Sex. In accordance with Title VII of the Civil Rights Act, as amended, 42 U.S.C. § 2000e, and Federal Transit Law at 49 U.S.C. § 5332, the Contractor agrees to comply with all applicable Equal Employment Opportunity requirements of U.S. Dept. of Labor regulations, "Office of Federal Contract Compliance Programs, Equal Employment Opportunity, Department of Labor, 41 CFR, Parts 60 *et seq.*", and with any applicable Federal statutes, executive orders, regulations, and Federal policies that may in the future affect construction activities undertaken in the course of this Project. Contractor agrees to take affirmative action to ensure that applicants are employed, and that employees are treated during employment, without regard to their race, color, creed, national origin, sex, marital status, or age. Such action shall include, but not be limited to, the following: employment, upgrading, demotion or transfer, recruitment or recruitment advertising, layoff or termination, rates of pay or other forms of compensation; and selection for training, including apprenticeship. In addition, Contractor agrees to comply with any implementing requirements FTA may issue.
 - b. Age. In accordance with the Age Discrimination in Employment Act (ADEA) of 1967, as amended, 29 U.S.C. Sections 621 through 634, and Equal Employment Opportunity Commission (EEOC) implementing regulations, "Age Discrimination in Employment Act", 29 CFR Part 1625, prohibit employment discrimination by Contractor against individuals on the basis of age, including present and prospective employees. In addition, Contractor agrees to comply with any implementing requirements FTA may issue.

- c. Disabilities. In accordance with Section 102 of the Americans with Disabilities Act of 1990, as amended (ADA), 42 U.S.C. Sections 12101 *et seq.*, prohibits discrimination against qualified individuals with disabilities in programs, activities, and services, and imposes specific requirements on public and private entities. Contractor agrees that it will comply with the requirements of the Equal Employment Opportunity Commission (EEOC), "Regulations to Implement the Equal Employment Provisions of the Americans with Disabilities Act," 29 CFR, Part 1630, pertaining to employment of persons with disabilities and with their responsibilities under Titles I through V of the ADA in employment, public services, public accommodations, telecommunications, and other provisions.
- d. Segregated Facilities. Contractor certifies that their company does not and will not maintain or provide for their employees any segregated facilities at any of their establishments, and that they do not and will not permit their employees to perform their services at any location under the Contractor's control where segregated facilities are maintained. As used in this certification the term "segregated facilities" means any waiting rooms, work areas, restrooms and washrooms, restaurants and other eating areas, parking lots, drinking fountains, recreation or entertainment areas, transportation, and housing facilities provided for employees which are segregated by explicit directive or are in fact segregated on the basis of race, color, religion or national origin because of habit, local custom, or otherwise. Contractor agrees that a breach of this certification will be a violation of this Civil Rights clause.
- 3) Solicitations for Subcontracts, Including Procurements of Materials and Equipment. In all solicitations, either by competitive bidding or negotiation, made by Contractor for work to be performed under a subcontract, including procurements of materials or leases of equipment, each potential subcontractor or supplier shall be notified by Contractor of Contractor's obligations under this Contract and the regulations relative to non-discrimination on the grounds of race, color, creed, sex, disability, age or national origin.
- 4) Sanctions of Non-Compliance. In the event of Contractor's non-compliance with the non-discrimination provisions of this Contract, Public Agency shall impose such Contract sanctions as it or the FTA may determine to be appropriate, including, but not limited to: 1) Withholding of payments to Contractor under the Contract until Contractor complies, and/or; 2) Cancellation, termination or suspension of the Contract, in whole or in part.

Contractor agrees to include the requirements of this clause in each subcontract financed in whole or in part with Federal assistance provided by FTA, modified only if necessary to identify the affected parties.

DISADVANTAGED BUSINESS PARTICIPATION

This Contract is subject to the requirements of Title 49, Code of Federal Regulations, Part 26, "*Participation by Disadvantaged Business Enterprises in Department of Transportation Financial Assistance Programs*", therefore, it is the policy of the Department of Transportation (DOT) to ensure that Disadvantaged Business Enterprises (DBEs), as defined in 49 CFR Part 26, have an equal opportunity to receive and participate in the performance of DOT-assisted contracts.

- 1) Non-Discrimination Assurances. Contractor or subcontractor shall not discriminate on the basis of race, color, national origin, or sex in the performance of this Contract. Contractor shall carry out all applicable requirements of 49 CFR Part 26 in the award and administration of DOT-assisted contracts. Failure by Contractor to carry out these requirements is a material breach of this Contract, which may result in the termination of this Contract or other such remedy as public agency deems appropriate. Each subcontract Contractor signs with a subcontractor must include the assurance in this paragraph. (See 49 CFR 26.13(b)).
- 2) Prompt Payment. Contractor is required to pay each subcontractor performing Work under this prime Contract for satisfactory performance of that work no later than thirty (30) days after Contractor's receipt of payment for that Work from public agency. In addition, Contractor is required to return any retainage payments to those subcontractors within thirty (30) days after the subcontractor's work related to this

Contract is satisfactorily completed and any liens have been secured. Any delay or postponement of payment from the above time frames may occur only for good cause following written approval of public agency. This clause applies to both DBE and non-DBE subcontractors. Contractor must promptly notify public agency whenever a DBE subcontractor performing Work related to this Contract is terminated or fails to complete its Work, and must make good faith efforts to engage another DBE subcontractor to perform at least the same amount of work. Contractor may not terminate any DBE subcontractor and perform that Work through its own forces, or those of an affiliate, without prior written consent of public agency.

- 3) DBE Program. In connection with the performance of this Contract, Contractor will cooperate with public agency in meeting its commitments and goals to ensure that DBEs shall have the maximum practicable opportunity to compete for subcontract work, regardless of whether a contract goal is set for this Contract. Contractor agrees to use good faith efforts to carry out a policy in the award of its subcontracts, agent agreements, and procurement contracts which will, to the fullest extent, utilize DBEs consistent with the efficient performance of the Contract.

ENERGY CONSERVATION REQUIREMENTS

Contractor agrees to comply with mandatory standards and policies relating to energy efficiency which are contained in the State energy conservation plans issued under the Energy Policy and Conservation Act, as amended, 42 U.S.C. Sections 6321 *et seq.* and 41 CFR Part 301-10.

FEDERAL CHANGES

Contractor shall at all times comply with all applicable FTA regulations, policies, procedures and directives, including without limitation those listed directly or by reference in the Contract between public agency and the FTA, as they may be amended or promulgated from time to time during the term of this contract. Contractor's failure to so comply shall constitute a material breach of this Contract.

INCORPORATION OF FEDERAL TRANSIT ADMINISTRATION (FTA) TERMS

The provisions include, in part, certain Standard Terms and Conditions required by the U.S. Department of Transportation (DOT), whether or not expressly set forth in the preceding Contract provisions. All contractual provisions required by the DOT, as set forth in the most current FTA Circular 4220.1F, dated November 1, 2008, are hereby incorporated by reference. Anything to the contrary herein notwithstanding, all FTA mandated terms shall be deemed to control in the event of a conflict with other provisions contained in this Contract. Contractor agrees not to perform any act, fail to perform any act, or refuse to comply with any public agency requests that would cause public agency to be in violation of the FTA terms and conditions.

NO FEDERAL GOVERNMENT OBLIGATIONS TO THIRD PARTIES

Agency and Contractor acknowledge and agree that, absent the Federal Government's express written consent and notwithstanding any concurrence by the Federal Government in or approval of the solicitation or award of the underlying Contract, the Federal Government is not a party to this Contract and shall not be subject to any obligations or liabilities to agency, Contractor, or any other party (whether or not a party to that contract) pertaining to any matter resulting from the underlying Contract.

Contractor agrees to include the above clause in each subcontract financed in whole or in part with federal assistance provided by the FTA. It is further agreed that the clause shall not be modified, except to identify the subcontractor who will be subject to its provisions.

PROGRAM FRAUD AND FALSE OR FRAUDULENT STATEMENTS

Contractor acknowledges that the provisions of the Program Fraud Civil Remedies Act of 1986, as amended, 31 U.S.C. §§ 3801 et seq. and U.S. DOT regulations, "Program Fraud Civil Remedies," 49 CFR Part 31, apply to its actions pertaining to this Contract. Upon execution of the underlying Contract, Contractor certifies or affirms the truthfulness and accuracy of any statement it has made, it makes, it may make, or causes to be made, pertaining to the underlying Contract or the FTA assisted project for which this Contract Work is being performed.

In addition to other penalties that may be applicable, Contractor further acknowledges that if it makes, or causes to be made, a false, fictitious, or fraudulent claim, statement, submission, or certification, the Federal Government reserves the right to impose the penalties of the Program Fraud Civil Remedies Act of 1986 on Contractor to the extent the Federal Government deems appropriate.

Contractor also acknowledges that if it makes, or causes to be made, a false, fictitious, or fraudulent claim, statement, submission, or certification to the Federal Government under a contract connected with a project that is financed in whole or in part with Federal assistance originally awarded by FTA under the authority of 49 U.S.C. § 5307, the Government reserves the right to impose the penalties of 18 U.S.C. § 1001 and 49 U.S.C. § 5307 (n)(1) on the Contractor, to the extent the Federal Government deems appropriate.

Contractor agrees to include the above clauses in each subcontract financed in whole or in part with Federal assistance provided by FTA. It is further agreed that the clauses shall not be modified, except to identify the subcontractor who will be subject to the provisions.

State Notice Addendum

Pursuant to certain state notice provisions the following public agencies and political subdivisions of the referenced public agencies are eligible to access the contract award made pursuant to this solicitation. Public agencies and political subdivisions are hereby given notice of the foregoing request for proposal for purposes of complying with the procedural requirement of said statutes:

Nationwide: http://www.usa.gov/Agencies/Local_Government/Cities.shtml

Other States: Cities, Towns, Villages, and Boroughs

<p>No.</p> <p>Cities, Towns, Villages and Boroughs in Oregon</p> <p>1 CEDAR MILL COMMUNITY LIBRARY</p> <p>2 CITY COUNTY INSURANCE SERVICES</p> <p>3 CITY OF ADAIR VILLAGE</p> <p>4 CITY OF ALBANY</p> <p>5 CITY OF ASHLAND</p> <p>6 CITY OF ASTORIA OREGON</p> <p>7 CITY OF AUMSVILLE</p> <p>8 CITY OF AURORA</p> <p>9 CITY OF BEAVERTON</p> <p>10 CITY OF BOARDMAN</p> <p>11 CITY OF BURNS</p> <p>12 CITY OF CANBY</p> <p>13 CITY OF CANNON BEACH OR</p> <p>14 CITY OF CANYONVILLE</p> <p>15 CITY OF CENTRAL POINT POLICE DEPARTMENT</p> <p>16 CITY OF CLATSKANIE</p> <p>17 CITY OF COBURG</p> <p>18 CITY OF CONDON</p> <p>19 CITY OF COOS BAY</p> <p>20 CITY OF CORVALLIS</p> <p>21 CITY OF COTTAGE GROVE</p> <p>22 CITY OF CRESWELL</p> <p>23 CITY OF DALLAS</p> <p>24 CITY OF DAMASCUS</p> <p>25 CITY OF DUNDEE</p> <p>26 CITY OF EAGLE POINT</p> <p>27 CITY OF ECHO</p> <p>28 CITY OF ESTACADA</p> <p>29 CITY OF EUGENE</p> <p>30 CITY OF FAIRVIEW</p> <p>31 CITY OF FALLS CITY</p> <p>32 CITY OF GATES</p> <p>33 CITY OF GEARHART</p> <p>34 CITY OF GERVAIS</p> <p>35 CITY OF GOLD HILL</p> <p>36 CITY OF GRANTS PASS</p> <p>37 CITY OF GRESHAM</p> <p>38 CITY OF HAPPY VALLEY</p> <p>39 CITY OF HILLSBORO</p> <p>40 CITY OF HOOD RIVER</p> <p>41 CITY OF JOHN DAY</p> <p>42 CITY OF KLAMATH FALLS</p> <p>43 CITY OF LA GRANDE</p> <p>44 CITY OF LAKE OSWEGO</p> <p>45 CITY OF LAKESIDE</p> <p>46 CITY OF LEBANON</p> <p>47 CITY OF MALIN</p> <p>48 CITY OF MCMINNVILLE</p> <p>49 CITY OF MEDFORD</p> <p>50 CITY OF MILL CITY</p> <p>51 CITY OF MILLERSBURG</p> <p>52 CITY OF MILWAUKIE</p> <p>53 CITY OF MORO</p> <p>54 CITY OF MOSIER</p> <p>55 CITY OF NEWBERG</p> <p>56 CITY OF NORTH PLAINS</p> <p>57 CITY OF OREGON CITY</p>	<p>58 CITY OF PHOENIX</p> <p>59 CITY OF PILOT ROCK</p> <p>60 CITY OF PORT ORFORD</p> <p>61 CITY OF PORTLAND</p> <p>62 CITY OF POWERS</p> <p>63 CITY OF REDMOND</p> <p>64 CITY OF REEDSPORT</p> <p>65 CITY OF RIDDLE</p> <p>66 CITY OF SALEM</p> <p>67 CITY OF SANDY</p> <p>68 CITY OF SANDY</p> <p>69 CITY OF SCAPPOOSE</p> <p>70 CITY OF SEASIDE</p> <p>71 CITY OF SHADY COVE</p> <p>72 CITY OF SHERWOOD</p> <p>73 CITY OF SPRINGFIELD</p> <p>74 CITY OF ST. PAUL</p> <p>75 CITY OF STAYTON</p> <p>76 CITY OF TIGARD, OREGON</p> <p>77 CITY OF TUALATIN, OREGON</p> <p>78 CITY OF WARRENTON</p> <p>79 CITY OF WEST LINN/PARKS</p> <p>80 CITY OF WILSONVILLE</p> <p>81 CITY OF WINSTON</p> <p>82 CITY OF WOOD VILLAGE</p> <p>83 CITY OF WOODBURN</p> <p>84 CITY OF YACHATS</p> <p>85 FLORENCE AREA CHAMBER OF COMMERCE</p> <p>86 GASTON RURAL FIRE DEPARTMENT</p> <p>87 GLADSTONE POLICE DEPARTMENT</p> <p>88 HOUSING AUTHORITY OF THE CITY OF SALEM</p> <p>89 KEIZER POLICE DEPARTMENT</p> <p>90 LEAGUE OF OREGON CITIES</p> <p>91 MALIN COMMUNITY PARK AND RECREATION DISTRICT</p> <p>92 METRO</p> <p>93 MONMOUTH - INDEPENDENCE NETWORK</p> <p>94 PORTLAND DEVELOPMENT COMMISSION</p> <p>95 RAINIER POLICE DEPARTMENT</p> <p>96 RIVERGROVE WATER DISTRICT</p> <p>97 SUNSET EMPIRE PARK AND RECREATION</p> <p>98 THE NEWPORT PARK AND RECREATION CENTER</p> <p>99 TILLAMOOK PEOPLES UTILITY DISTRICT</p> <p>100 TUALATIN VALLEY FIRE & RESCUE</p> <p>101 WEST VALLEY HOUSING AUTHORITY</p> <p>No.</p> <p>Counties and Parishes</p> <p>1 ASSOCIATION OF OREGON COUNTIES</p> <p>2 BENTON COUNTY</p> <p>3 CLACKAMAS COUNTY DEPT OF TRANSPORTATION</p> <p>4 CLATSOP COUNTY</p> <p>5 COLUMBIA COUNTY, OREGON</p> <p>6 COOS COUNTY HIGHWAY DEPARTMENT</p> <p>7 CROOK COUNTY ROAD DEPARTMENT</p> <p>8 CURRY COUNTY OREGON</p> <p>9 DESCHUTES COUNTY</p> <p>10 DOUGLAS COUNTY</p> <p>11 GILLIAM COUNTY</p> <p>12 GILLIAM COUNTY OREGON</p> <p>13 GRANT COUNTY, OREGON</p> <p>14 HARNEY COUNTY SHERIFFS OFFICE</p>
--	---

15	HOOD RIVER COUNTY	10	CANBY SCHOOL DISTRICT
16	HOUSING AUTHORITY OF CLACKAMAS COUNTY	11	CANYONVILLE CHRISTIAN ACADEMY
17	JACKSON COUNTY HEALTH AND HUMAN SERVICES	12	CASCADE SCHOOL DISTRICT
18	JEFFERSON COUNTY	13	CASCADES ACADEMY OF CENTRAL OREGON
19	KLAMATH COUNTY VETERANS SERVICE OFFICE	14	CENTENNIAL SCHOOL DISTRICT
20	LAKE COUNTY	15	CENTRAL CATHOLIC HIGH SCHOOL
21	LANE COUNTY	16	CENTRAL POINT SCHOOL DISTRICT NO. 6
22	LINCOLN COUNTY	17	CENTRAL SCHOOL DISTRICT 13J
23	LINN COUNTY	18	CLACKAMAS EDUCATION SERVICE DISTRICT
24	MARION COUNTY , SALEM, OREGON	19	COOS BAY SCHOOL DISTRICT
25	MORROW COUNTY	20	COOS BAY SCHOOL DISTRICT NO.9
26	MULTNOMAH COUNTY	21	COQUILLE SCHOOL DISTRICT 8
27	MULTNOMAH COUNTY	22	COUNTY OF YAMHILL SCHOOL DISTRICT 29
28	MULTNOMAH LAW LIBRARY	23	CRESWELL SCHOOL DISTRICT
29	NAMI LANE COUNTY	24	CROSSROADS CHRISTIAN SCHOOL
30	POLK COUNTY	25	CULVER SCHOOL DISTRICT NO.
31	SHERMAN COUNTY	26	DALLAS SCHOOL DISTRICT NO. 2
32	UMATILLA COUNTY, OREGON	27	DAVID DOUGLAS SCHOOL DISTRICT
33	UNION COUNTY	28	DAYTON SCHOOL DISTRICT NO.8
34	WALLOWA COUNTY	29	DE LA SALLE N CATHOLIC HS
35	WASCO COUNTY	30	DESCHUTES COUNTY SD NO.6 - SISTERS SD
36	WASHINGTON COUNTY	31	DOUGLAS COUNTY SCHOOL DISTRICT 116
37	YAMHILL COUNTY	32	DOUGLAS EDUCATION SERVICE DISTRICT
1	BOARD OF WATER SUPPLY	33	DUFUR SCHOOL DISTRICT NO.29
2	COUNTY OF HAWAII	34	ELKTON SCHOOL DISTRICT NO.34
3	MAUI COUNTY COUNCIL	35	ESTACADA SCHOOL DISTRICT NO.108
No.	Higher Education	36	FOREST GROVE SCHOOL DISTRICT
1	BIRTHINGWAY COLLEGE OF MIDWIFERY	37	GASTON SCHOOL DISTRICT 511J
2	BLUE MOUNTAIN COMMUNITY COLLEGE	38	GEN CONF OF SDA CHURCH WESTERN OR
3	CENTRAL OREGON COMMUNITY COLLEGE	39	GLADSTONE SCHOOL DISTRICT
4	CHEMEKETA COMMUNITY COLLEGE	40	GLENDALE SCHOOL DISTRICT
5	CLACKAMAS COMMUNITY COLLEGE	41	GLIDE SCHOOL DISTRICT NO.12
6	COLUMBIA GORGE COMMUNITY COLLEGE	42	GRANTS PASS SCHOOL DISTRICT 7
7	GEORGE FOX UNIVERSITY	43	GREATER ALBANY PUBLIC SCHOOL DISTRICT
8	KLAMATH COMMUNITY COLLEGE DISTRICT	44	GRESHAM-BARLOW SCHOOL DISTRICT
9	LANE COMMUNITY COLLEGE	45	HARNEY COUNTY SCHOOL DIST. NO.3
10	LEWIS AND CLARK COLLEGE	46	HARNEY EDUCATION SERVICE DISTRICT
11	LINFIELD COLLEGE	47	HEAD START OF LANE COUNTY
12	LINN-BENTON COMMUNITY COLLEGE	48	HERITAGE CHRISTIAN SCHOOL
13	MARYLHURST UNIVERSITY	49	HIGH DESERT EDUCATION SERVICE DISTRICT
14	MT. HOOD COMMUNITY COLLEGE	50	HOOD RIVER COUNTY SCHOOL DISTRICT
15	MULTNOMAH BIBLE COLLEGE	51	JACKSON CO SCHOOL DIST NO.9
16	NATIONAL COLLEGE OF NATURAL MEDICINE	52	JEFFERSON COUNTY SCHOOL DISTRICT 509-J
17	NORTHWEST CHRISTIAN COLLEGE	53	JEFFERSON SCHOOL DISTRICT
18	OREGON HEALTH AND SCIENCE UNIVERSITY	54	KLAMATH FALLS CITY SCHOOLS
19	OREGON UNIVERSITY SYSTEM	55	LA GRANDE SCHOOL DISTRICT
20	PACIFIC UNIVERSITY	56	LAKE OSWEGO SCHOOL DISTRICT 7J
21	PORTLAND COMMUNITY COLLEGE	57	LANE COUNTY SCHOOL DISTRICT 4J
22	PORTLAND STATE UNIV.	58	LANE COUNTY SCHOOL DISTRICT 69
23	REED COLLEGE	59	LEBANON COMMUNITY SCHOOLS NO.9
24	ROGUE COMMUNITY COLLEGE	60	LINCOLN COUNTY SCHOOL DISTRICT
25	SOUTHWESTERN OREGON COMMUNITY COLLEGE	61	LINN CO. SCHOOL DIST. 95C - SCIO SD
26	TILLAMOOK BAY COMMUNITY COLLEGE	62	LOST RIVER JR/SR HIGH SCHOOL
27	UMPQUA COMMUNITY COLLEGE	63	LOWELL SCHOOL DISTRICT NO.71
28	WESTERN STATES CHIROPRACTIC COLLEGE	64	MARION COUNTY SCHOOL DISTRICT 103 - WASHINGTON ES
29	WILLAMETTE UNIVERSITY	65	MCMINNVILLE SCHOOL DISTRICT NO.40
1	ARGOSY UNIVERSITY	66	MEDFORD SCHOOL DISTRICT 549C
2	BRIGHAM YOUNG UNIVERSITY - HAWAII	67	MITCH CHARTER SCHOOL
3	COLLEGE OF THE MARSHALL ISLANDS	68	MOLALLA RIVER ACADEMY
4	RESEARCH CORPORATION OF THE UNIVERSITY OF HAWAII	69	MOLALLA RIVER SCHOOL DISTRICT NO.35
5	UNIVERSITY OF HAWAII AT MANOA	70	MONROE SCHOOL DISTRICT NO.1J
No.	K - 12	71	MORROW COUNTY SCHOOL DISTRICT
1	ARCHBISHOP FRANCIS NORBERT BLANCHET SCHOOL	72	MT. ANGEL SCHOOL DISTRICT NO.91
2	BAKER COUNTY SCHOOL DIST. 16J - MALHEUR ESD	73	MT.SCOTT LEARNING CENTERS
3	BAKER SCHOOL DISTRICT 5-J	74	MULTISENSORY LEARNING ACADEMY
4	BANDON SCHOOL DISTRICT	75	MULTNOMAH EDUCATION SERVICE DISTRICT
5	BANKS SCHOOL DISTRICT	76	MYRTLE POINT SCHOOL DISTRICT NO.41
6	BEAVERTON SCHOOL DISTRICT	77	NEAH-KAH-NIE DISTRICT NO.56
7	BEND / LA PINE SCHOOL DISTRICT	78	NESTUCCA VALLEY SCHOOL DISTRICT NO.101
8	BEND-LA PINE SCHOOL DISTRICT	79	NOBEL LEARNING COMMUNITIES
9	BROOKING HARBOR SCHOOL DISTRICT NO.17-C	80	NORTH BEND SCHOOL DISTRICT 13
		81	NORTH CLACKAMAS SCHOOL DISTRICT

82	NORTH SANTIAM SCHOOL DISTRICT 29J	23	CATHOLIC CHARITIES
83	NORTH WASCO CTY SCHOOL DISTRICT 21 - CHENOWITH	24	CATHOLIC COMMUNITY SERVICES
84	NORTHWEST REGIONAL EDUCATION SERVICE DISTRICT	25	CENTER FOR RESEARCH TO PRACTICE
85	NYSSA SCHOOL DISTRICT NO. 26	26	CENTRAL BIBLE CHURCH
86	ONTARIO MIDDLE SCHOOL	27	CENTRAL CITY CONCERN
87	OREGON TRAIL SCHOOL DISTRICT NO.46	28	CENTRAL DOUGLAS COUNTY FAMILY YMCA
88	OUR LADY OF THE LAKE SCHOOL	29	CENTRAL OREGON COMMUNITY ACTION AGENCY NETWORK
89	PHILOMATH SCHOOL DISTRICT	30	CHILDEPEACE MONTESSORI
90	PHOENIX-TALENT SCHOOL DISTRICT NO.4	31	CITY BIBLE CHURCH
91	PORTLAND ADVENTIST ACADEMY	32	CLACKAMAS RIVER WATER
92	PORTLAND JEWISH ACADEMY	33	CLASSROOM LAW PROJECT
93	PORTLAND PUBLIC SCHOOLS	34	COAST REHABILITATION SERVICES
94	RAINIER SCHOOL DISTRICT	35	COLLEGE HOUSING NORTHWEST
95	REDMOND SCHOOL DISTRICT	36	COLUMBIA COMMUNITY MENTAL HEALTH
96	REEDSPORT SCHOOL DISTRICT	37	COMMUNITY ACTION ORGANIZATION
97	REYNOLDS SCHOOL DISTRICT	38	COMMUNITY ACTION TEAM, INC.
98	ROGUE RIVER SCHOOL DISTRICT NO.35	39	COMMUNITY CANCER CENTER
99	ROSEBURG PUBLIC SCHOOLS	40	COMMUNITY HEALTH CENTER, INC
100	SALEM-KEIZER PUBLIC SCHOOLS	41	COMMUNITY VETERINARY CENTER
101	SCAPPOOSE SCHOOL DISTRICT 1J	42	CONFEDERATED TRIBES OF GRAND RONDE
102	SEASIDE SCHOOL DISTRICT 10	43	CONSERVATION BIOLOGY INSTITUTE
103	SEVEN PEAKS SCHOOL	44	CONTEMPORARY CRAFTS MUSEUM AND GALLERY
104	SHERWOOD SCHOOL DISTRICT 88J	45	CORVALLIS MOUNTAIN RESCUE UNIT
105	SILVER FALLS SCHOOL DISTRICT	46	COVENANT CHRISTIAN HOOD RIVER
106	SIUSLAW SCHOOL DISTRICT	47	COVENANT RETIREMENT COMMUNITIES
107	SOUTH COAST EDUCATION SERVICE DISTRICT	48	DECISION SCIENCE RESEARCH INSTITUTE, INC.
108	SOUTH LANE SCHOOL DISTRICT 45J3	49	DELIGHT VALLEY CHURCH OF CHRIST
109	SOUTHERN OREGON EDUCATION SERVICE DISTRICT	50	DOGS FOR THE DEAF, INC.
110	SOUTHWEST CHARTER SCHOOL	51	DOUGLAS ELECTRIC COOPERATIVE, INC.
111	SPRINGFIELD SCHOOL DISTRICT NO.19	52	EAST HILL CHURCH
112	STANFIELD SCHOOL DISTRICT	53	EAST SIDE FOURSQUARE CHURCH
113	SWEET HOME SCHOOL DISTRICT NO.55	54	EAST WEST MINISTRIES INTERNATIONAL
114	THE CATLIN GABEL SCHOOL	55	EDUCATIONAL POLICY IMPROVEMENT CENTER
115	TIGARD-TUALATIN SCHOOL DISTRICT	56	ELMIRA CHURCH OF CHRIST
116	UMATILLA-MORROW ESD	57	EMERALD PUD
117	VERNONIA SCHOOL DISTRICT 47J	58	EMMAUS CHRISTIAN SCHOOL
118	WEST HILLS COMMUNITY CHURCH	59	EN AVANT, INC.
119	WEST LINN WILSONVILLE SCHOOL DISTRICT	60	ENTERPRISE FOR EMPLOYMENT AND EDUCATION
120	WHITEAKER MONTESSORI SCHOOL	61	EUGENE BALLET COMPANY
121	YONCALLA SCHOOL DISTRICT NO.32	62	EUGENE SYMPHONY ASSOCIATION, INC.
1	CONGREGATION OF CHRISTIAN BROTHERS OF HAWAII, INC.	63	EUGENE WATER & ELECTRIC BOARD
2	EMMANUAL LUTHERAN SCHOOL	64	EVERGREEN AVIATION MUSEUM AND CAP. MICHAEL KING.
3	HANAHAU'OLI SCHOOL	65	FAIR SHARE RESEARCH AND EDUCATION FUND
4	HAWAII TECHNOLOGY ACADEMY	66	FAITH CENTER
5	ISLAND SCHOOL	67	FAITHFUL SAVIOR MINISTRIES
6	KAMEHAMEHA SCHOOLS	68	FAMILIES FIRST OF GRANT COUNTY, INC.
7	KE KULA O S. M. KAMAKAU	69	FANCONI ANEMIA RESEARCH FUND INC.
8	MARYKNOLL SCHOOL	70	FARMWORKER HOUSING DEV CORP
9	PACIFIC BUDDHIST ACADEMY	71	FIRST CHURCH OF THE NAZARENE
No.	Nonprofit & Other	72	FIRST UNITARIAN CHURCH
1	211INFO	73	FORD FAMILY FOUNDATION
2	ACUMENTRA HEALTH	74	FOUNDATIONS FOR A BETTER OREGON
3	ADDICTIONS RECOVERY CENTER, INC	75	FRIENDS OF THE CHILDREN
4	ALLFOURONE/CRESTVIEW CONFERENCE CTR.	76	GATEWAY TO COLLEGE NATIONAL NETWORK
5	ALVORD-TAYLOR INDEPENDENT LIVING SERVICES	77	GOAL ONE COALITION
6	ALZHEIMERS NETWORK OF OREGON	78	GOLD BEACH POLICE DEPARTMENT
7	ASHLAND COMMUNITY HOSPITAL	79	GOOD SHEPHERD COMMUNITIES
8	ATHENA LIBRARY FRIENDS ASSOCIATION	80	GOODWILL INDUSTRIES OF LANE AND SOUTH COAST COUNTIES
9	BARLOW YOUTH FOOTBALL	81	GRANT PARK CHURCH
10	BAY AREA FIRST STEP, INC.	82	GRANTS PASS MANAGEMENT SERVICES, DBA
11	BENTON HOSPICE SERVICE	83	GREATER HILLSBORO AREA CHAMBER OF COMMERCE
12	BETHEL CHURCH OF GOD	84	HALFWAY HOUSE SERVICES, INC.
13	BIRCH COMMUNITY SERVICES, INC.	85	HEARING AND SPEECH INSTITUTE INC
14	BLACHLY LANE ELECTRIC COOPERATIVE	86	HELP NOW! ADVOCACY CENTER
15	BLIND ENTERPRISES OF OREGON	87	HIGHLAND HAVEN
16	BONNEVILLE ENVIRONMENTAL FOUNDATION	88	HIGHLAND UNITED CHURCH OF CHRIST
17	BOYS AND GIRLS CLUBS OF PORTLAND METROPOLITAN AREA	89	HIV ALLIANCE, INC
18	BROAD BASE PROGRAMS INC.	90	HOUSING AUTHORITY OF LINCOLN COUNTY
19	CANBY FOURSQUARE CHURCH	91	HOUSING AUTHORITY OF PORTLAND
20	CANCER CARE RESOURCES	92	HOUSING NORTHWEST
21	CASCADIA BEHAVIORAL HEALTHCARE	93	INDEPENDENT INSURANCE AGENTS AND BROKERS OF OREGON
22	CASCADIA REGION GREEN BUILDING COUNCIL	94	INTERNATIONAL SOCIETY FOR TECHNOLOGY IN EDUCATION

95	INTERNATIONAL SUSTAINABLE DEVELOPMENT FOUNDATION	167	PREGNANCY RESOUCCE CENTERS OF GRETER PORTLAND
96	IRCO	168	PRINGLE CREEK SUSTAINABLE LIVING CENTER
97	JASPER MOUNTAIN	169	PUBLIC DEFENDER SERVICES OF LANE COUNTY, INC.
98	JUNIOR ACHIEVEMENT	170	QUADRIPLEGICS UNITED AGAINST DEPENDENCY, INC.
99	KLAMATH HOUSING AUTHORITY	171	REBUILDING TOGETHER - PORTLAND INC.
100	LA CLINICA DEL CARINO FAMILY HEALTH CARE CENTER	172	REGIONAL ARTS AND CULTURE COUNCIL
101	LA GRANDE UNITED METHODIST CHURCH	173	RELEVANT LIFE CHURCH
102	LANE ELECTRIC COOPERATIVE	174	RENEWABLE NORTHWEST PROJECT
103	LANE MEMORIAL BLOOD BANK	175	ROGUE FEDERAL CREDIT UNION
104	LANECO FEDERAL CREDIT UNION	176	ROSE VILLA, INC.
105	LAUREL HILL CENTER	177	SACRED HEART CATHOLIC DAUGHTERS
106	LIFEWORKS NW	178	SAIF CORPORATION
107	LIVING WAY FELLOWSHIP	179	SAINT ANDREW NATIVITY SCHOOL
108	LOAVES & FISHES CENTERS, INC.	180	SAINT CATHERINE OF SIENA CHURCH
109	LOCAL GOVERNMENT PERSONNEL INSTITUTE	181	SAINT JAMES CATHOLIC CHURCH
110	LOOKING GLASS YOUTH AND FAMILY SERVICES	182	SALEM ALLIANCE CHURCH
111	MACDONALD CENTER	183	SALEM ELECTRIC
112	MAKING MEMORIES BREAST CANCER FOUNDATION, INC.	184	SALMON-SAFE INC.
113	METRO HOME SAFETY REPAIR PROGRAM	185	SCIENCEWORKS
114	METROPOLITAN FAMILY SERVICE	186	SE WORKS
115	MID COLUMBIA COUNCIL OF GOVERNMENTS	187	SECURITY FIRST CHILD DEVELOPMENT CENTER
116	MID-COLUMBIA CENTER FOR LIVING	188	SELF ENHANCEMENT INC.
117	MID-WILLAMETTE VALLEY COMMUNITY ACTION AGENCY, INC	189	SERENITY LANE
118	MORNING STAR MISSIONARY BAPTIST CHURCH	190	SEXUAL ASSAULT RESOURCE CENTER
119	MORRISON CHILD AND FAMILY SERVICES	191	SEXUAL ASSAULT RESOURCE CENTER
120	MOSAIC CHURCH	192	SHELTERCARE
121	NATIONAL PSORIASIS FOUNDATION	193	SHERIDAN JAPANESE SCHOOL FOUNDATION
122	NATIONAL WILD TURKEY FEDERATION	194	SHERMAN DEVELOPMENT LEAGUE, INC.
123	NEW AVENUES FOR YOUTH INC	195	SILVERTON AREA COMMUNITY AID
124	NEW BEGINNINGS CHRISTIAN CENTER	196	SISKIYOU INITIATIVE
125	NEW HOPE COMMUNITY CHURCH	197	SMART
126	NEWBERG FRIENDS CHURCH	198	SOCIAL VENTURE PARTNERS PORTLAND
127	NORTH BEND CITY- COOS/URRY HOUSING AUTHORITY	199	SOUTH COAST HOSPICE, INC.
128	NORTHWEST FOOD PROCESSORS ASSOCIATION	200	SOUTH LANE FAMILY NURSERY DBA FAMILY RELIEF NURSE
129	NORTHWEST LINE JOINT APPRENTICESHIP & TRAINING COMMITTEE	201	SOUTHERN OREGON CHILD AND FAMILY COUNCIL, INC.
130	NORTHWEST REGIONAL EDUCATIONAL LABORATORY	202	SOUTHERN OREGON HUMANE SOCIETY
131	NORTHWEST YOUTH CORPS	203	SPARC ENTERPRISES
132	OCHIN	204	SPIRIT WIRELESS
133	OHSU FOUNDATION	205	SPONSORS, INC.
134	OLIVET BAPTIST CHURCH	206	SPOTLIGHT THEATRE OF PLEASANT HILL
135	OMNIMEDIX INSTITUTE	207	SPRINGFIELD UTILITY BOARD
136	OPEN MEADOW ALTERNATIVE SCHOOLS, INC.	208	ST VINCENT DE PAUL
137	OREGON BALLET THEATRE	209	ST. ANTHONY CHURCH
138	OREGON CITY CHURCH OF THE NAZARENE	210	ST. ANTHONY SCHOOL
139	OREGON COAST COMMUNITY ACTION	211	ST. MARYS OF MEDFORD, INC.
140	OREGON DEATH WITH DIGNITY	212	ST. VINCENT DEPAUL OF LANE COUNTY
141	OREGON DONOR PROGRAM	213	STAND FOR CHILDREN
142	OREGON EDUCATION ASSOCIATION	214	STAR OF HOPE ACTIVITY CENTER INC.
143	OREGON ENVIRONMENTAL COUNCIL	215	SUMMIT VIEW COVENANT CHURCH
144	OREGON MUSUEM OF SCIENCE AND INDUSTRY	216	SUNNYSIDE FOURSQUARE CHURCH
145	OREGON PROGRESS FORUM	217	SUNRISE ENTERPRISES
146	OREGON REPERTORY SINGERS	218	SUSTAINABLE NORTHWEST
147	OREGON STATE UNIVERSITY ALUMNI ASSOCIATION	219	TENAS ILLAHEE CHILDCARE CENTER
148	OREGON SUPPORTED LIVING PROGRAM	220	THE EARLY EDUCATION PROGRAM, INC.
149	OSLC COMMUNITY PROGRAMS	221	THE NATIONAL ASSOCIATION OF CREDIT MANAGEMENT-OREGON, INC.
150	OUTSIDE IN	222	THE NEXT DOOR
151	OUTSIDE IN	223	THE OREGON COMMUNITY FOUNDATION
152	PACIFIC CASCADE FEDERAL CREDIT UNION	224	THE SALVATION ARMY - CASCADE DIVISION
153	PACIFIC FISHERY MANAGEMENT COUNCIL	225	TILLAMOOK CNTY WOMENS CRISIS CENTER
154	PACIFIC INSTITUTES FOR RESEARCH	226	TILLAMOOK ESTUARIES PARTNERSHIP
155	PACIFIC STATES MARINE FISHERIES COMMISSION	227	TOUCHSTONE PARENT ORGANIZATION
156	PARALYZED VETERANS OF AMERICA	228	TRAILS CLUB
157	PARTNERSHIPS IN COMMUNITY LIVING, INC.	229	TRAINING EMPLOYMENT CONSORTIUM
158	PENDLETON ACADEMIES	230	TRI-COUNTY HEALTH CARE SAFETY NET ENTERPRISE
159	PENTAGON FEDERAL CREDIT UNION	231	TRILLIUM FAMILY SERVICES, INC.
160	PLANNED PARENTHOOD OF SOUTHWESTERN OREGON	232	UMPQUA COMMUNITY DEVELOPMENT CORPORATION
161	PORT CITY DEVELOPMENT CENTER	233	UNION GOSPEL MISSION
162	PORTLAND ART MUSEUM	234	UNITED CEREBRAL PALSY OF OR AND SW WA
163	PORTLAND BUSINESS ALLIANCE	235	UNITED WAY OF THE COLUMBIA WILLAMETTE
164	PORTLAND HABILITATION CENTER, INC.	236	US CONFERENCE OF MENONNITE BRETHREN CHURCHES
165	PORTLAND SCHOOLS FOUNDATION	237	US FISH AND WILDLIFE SERVICE
166	PORTLAND WOMENS CRISIS LINE		

238	USAGENCIES CREDIT UNION	13	GLADSTONE POLICE DEPARTMENT
239	VERMONT HILLS FAMILY LIFE CENTER	14	GLENDALE RURAL FIRE DISTRICT
240	VIRGINIA GARCIA MEMORIAL HEALTH CENTER	15	HOODLAND FIRE DISTRICT NO.74
241	VOLUNTEERS OF AMERICA OREGON	16	HOODLAND FIRE DISTRICT #74
242	WE CARE OREGON	17	HOUSING AUTHORITY AND COMMUNITY SERVICES AGENCY
243	WESTERN RIVERS CONSERVANCY	18	KLAMATH COUNTY 9-1-1
244	WESTERN STATES CENTER	19	LANE EDUCATION SERVICE DISTRICT
245	WESTSIDE BAPTIST CHURCH	20	LANE TRANSIT DISTRICT
246	WILD SALMON CENTER	21	MALIN COMMUNITY PARK AND RECREATION DISTRICT
247	WILLAMETTE FAMILY	22	MARION COUNTY FIRE DISTRICT #1
248	WILLAMETTE VIEW INC.	23	METRO
249	WOODBURN AREA CHAMBER OF COMMERCE	24	METROPOLITAN EXPOSITION-RECREATION COMMISSION
250	WORD OF LIFE COMMUNITY CHURCH	25	MONMOUTH - INDEPENDENCE NETWORK
251	WORKSYSTEMS INC	26	MULTONAH COUNTY DRAINAGE DISTRICT #1
252	YOUTH GUIDANCE ASSOC.	27	NEAH KAH NIE WATER DISTRICT
253	YWCA SALEM	28	NW POWER POOL
1	ALOHOLIC REHABILITATION SVS OF HI INC DBA HINA MAUKA	29	OAK LODGE WATER DISTRICT
2	ALOHACARE	30	OR INT'L PORT OF COOS BAY
3	AMERICAN LUNG ASSOCIATION	31	PORT OF ST HELENS
4	BISHOP MUSEUM	32	PORT OF UMPQUA
5	BUILDING INDUSTRY ASSOCIATION OF HAWAII	33	REGIONAL AUTOMATED INFORMATION NETWORK
6	CTR FOR CULTURAL AND TECH INTERCHNG BETW EAST AND WEST	34	RIVERGROVE WATER DISTRICT
7	EAH, INC.	35	SALEM AREA MASS TRANSIT DISTRICT
8	EASTER SEALS HAWAII	36	SANDY FIRE DISTRICT NO. 72
9	GOODWILL INDUSTRIES OF HAWAII, INC.	37	SUNSET EMPIRE PARK AND RECREATION
10	HABITAT FOR HUMANITY MAUI	38	THE NEWPORT PARK AND RECREATION CENTER
11	HALE MAHAOLU	39	THE PORT OF PORTLAND
12	HAROLD K.L. CASTLE FOUNDATION	40	TILLAMOOK PEOPLES UTILITY DISTRICT
13	HAWAII AGRICULTURE RESEARCH CENTER	41	TUALATIN HILLS PARK AND RECREATION DISTRICT
14	HAWAII EMPLOYERS COUNCIL	42	TUALATIN VALLEY FIRE & RESCUE
15	HAWAII FAMILY LAW CLINIC DBA ALA KUOLA	43	TUALATIN VALLEY WATER DISTRICT
16	HONOLULU HABITAT FOR HUMANITY	44	UNION SOIL & WATER CONSERVATION DISTRICT
17	IUPAT, DISTRICT COUNCIL 50	45	WEST MULTNOMAH SOIL AND WATER CONSERVATION DISTRICT
18	LANAKILA REHABILITATION CENTER INC.	46	WEST VALLEY HOUSING AUTHORITY
19	LEEWARD HABITAT FOR HUMANITY	47	WILLAMALANE PARK AND RECREATION DISTRICT
20	MAUI COUNTY FCU	48	YOUNGS RIVER LEWIS AND CLARK WATER DISTRICT
21	MAUI ECONOMIC DEVELOPMENT BOARD		
22	MAUI ECONOMIC OPPORTUNITY, INC.	No.	State Agencies
23	MAUI FAMILY YMCA	1	BOARD OF MEDICAL EXAMINERS
24	NA HALE O MAUI	2	OFFICE OF MEDICAL ASSISTANCE PROGRAMS
25	NA LEI ALOHA FOUNDATION	3	OFFICE OF THE STATE TREASURER
26	NETWORK ENTERPRISES, INC.	4	OREGON BOARD OF ARCHITECTS
27	ORI ANUENUE HALE, INC.	5	OREGON CHILD DEVELOPMENT COALITION
28	PARTNERS IN DEVELOPMENT FOUNDATION	6	OREGON DEPARTMENT OF EDUCATION
29	POLYNESIAN CULTURAL CENTER	7	OREGON DEPARTMENT OF FORESTRY
30	PUNAHOU SCHOOL	8	OREGON DEPT OF TRANSPORTATION
31	ST. THERESA CHURCH	9	OREGON DEPT. OF EDUCATION
32	WAIANAEE COMMUNITY OUTREACH	10	OREGON LOTTERY
33	WAILUKU FEDERAL CREDIT UNION	11	OREGON OFFICE OF ENERGY
34	YMCA OF HONOLULU	12	OREGON STATE BOARD OF NURSING
		13	OREGON STATE POLICE
No.	Special/Independent Districts	14	OREGON TOURISM COMMISSION
1	BAY AREA HOSPITAL DISTRICT	15	OREGON TRAVEL INFORMATION COUNCIL
2	CENTRAL OREGON INTERGOVERNMENTAL COUNCIL	16	SANTIAM CANYON COMMUNICATION CENTER
3	CENTRAL OREGON IRRIGATION DISTRICT	17	SEIU LOCAL 503, OPEU
4	CHEHALEM PARK AND RECREATION DISTRICT	1	ADMIN. SERVICES OFFICE
5	CITY COUNTY INSURANCE SERVICES	2	HAWAII CHILD SUPPORT ENFORCEMENT AGENCY
6	CLEAN WATER SERVICES	3	HAWAII HEALTH SYSTEMS CORPORATION
7	COLUMBIA 911 COMMUNICATIONS DISTRICT	4	SOH- JUDICIARY CONTRACTS AND PURCH
8	COLUMBIA RIVER PUD	5	STATE DEPARTMENT OF DEFENSE
9	DESCHUTES COUNTY RFPD NO.2	6	STATE OF HAWAII
10	DESCHUTES PUBLIC LIBRARY SYSTEM	7	STATE OF HAWAII
11	EAST MULTNOMAH SOIL AND WATER CONSERVANCY	8	STATE OF HAWAII, DEPT. OF EDUCATION
12	GASTON RURAL FIRE DEPARTMENT		

Passport in the News

Forbes

June 22, 2015
Larry Myler

Clean Technology is Good Business

Would you like to expand your bottom line by shrinking the carbon footprint off every customer you serve? Many companies are successfully doing just that by developing new technologies that help customers become more sustainable in their operations. This is good business, and it's big business because most large organizations have a directive to decrease consumption and become more sustainable. Cox Enterprises, a conglomerate with 50,000 employees, has the goal of achieving carbon neutrality on an accelerated timeline. Robert Fairey, Senior Director Energy Procurement and Waste Diversion at Cox, has targeted three major pillars for management and reduction: Water, waste and energy. A large problem Fairey wrestled with was the number of utility companies that supply Cox with water, waste management and energy. "We have over 40,000 utility accounts across our divisions," laments Fairey. "That has been difficult to keep up with, to say the least."

Enter Urjanet, a clean-tech company that consolidates all of those individual bills from numerous accounts into a single data set that can be managed in one dashboard by customers like Cox Enterprises. "Now we can analyze costs and benefits, make better decisions, understand our consumption patterns, and better manage water, waste and energy usage," reports Fairey.

Urjanet CEO, Sanjoy Malik, describes the problem his company solves. "Many large organizations are still dealing with separate paper bills to make energy purchase decisions. Some of our clients were trying to manage as much as \$1B in electricity purchases alone."

Another example of a carbon challenge and its tech solution involves municipalities that need to better manage transportation within their borders. Most cities struggle with how to efficiently move, park, manage and collect revenue from transporting people and cargo. If handled well, environmental impacts and costs related to transportation can be reduced, even while revenues increase.

Salt Lake City, as an example, recently adopted a new system named Park SLC, powered by tech company, Passport. According to Robin Hutcheson, Salt Lake City Transportation Division Director, "Passport allowed us to configure our platform to meet our city's unique challenges and goals." With every city having different needs and goals, a key to this solution has been flexibility. Passport Founder and Co-CEO Bob Youakim observes, "We had to create a system that could be adapted to the requirements of cities like Chicago, Omaha, Boston, Toronto and Victoria."

The need for carbon footprint reduction is in full swing inside large organizations. How can your company take advantage of this megatrend by developing flexible technology that simplifies this task?

FierceWireless

October 7, 2016
Colin Gibbs

Editor's note: Welcome to the 2016 Fierce 15, an annual list that recognizes 15 of the most interesting startups in the wireless industry. We'll publish one profile a day for 15 days; Passport is the fifth company to be recognized this year.

Company: Passport
Where it's based: Charlotte, North Carolina
When it was founded: 2010
Website: passportinc.com

Why it's Fierce: In just under six years, Passport has expanded from a self-funded startup trying to solve parking issues to the largest mobile parking and transit payment platform in the world. It runs through private labels from city to city, so even if you haven't heard the name, you may have used the engine.

"We're the biggest name you've never heard of," said Passport CEO Bob Youakim with a chuckle during an interview with FierceWireless. "You can't go in one of these cities and not be up against us, whether it's transit, parking or some other payment mechanism you're engaging with."

Youakim started Passport after recognizing that current parking systems were frustrating the consumer and causing the parking operator, be it a garage, city or other entity, to lose revenue. His timing proved effective, as three trends arose around that time that enabled the kind of mobile-based platform Passport became:

- Cloud-based infrastructure
- The rise and ubiquity of mobile devices
- People's increased comfort level making payments using mobile-based platforms

"When you add those all together and you attack a market that is tired, sleepy, more dinosaur-esque and ripe for destruction, and you can bring a solution that's easily adoptable and scalable to their operations, it's a home run," Youakim said.

Fierce 15 2016: Passport shifts into high gear on mobile parking and transport payments

Passport enters markets through partnerships with clients including governments, agencies, universities and private operators. The company provides the underlying engine, but specifics of each implementation are adaptable to a client's preferences. As such, Passport has three possible funding models, between which the client can choose:

- Convenience fee on the end user
- Percentage of client's revenue
- Flat monthly fee for the client

About a year and a half ago, Passport also brought its platform to transit payments. While that was never the original intention of the company, the platform was adaptable enough to fit the industry.

"This doesn't happen very often: We had an acute focus on solving the parking issue, and then when we looked at a very analogous market in transit, we realized, 'wait a second, this is the exact same thing,'" Youakim said.

"You're going to a ticket vending machine, you have to pay for a ticket ... we realized we need to apply this technology to a completely different vertical."

Youakim launched Passport with \$500,000 of his own funds along with matching \$500,000 from his family. The company went through funding rounds and is now privately owned by three companies: Grotech Ventures, MK Capital and relevance capital.

Passport is currently expanding from 60-70 employees and has over 250 total clients. It is also launching internationally, with an upcoming U.K. launch in November and plans to enter the Australian market down the road.

What's next: Commuting and transit is one of the fastest changing industries, both because demand is increasing for public transportation and because the rise of self-driving cars threatens to disrupt the current model entirely. But Passport believes its mobile payment platform is adaptable enough that it can theoretically rise to meet the needs of the market that emerges – including with autonomous vehicles.

"We're focused on seeing how our solution can remain relevant as it relates to the broader base," Youakim said. "And there's no more exciting time than today."



Parking downtown? There's gonna be an app for that!

September 2, 2016
Miles Jay Oliver

Imagine sitting in a meeting in downtown Shreveport that you can't leave.

The meeting was supposed to last about an hour and a half, and you've paid for the two-hour maximum at your parking meter two blocks away.

Now, though, it doesn't seem likely that you're going to be out of there any time soon. All you can think about is whether you're about to get a parking ticket.

If only there were a way to pay for an extension without running down to pump another handful of silver into the meter.

Well, that's just what Shreveport's Downtown Development Authority is working to do for everyone who uses the parking meters in downtown Shreveport.

The Passport parking app is in its last stages of preparation for Shreveport and should be ready for users within the next 30 to 45 days.

"The app is ready — we are having to do some prep in order to apply it to our particular downtown," said parking administrator Lorenzo Lee, who has been with ShrevePark Parking Services — a division of DDA — since January 2014.

Lee is excited to be introducing Shreveport to the next wave in savvy technology for anyone parking downtown.

Although several potential software programs were reviewed, the DDA's executive director Liz Swaine said Passport was by far the best.

"They just seemed to have it all together," Swaine said, noting that Passport satisfied the DDA's hope to find an app that would be easy to use.

Motorists will be able to use the app by programming their license plates and making payments directly from their phones. With new signage indicating parking zones downtown, app users will be able to pay for the time and space to the specific zone in which their vehicle is parked.

Enforcement will keep track of who has paid through the app for parking, and users will be given an option to extend their parking time by paying for additional time without dashing out to pay curbside. Everything can be done through an app downloaded to your phone.

Preloaded accounts will have the fee of 10 cents per transaction, while users without the preload will pay 35 cents per transaction.

All revenue generated through parking fees will continue going to the city of Shreveport.

Once the app is up and running, there will be an initial trial period of 90 days downtown. During the trial period, the city and the DDA will determine whether to go into a long-term commitment with Passport.

"ShrevePark will be cutting parkers a lot of slack for several weeks," said Swaine, who realizes people will have to learn how to use the app.

The app has shown success in other communities, including Boston, Chicago, Sacramento and Detroit. Locally, at least one parking company already is using Passport as a method of payment for their surface lots.

Accounting for those not comfortable with using cell phones or paying via phone apps, the DDA provided assurance that the old means of paying for parking is not disappearing any time soon.

Training Materials

Passport

New Client Launch Training Guide - Mobile Pay

Client:

Client Success Manager:

Launch Date:

Welcome to Mobile Pay!

Thank you so much for letting us serve your parking community! We are excited for your Mobile Pay app to launch soon. Our client success team consists of customer support specialists who assist with parker inquiries and our technical help desk who assist with client inquiries on technical issues with our platform.

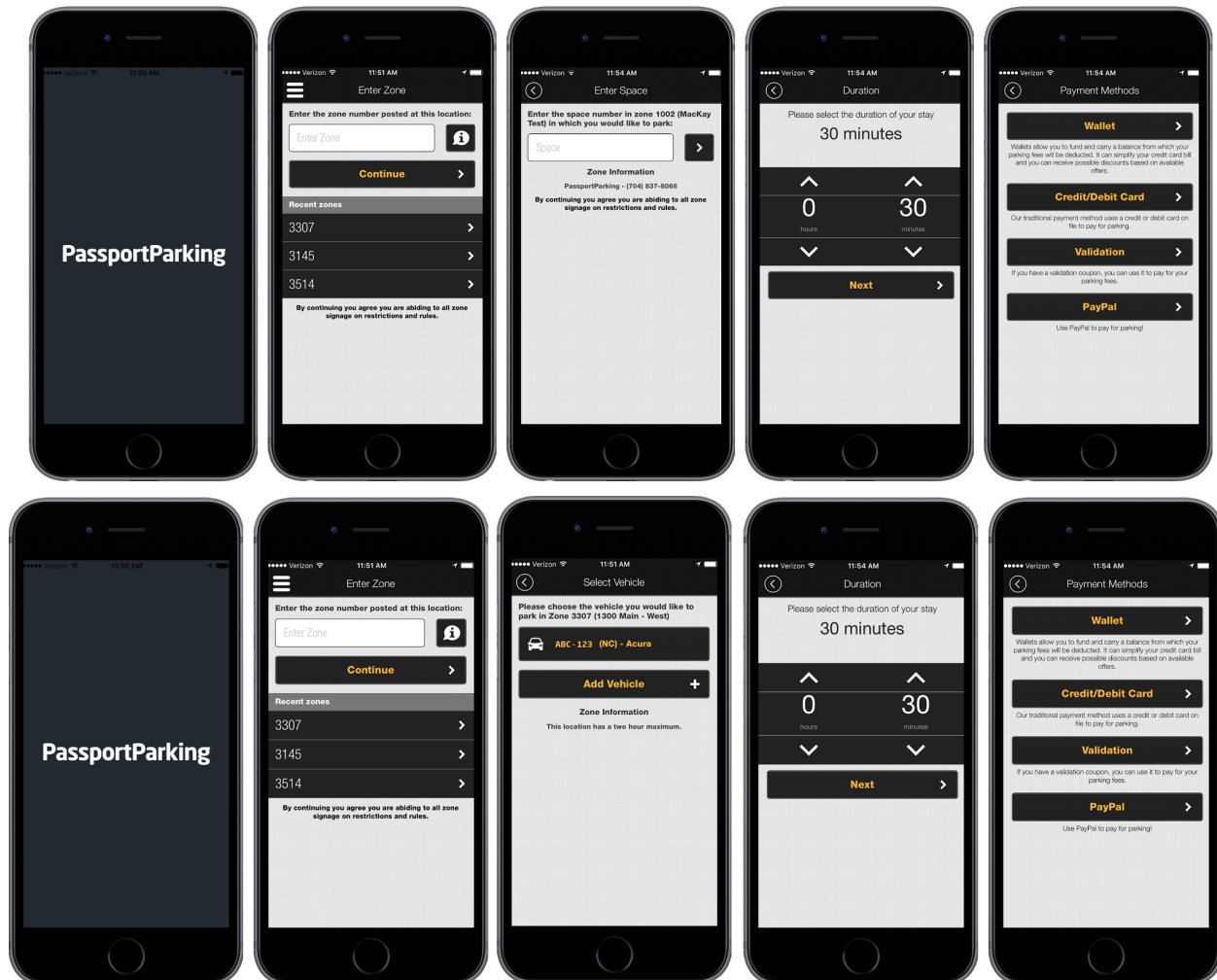
As your Client Success Manager, I will serve as your main point of contact going forward for all account related questions. To ensure a successful launch, this training will cover your front-facing user mobile application and the back-end system we call OpsMan. We have a lot to cover, so let's get started!

Mobile Application Review

Training Date:

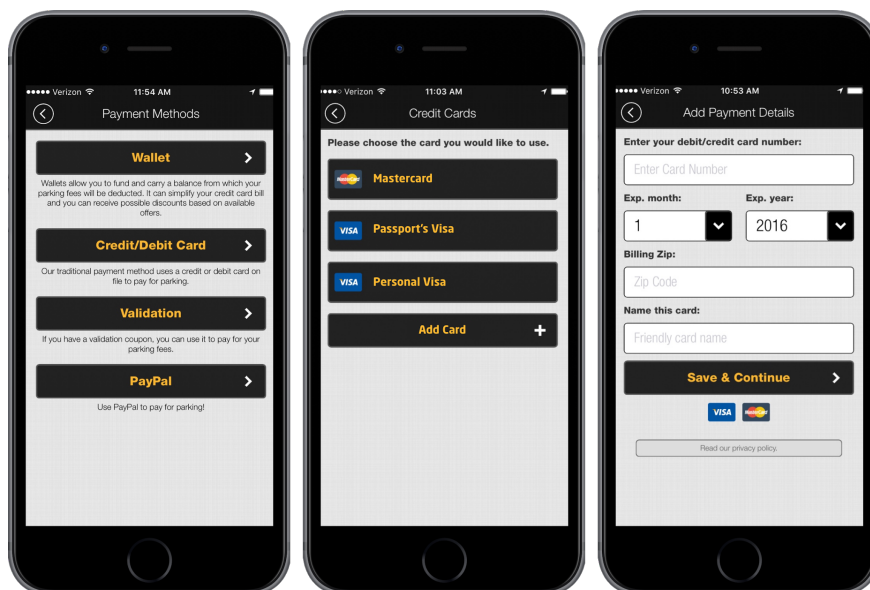
- 1. Downloading the mobile app to your phone or tablet:** visit the App store on Apple devices and Google Play on Android devices and search 'Passport Inc' to find your app (generic or white labeled). Follow the instructions for installation.
- 2. Creating a new user account:** Click 'sign up' to start a new user account. Accept Terms & Conditions.
 - Login Selection* - A new parker can choose to sign-up with their phone, email or facebook account. We recommend referring customers to sign up with email so that you can also send them promotional e-mails or announcements. The user will receive a verification code to identify them in the the system. They will also set a security pin for future logins.
- 3. Starting a new session:** The parker can now pay for their parking session. Parkers can pay for multiple parking sessions simultaneously by starting each new session in the menu.
 - Enter zone* - The parker can enter the zone number located on the signs provided near the space. Zones in which a parker has recently parked will also show at the bottom of the screen.

- ❑ *Enter space or License Plate (LPN)*- The parker will enter the space number listed in the stall (for space-based) or LPN for (plate-based). This will also show the parker the rate.
- ❑ *Length of stay* - The parker can select from the maximum allowed time for the space or they can select time in increments (if the zone allows).

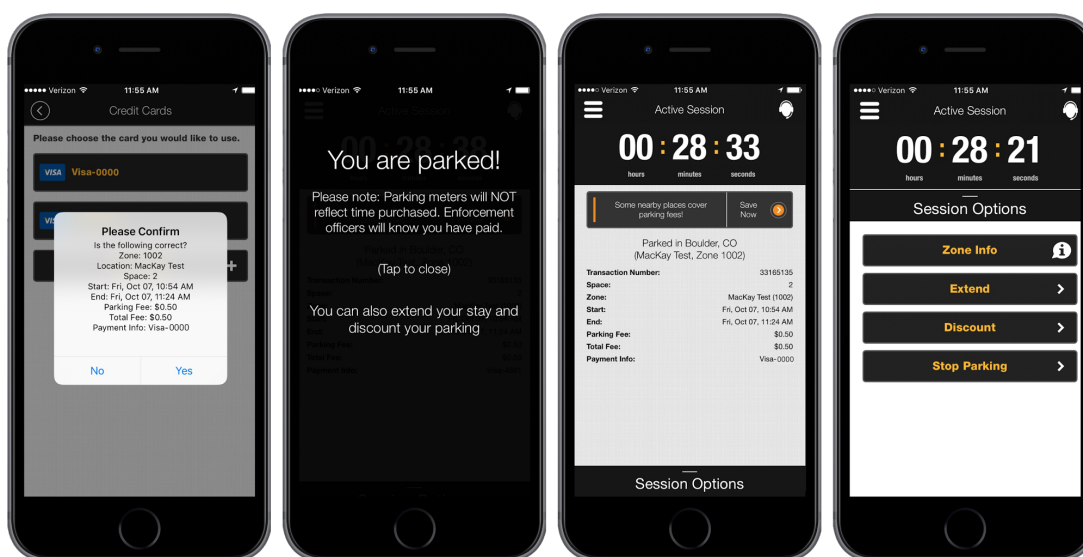


4. Payment: The parker can choose to pay via the following options:

- ❑ *Wallet (for clients with Wallet option)* - allows the parker to carry a balance from which parking fees will be deducted. Parkers will have simplified credit card billing and can also receive possible discounts and offers set by the client.
- ❑ *Credit/Debit Card* - The parker can add several credit or debit cards. Once a card is entered the first time, the card will be saved for future sessions.
- ❑ *Validation* - The parker may enter coupon codes offered by the client or local businesses.
- ❑ *PayPal* - The parker can link their PayPal account.



5. **Reviewing an Active Session:** Upon confirmation, the parker's session will begin. The parker has several options while in an active session.
- ❑ *Zone Info* - Provides rate and location information.
 - ❑ *Extending Time* - Allows the parker to extend time without returning to the space
 - ❑ *Stop Parking* - Allows the parker to end their parking session and free up the space for another parker.
 - ❑ *Expiration alert* - The parker will receive an alert when their parking session is near expiration and can have the option extend.

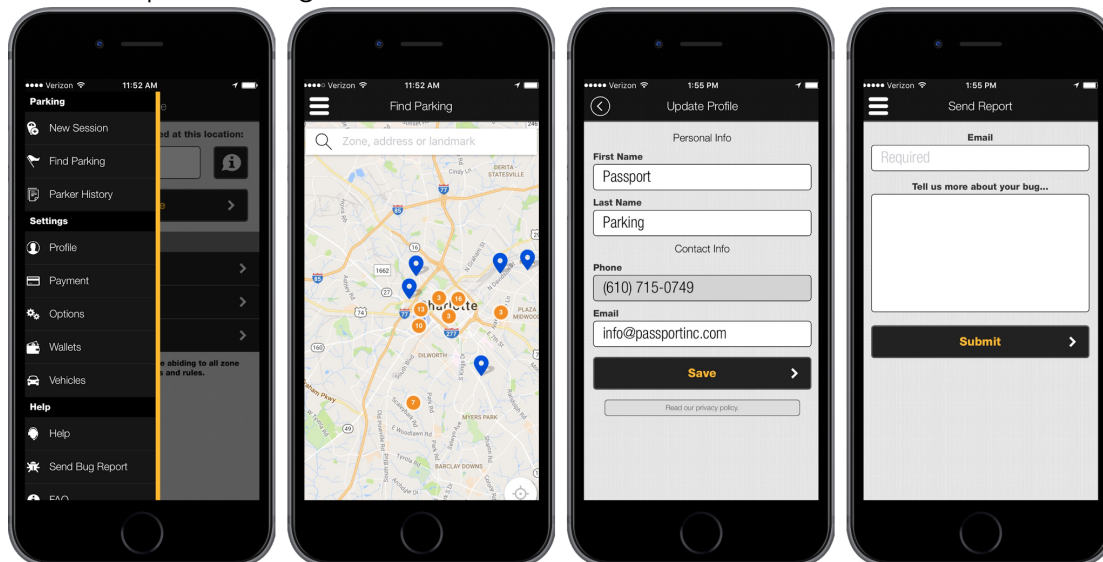


Please note:

- ❑ *The time on the clock may be less than the time purchased.* Parking time sessions start upon the initiation of the transaction when they view the rate. The maximum time allowed may be less than the the set time if a parker starts a session close to the ending time of the zone.
- ❑ *On street meter may not match.* Parkers should also note that the parking meters may not reflect the purchased time and instead, will be reflected via mobile phone to enforcement officers.
- ❑ *Transactions will not show until they are settled.* Credit card charges won't show and a receipt will not be emailed until the parking session is over.

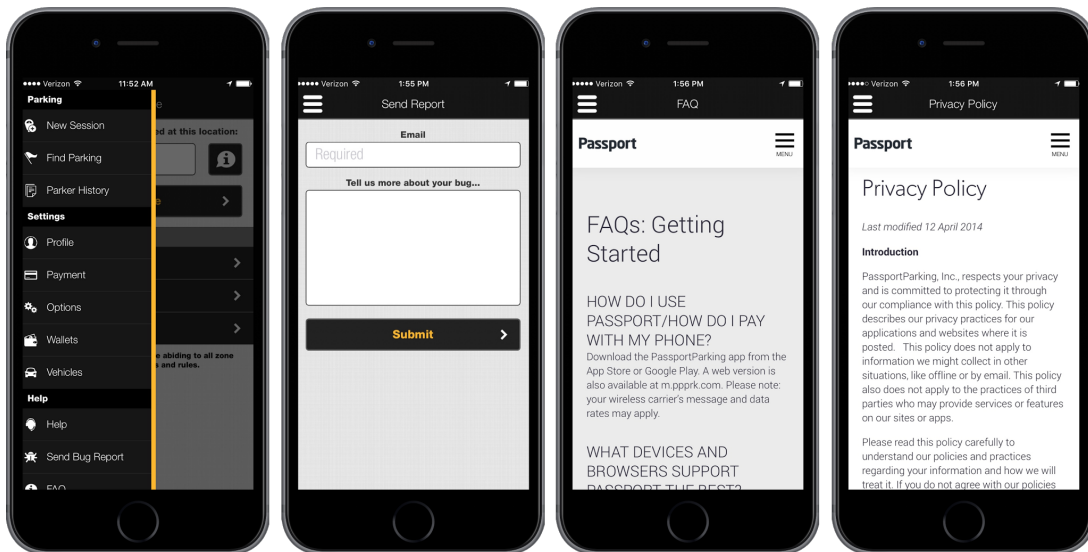
6. Parker Options and Settings: Here are some additional features a parker may be interested in:

- ❑ *Find Parking (for applicable clients)* - A parker can use this option to find parking near a zone, address or landmark.
- ❑ *Parker History* - A parker can review all of their past transactions. They can also email their receipts from here and also dispute tickets via a form emailed to the operator.
- ❑ *Profile* - The parker's passport ID and contact information.
- ❑ *Payment* - The parker can add and delete new credit cards.
- ❑ *Options* - The parker can select receiving reminders, reminder sound and emailed receipts
- ❑ *Wallets (for clients with wallet option)* - The parker can manage the funds in their wallet.
- ❑ *Vehicles* - The parker can save their vehicle information, particularly useful for 'Pay by LPN'.
- ❑ *Logout* - The parker can log out of the app and will need to enter their pin upon next login.



7. Help: Here are some of our resources for parkers to receive help:

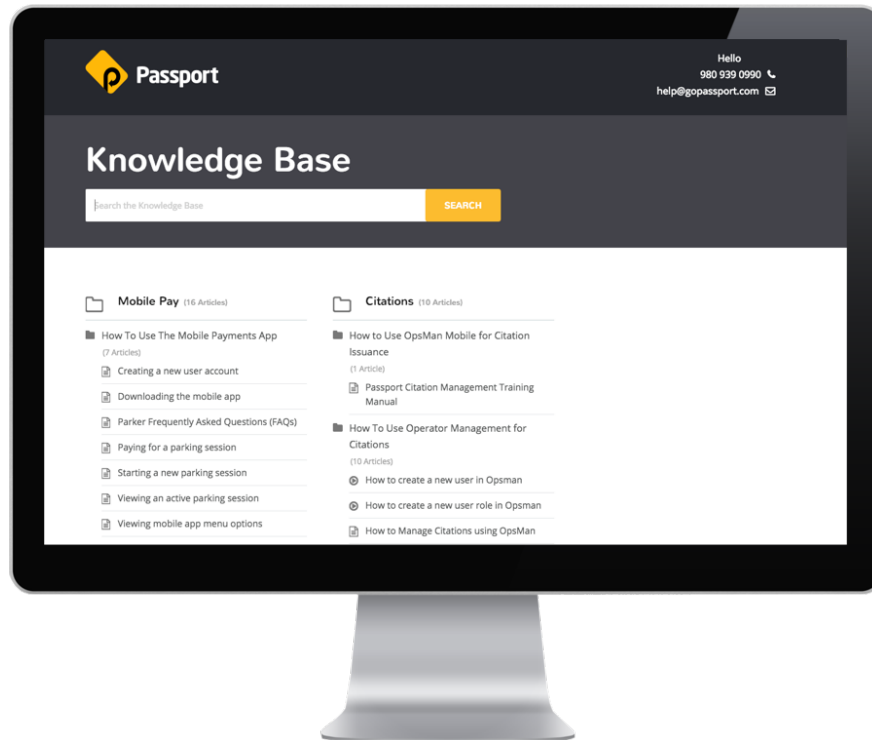
- ❑ *Send Bug Report* - This form will allow parkers to submit bugs and descriptions directly to our development team. This is important for clients and end users to show us exactly the root cause of issues you may see in the appl.
- ❑ *FAQ* - Our on screen help provides answers to the most common questions, that we've also answered in this training. These can also be found our company website: <https://passportinc.com/consumers/>
- ❑ *Help Desk* - Parkers will be able to call our help desk via a button in the app.
- ❑ *Terms & Conditions and Privacy Policy*: full text of these policies are available for review.



Operations Management Web Platform (OpsMan)

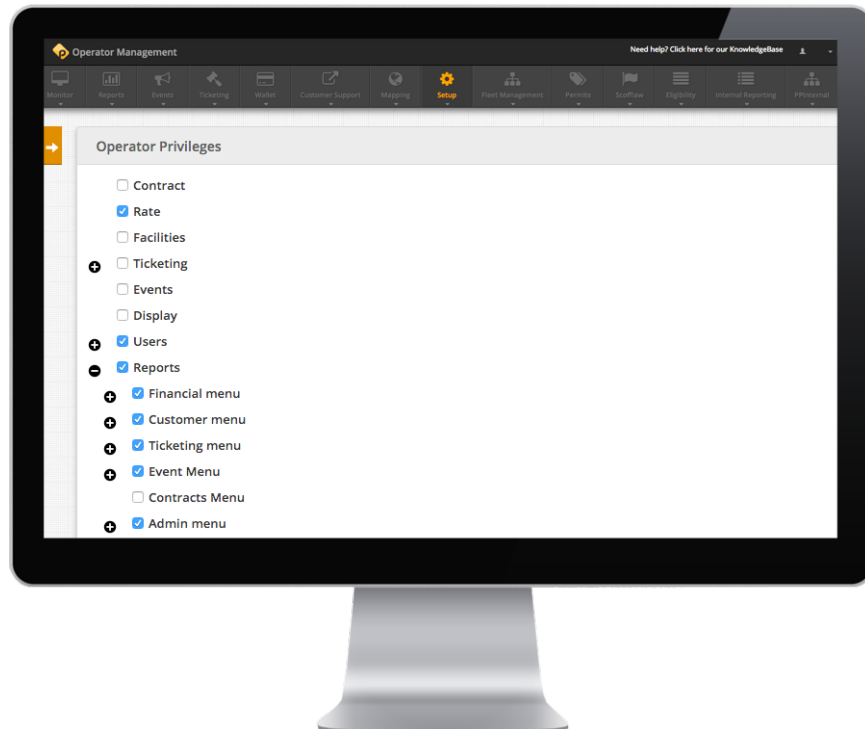
Training Date:

1. **Introduction:** Our Operations Management web platform is your backend portal for all administrative, support and reporting tasks. All data in the system is synced in real time with the mobile application. You can enter with the username (email) and temp password provided by your CSM.
 - ❑ The OpsMan Web Address is <https://ppprk.com/park/>. We suggest you favorite in your browser.
 - ❑ Along the top are the various functions you have access to as an administrator. We will review each of these in detail.
 - ❑ You also have access to our [KnowledgeBase](#) where we will have content to guide you through common tasks in this system.

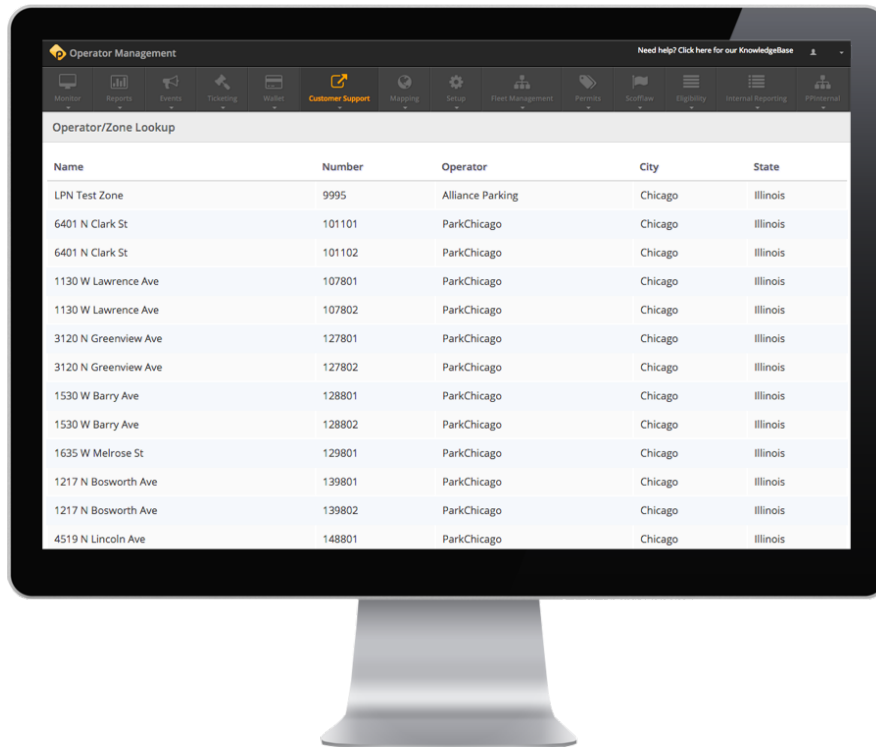


2. **Setup:** *(for trainer only, not visible to client)* this tab provides details of the organization's specific setup such as zones, space rates, restrictions, notifications, etc. This is where you can see the parameters of your specific buildout.
3. **Users:** In this tab, you will setup the users in your team who will have access to this system, as well as what they are allowed to see by assigning user roles.
 - ❑ [User Roles](#) - This allows the organization to assign only the areas each user needs access to. You can also assign multiple roles to each user.
 - ❑ *To create a new user role* - To create a new role, you'll type in the role name. You'll then elect the privileges that role should have (i.e. reporting, OpsMan Mobile, ticketing) and save. The new role will be in the drop down menu under users.
 - ❑ *Role Management* - Some common roles for clients we may suggest include:
 - ❑ Administrator (owner of the system within your organization and full access)
 - ❑ Finance (users interested in financial reporting including revenue, transaction details)
 - ❑ Support (users that may receive inquiries from parkers)
 - ❑ Tech
 - ❑ [Users](#) - This is the list of everyone who has access to your system. To create a new user, click the button 'create new user' and fill in their email address, name, nickname (such as initials) and set their permissions and set a temporary password. You can then save this as a new user.

- ❑ *Assignable Privileges (for trainer only)* - These are brief descriptions of what privileges can be given to users.
 - ❑ *Users* - allows a user to manage other [users](#) and [roles](#)
 - ❑ *Reports* - allows a user to access financial and customer reports.
 - ❑ *Monitor* - allows a user to review a live feed of parking sessions by zone.
 - ❑ *Zone Cash* - allows a user to create, modify or delete offers and refund wallets
 - ❑ [Customer Support](#) - allows a user to provide support to customers with ability to look up individual customer data
 - ❑ *Setup* - provides details of the organization's specific setup such as restrictions
 - ❑ [Events](#) - allows a user to create specific parking rules for limited time events



4. **Customer Support:** this tab allows a user the ability to look up individual customer data
 - ❑ [Support](#) - allows a user to look up all individual customer data
 - ❑ *Zone Lookup* - allows a user to look up the information for individual zones including maximum parking time restrictions, location and particular notes about the zone (i.e. under construction).
 - ❑ *Push Notifications* - allows a user to send notifications to all users signed up for Mobile Pay or to send to specific users, including a custom title and message.

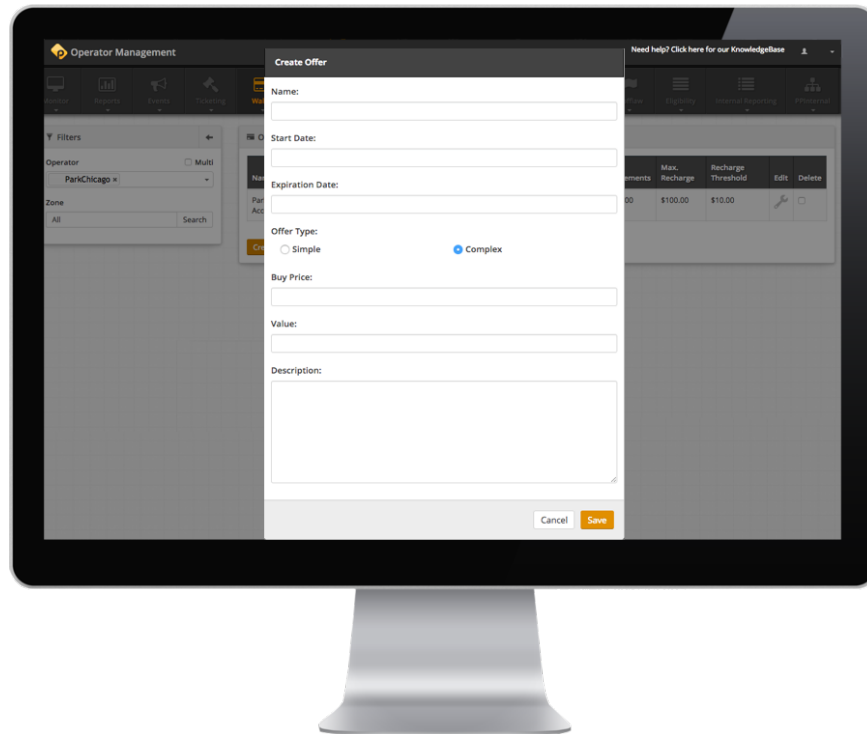


The screenshot shows a computer monitor displaying the 'Operator Management' interface. The top navigation bar includes 'Operator Management' and a help link. Below the navigation bar is a table titled 'Operator/Zone Lookup' with the following data:

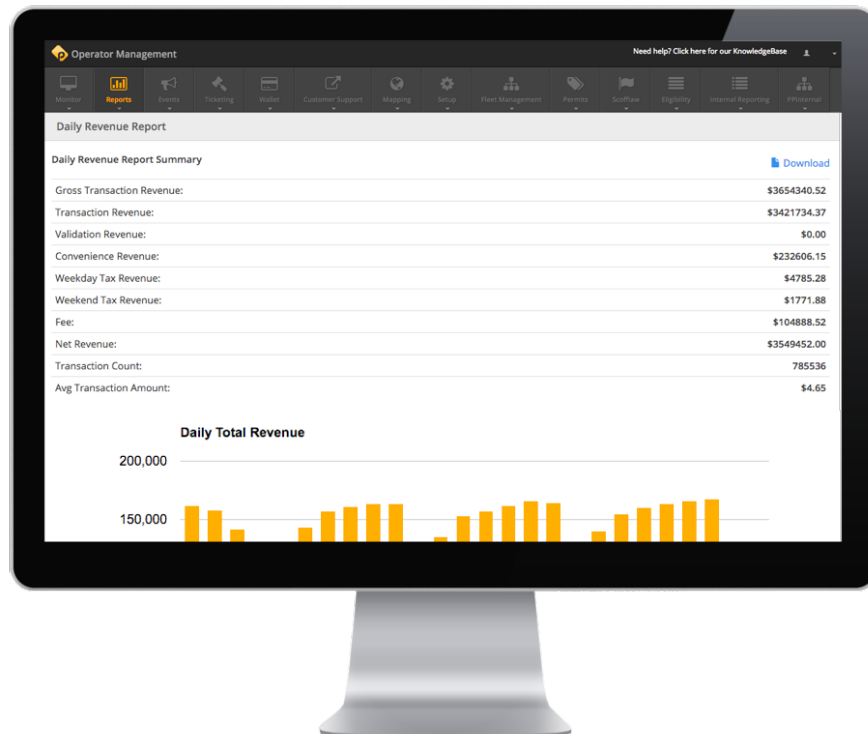
Name	Number	Operator	City	State
LPN Test Zone	9995	Alliance Parking	Chicago	Illinois
6401 N Clark St	101101	ParkChicago	Chicago	Illinois
6401 N Clark St	101102	ParkChicago	Chicago	Illinois
1130 W Lawrence Ave	107801	ParkChicago	Chicago	Illinois
1130 W Lawrence Ave	107802	ParkChicago	Chicago	Illinois
3120 N Greenview Ave	127801	ParkChicago	Chicago	Illinois
3120 N Greenview Ave	127802	ParkChicago	Chicago	Illinois
1530 W Barry Ave	128801	ParkChicago	Chicago	Illinois
1530 W Barry Ave	128802	ParkChicago	Chicago	Illinois
1635 W Melrose St	129801	ParkChicago	Chicago	Illinois
1217 N Bosworth Ave	139801	ParkChicago	Chicago	Illinois
1217 N Bosworth Ave	139802	ParkChicago	Chicago	Illinois
4519 N Lincoln Ave	148801	ParkChicago	Chicago	Illinois

5. **Monitor:** this tab allows a user to review a live feed of parking sessions by zone.
 - Monitor* - in this section, a user in OpsMan can see live parking sessions by zone as indicated by:
 - Yellow (NE) - Coming close to expiring their session
 - Green (AS) - a currently active parking session
 - Blue (PF) - Paid but free
 - Red (UP) - Unpaid but Occupied (including expired sessions)
 - Live Feed* - this option is only available to clients with citation management

6. **Wallet (if applicable):** this tab is where to manage your organization's wallets if they are offered to customers. Here you can create, modify or delete offers.
 - To create a new offer* - Click 'create a new offer.' Enter the information including what you want to name the offer, start date, expiration date, the offer type (simple or complex), the price to buy the offer (what the parker pays), the value of the offer (what the parker buys) and a brief description.
 - For a simple offer, (which is actually more complex!), you will be able to include the recharge data including the threshold, minimum to recharge, increment steps and max recharge.



7. **Events:** this is to create a one-time event with a special rate that will impact the zones specified (i.e. festivals, game days). The user will need to include the event title, event dates and times, the new rate and the rate start time (which may differ from the event start time). You can also allow free parking through the event if parked before the start rate time and permit parking.
8. **Reports:** this tab provides access to all the various types of reporting available. Reports can also be downloaded. Here are the most common:
 - Financial > Transaction Report* - Includes data such as transaction revenue, convenience revenue, net revenue, transaction count and average transaction amount. This report can be scheduled for email delivery.
 - Financial > Daily Total Revenue* - Includes a bar graph of the same data as transaction report
 - Financial > Summary Zone* - Includes same data as Transaction Report, split by zone
 - Customer > User* - Includes data such as # of new customers, # of unique customers, total transactions, wallet fund transactions, # of wallets, # of deactivated accounts and # of active accounts.
 - Merchant report



Next Steps

1. **Practicing with OpsMan:** we recommend spending time after this training to review the tabs we discussed and to try running reports. This will help you get comfortable with where things are and to start setting up reports you'd like to see more regularly.
2. **Reviewing your setup:** while you are practicing with the system, please review your setup to ensure the system is set to your requirements including zones, rates and restrictions. Should you find anything does not match your requirements, please contact me immediately.
3. **Marketing to your parking community:** spread the word! If you haven't already, you will receive your marketing materials ordered at the time of implementation according to the package you selected. Please ensure all materials reflect the correct information and start distributing this material, including proper signage as soon as possible.
4. **Staying in touch:** As a reminder, I am available for any account related questions. If you're not sure where to send an inquiry, you can feel free to reach out to me and I can re-direct to the right team.

Happy Parking! Looking forward to a great partnership.



Passport
Type 2 SSAE 16
2015



**REPORT ON MANAGEMENT'S DESCRIPTION OF PASSPORT'S SYSTEM AND
THE SUITABILITY OF THE DESIGN AND OPERATING
EFFECTIVENESS OF CONTROLS**

**Pursuant to Statement on Standards for Attestation Engagements No. 16
(SSAE 16) Type 2**

January 1, 2015 Through November 30, 2015

Table of Contents

SECTION 1 INDEPENDENT SERVICE AUDITOR’S REPORT	2
SECTION 2 PASSPORT’S ASSERTION	5
SECTION 3 DESCRIPTION OF THE SYSTEM PROVIDED BY THE SERVICE ORGANIZATION	8
OVERVIEW OF OPERATIONS	9
Company Background	9
Description of Services Provided	9
CONTROL ENVIRONMENT	10
Integrity and Ethical Values	10
Commitment to Competence	11
Executive Participation	11
Management’s Philosophy and Operating Style	11
Organizational Structure and Assignment of Authority and Responsibility	11
Human Resources Policies and Practices	12
RISK ASSESSMENT	12
CONTROL OBJECTIVE AND RELATED CONTROL ACTIVITIES	13
MONITORING	13
INFORMATION AND COMMUNICATION SYSTEMS	13
Information Systems	13
Communication Systems	15
COMPLEMENTARY USER ENTITY CONTROLS	16
SECTION 4 TESTING OF CONTROL OBJECTIVES AND RELATED CONTROL ACTIVITIES PROVIDED BY THE SERVICE AUDITOR	17
GUIDANCE REGARDING INFORMATION PROVIDED BY THE SERVICE AUDITOR	18
INFORMATION SECURITY	19
APPLICATION CHANGE CONTROL	23
SERVICE FEE IMPLEMENTATION	25
WALLET LOADING	26
TRANSACTION PROCESSING	27
OPERATOR REPORTING	29

SECTION 1
INDEPENDENT SERVICE AUDITOR'S REPORT



**INDEPENDENT SERVICE AUDITOR'S REPORT
ON A DESCRIPTION OF PASSPORT'S SYSTEM AND
THE SUITABILITY OF THE DESIGN AND OPERATING EFFECTIVENESS OF CONTROLS**

To Passport:

We have examined Passport's (or 'the Company') description of its Mobile Pay Transaction System at its Charlotte, North Carolina location for processing user entities' transactions for the period January 1, 2015 through November 30, 2015, and the suitability of the design and operating effectiveness of controls to achieve the related control objectives stated in the description. The description indicates that certain control objectives specified in the description can be achieved only if complementary user entity controls contemplated in the design of Passport's controls are suitably designed and operating effectively, along with related controls at the service organization. We have not evaluated the suitability of the design and operating effectiveness of such complementary user entity controls.

Passport uses Twilio for IVR and SMS Communication, Amazon AWS for third party cloud computing provider, and Authorize.net for payment gateway service provider ("subservice organizations"). The description in Section 3 includes only the controls and related control objectives of Passport and excludes the control objectives and related controls of the subservice organizations. Our examination did not extend to controls of the subservice organizations.

In Section 2 of this report, Passport has provided an assertion about the fairness of the presentation of the description and suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description. Passport is responsible for preparing the description and for the assertion, including the completeness, accuracy, and method of presentation of the description and the assertion, providing the services covered by the description, specifying the control objectives and stating them in the description, identifying the risks that threaten the achievement of the control objectives, selecting the criteria, and designing, implementing, and documenting controls to achieve the related control objectives stated in the description.

Our responsibility is to express an opinion on the fairness of the presentation of the description and on the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description, based on our examination. We conducted our examination 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 fairly presented and the controls were suitably designed and operating effectively to achieve the related control objectives stated in the description for the period January 1, 2015 through November 30, 2015.

An examination of a description of a service organization's system and the suitability of the design and operating effectiveness of the service organization's controls to achieve the related control objectives stated in the description involves performing procedures to obtain evidence about the fairness of the presentation of the description and the suitability of the design and operating effectiveness of those controls to achieve the related control objectives stated in the description. Our procedures included assessing the risks that the description is not fairly presented and that the controls were not suitably designed or operating effectively to achieve the related control objectives stated in the description. Our procedures also included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the related control objectives stated in the description were achieved. An examination engagement of this type also includes evaluating the overall presentation of the description and the suitability of the control objectives stated therein, and the suitability of the criteria specified by the service organization and described in Section 2. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Because of their nature, controls at a service organization may not prevent, or detect and correct, all errors or omissions in processing or reporting transactions. Also, the projection to the future of any evaluation of the fairness of the presentation of the description, or conclusions about the suitability of the design or operating effectiveness of the controls to achieve the related control objectives is subject to the risk that controls at a service organization may become inadequate or fail.

In our opinion, in all material respects, based on the criteria described in Passport's assertion in Section 2 of this report,

- the description fairly presents the system that was designed and implemented for the period January 1, 2015 through November 30, 2015.
- the controls related to the control objectives stated in the description were suitably designed to provide reasonable assurance that the control objectives would be achieved if the controls operated effectively for the period January 1, 2015 through November 30, 2015 and user entities applied the complementary user entity controls contemplated in the design of Passport's controls for the period January 1, 2015 through November 30, 2015.
- the controls tested, which together with the complementary user entity controls referred to in the scope paragraph of this report, if operating effectively, were those necessary to provide reasonable assurance that the control objectives stated in the description were achieved, operated effectively for the period January 1, 2015 through November 30, 2015.

The specific controls tested and the nature, timing, and results of those tests are listed in Section 4.

This report, including the description of tests of controls and results thereof in Section 4, is intended solely for the information and use of Passport, user entities of Passport's system during some or all of the period January 1, 2015 through November 30, 2015, and the independent auditors of such user entities, who have a sufficient understanding to consider it, along with other information including information about controls implemented by user entities themselves, when assessing the risks of material misstatements of user entities' financial statements. This report is not intended to be and should not be used by anyone other than these specified parties.



January 12, 2016
Tampa, Florida

SECTION 2
PASSPORT'S ASSERTION



Passport's Assertion

January 12, 2016

We have prepared the description of Passport's Mobile Pay Transaction System for user entities of the system during some or all of the period January 1, 2015 through November 30, 2015, and their user auditors who have a sufficient understanding to consider it, along with other information, including information about controls implemented by user entities of the system themselves, when assessing the risks of material misstatements of user entities' financial statements. We confirm, to the best of our knowledge and belief, that:

- a. The description fairly presents the Mobile Pay Transaction System made available to user entities of the system during some or all of the period January 1, 2015 through November 30, 2015 for processing their transactions. The criteria we used in making this assertion were that the description:
 - i. presents how the system made available to user entities of the system was designed and implemented to process relevant transactions, including:
 - (1) The types of services provided including, as appropriate, the classes of transactions processed.
 - (2) The procedures, within both automated and manual systems, by which services are provided, including, as appropriate, procedures by which transactions are initiated, authorized, recorded, processed, corrected as necessary, and transferred to reports and other information prepared for user entities.
 - (3) The related accounting records, supporting information, and specific accounts that are used to initiate, authorize, record, process, and report transactions; this includes the correction of incorrect information and how information is transferred to the reports and other information prepared for user entities.
 - (4) How the system captures significant events and conditions, other than transactions.
 - (5) The process used to prepare reports and other information for user entities.
 - (6) The specified control objectives and controls designed to achieve those objectives, including as applicable, complementary user entity controls contemplated in the design of the service organization's controls.
 - (7) Other aspects of our control environment, risk assessment process, information and communication systems (including related business processes), control activities, and monitoring controls that are relevant to processing and reporting transactions of user entities of the system.
 - ii. does not omit or distort information relevant to the scope of the Mobile Pay Transaction System, while acknowledging that the description is prepared to meet the common needs of broad range of user entities of the system and the independent auditors of those user entities, and may not, therefore, include every aspect of the Mobile Pay Transaction System that each individual user entity of the system and its auditor may consider important in its own particular environment.

- b. The description includes relevant details of changes to the service organization's system during the period covered by the description when the description covers a period of time.
- c. The controls related to the control objectives stated in the description were suitably designed and operated effectively for the period January 1, 2015 through November 30, 2015 to achieve those control objectives. The criteria we used in making this assertion were that:
 - i. the risks that threaten the achievement of the control objectives stated in the description have been identified by the service organization;
 - ii. the controls identified in the description would, if operating as described, provide reasonable assurance that those risks would not prevent the control objectives stated in the description from being achieved; and
 - iii. the controls were consistently applied as designed, including whether manual controls were applied by individuals who have the appropriate competence and authority.



Bob Youakim
Managing Partner
Passport

SECTION 3
DESCRIPTION OF THE SYSTEM PROVIDED
BY THE SERVICE ORGANIZATION

OVERVIEW OF OPERATIONS

Company Background

Passport (or the “Company”) is a private company, headquartered in Charlotte, North Carolina. Passport offers a fully integrated cloud-based parking management and payment solution to its customers through the Internet and mobile application. The Passport mobile application provides the ability to pay for parking from a mobile phone. Payments are accepted through e-commerce via the Internet or mobile devices, including phone and text orders. The system also provides the ability for validation at checkout. The application also provides parking validation functionality allowing parking management companies to create custom parking validations, manage their funds, and monitor any activity. Parking management companies gain total control of all parking activity with real-time reporting and logs of each transaction.

Description of Services Provided

Passport offers a fully integrated cloud-based parking management and payment solution to its customers through the Internet and mobile application.

Business Role with Payment Cards

Passport receives card-not-present orders through their hosted online website and mobile ordering application. Customers “parkers” input payment card data at the time of account registration. Upon completion of the registration process, customers pay for their parking with the stored payment card data and are not required to submit new payment data each time they pay for parking. Passport provides a secure application payment interface for the customer registration process. Passport receives the payment information through the web or mobile interface.

Passport also provides text and interactive voice response (“IVR”) system interfaces as well. The pay via text process allows you to pay via texting the zone and space number to a phone number. This starts the parking booking process with credit card you have on file. The pay via voice process asks for zone number and space number and allows customer to change their credit card information via an IVR.

Passport uses service provided by Twilio, Amazon AWS, and Authorize.Net for the following services. Passport uses Twilio for IVR and SMS communication. Passport uses the services of Amazon AWS as a third party cloud computing provider that houses all Passport cardholder data and cloud computing space. Authorize.Net is a payment gateway service provider allowing merchants to accept credit card and electronic check payments through their Web site and over an IP (Internet Protocol) connection. This description does not include the control objectives and related controls of the Subservice Organizations.

Service Fee Implementation

Passport’s business customers utilize the online and mobile parking application to provide parking payment solutions to parkers. Business customers must set up an account with Passport to offer the online and mobile services for the parking locations owned by the business customers. As part of the account setup process, Passport completes an Implementation Checklist which includes details regarding the parking locations, spaces, times, and service fees. Service fees depend on the location, space, and time of the park. Rates can fluctuate to reflect current events, early park discounts, premium parking locations, standard rates, among other things. The Implementation Checklist is utilized to ensure the variables in the setup of the account, and the related service fees, are accurate. Confirmation of the accurate setup of new customer accounts, which includes the accurate service fee implementation, is received prior to customer account go-live. Access to make changes to the customer service fees is limited to authorized personnel within Passport. Business customers also have the ability to set up service fees after the initial account setup process.

Wallet Loading

Passport offers parkers the ability to purchase a wallet. A wallet allows the parker to pay a specific dollar amount which is credited to their wallet. Each time the parker purchases a space to park, the transaction amount for that space is deducted from the wallet. Notification of parker charges are communicated to the parker prior to the transaction processing. As part of the account setup process, Passport processes test transactions through the account. Test transactions are reviewed to ensure they are processed through the parker wallets accurately and timely. Test transactions are a step within the Implementation Checklist prior to the go-live date. Access to make changes to parker wallets is limited to authorized personnel within Passport.

Transaction Processing and Operator Reporting

Passport provides operator reports and transaction details of all parker activity to the business customers for their respective parking locations. Operator reports and the related transaction details are available to business customers on a real-time basis. Business customers can access their reports through their accounts with Passport. These reports are utilized by business customers to reconcile charges to their accounts and the funds posted to their bank accounts. Funds are posted to the business customer's bank accounts on a daily basis. During the account setup process, business customers are involved in reconciling test transactions. Errors in reporting, whether it is during the account setup process or during live processing of transactions, are communicated to Passport and researched and resolved by the Support team. Passport also monitors transaction processing on a daily basis. Errors are posted real time and are recorded on a log. The log is reviewed by members of the Support team on a daily basis. If errors have occurred, they are reviewed and resolved the same day.

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 the Organization's control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior is the product of Company'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:

- Organizational policy statements and codes of conduct are documented and communicate entity values and behavioral standards to personnel. The employee policy and procedures manual contains organizational policy statements and codes of conduct to which employees are required to adhere
- Policies and procedures require that employees sign an acknowledgment form indicating that 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. Credit checks are performed for back office employees as a component of the hiring process

Commitment to Competence

Company'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
- A training program has been developed to maintain the skill level of personnel in certain positions

Executive Participation

The Company's executives have the ultimate responsibility for overseeing the business policies of the service organization. The executive team, composed of internal business partners, meets to discuss matters pertinent to the Company's operations and to review financial results.

Management's Philosophy and Operating Style

Company'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
- Management meetings are held on a regular basis to discuss major initiatives and issues that impact the business as a whole. It is expected that management members are prepared to provide clear and concise updates

Organizational Structure and Assignment of Authority and Responsibility

The Company's organizational structure provides the framework within which activities for achieving objectives are planned, executed, controlled and monitored. The organizational structure described below details the departments of the service organization that provide Mobile Payment Services for its clients. The structure provides for an adequate segregation of duties as well as clearly defined areas of responsibility.

Department	Description
Information Technology	The Information Technology ("IT") Staff is responsible for activities associated with developing, maintaining and supporting critical data processing systems. The organizational structure of the Information Technology staff provides segregation of duties between client services, systems programming, application programming, computer operations, physical and logical security access and documentation
Operations	The Operations Staff is responsible for day-to-day collection activities, hiring, training, and quality assurance. The Operations Staff is also responsible for setting and sustaining client and the service organization's goals
Administrative	The Administrative Staff is responsible for receiving, identifying, posting and depositing all payments received each day in a timely and accurate manner. The Administrative Staff also documents all incoming correspondence. They also ensure that all required licensing is obtained and current

Human Resources Policies and Practices

Company'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, from the collectors who contact the individuals to the management team who ensures the service organization is operating at maximum efficiency.

Upon being hired, new employees are issued an employee packet documenting various procedural and administrative matters, which is then discussed during the new hire orientation program. Human Resources creates and ensures adherence to policies, which include but are not limited to Employment, Non-Disclosure, Employee Status, Timekeeping and Payroll, Work Conditions and Hours, Employee Conduct and Disciplinary Action, and Employee Benefit Programs. Employees sign off on policies which include but are not limited to Employee Conduct and Work Rules, Company Privacy Policy, and Collection Regulations and Rules of Conduct.

Management checks trustworthiness and reliability for all personnel prior to employment through pre-screening procedures. Standard pre-screening interviews and testing are conducted by the in-house recruiting department. Background investigations are performed by the recruiter through an FCRA-regulated vendor.

In addition, the Human Resources department administers the Information Security/Privacy Policies for all employees, which addresses the sensitivity of customer information and how the service organization safeguards this information. Employees are required to sign acknowledgement forms, which are kept in the Personnel files maintained by the Company.

Company Management follows a standard exit procedure for all personnel leaving employment or changing job roles or location. This procedure includes notifying the relevant management team, communicating official termination procedures, notifying the IT department to review all relevant access within the systems, returning all company property, including company books, materials, keys, ID badges, computers, cell phones, and any other company owned items.

RISK ASSESSMENT

Passport has placed into operation a risk assessment process to identify and manage risks that could affect the organization's ability to provide reliable transaction processing for user organizations. This process requires management to identify significant risks in their areas of responsibility and to implement appropriate measures to address those risks.

Risks that are considered during management's risk assessment activities include the following:

- Changes in operating environment
- New personnel
- New or revamped information systems
- Rapid growth
- New technology
- New accounting pronouncements

Management's recognition of risks that could affect the organization's ability to provide reliable transaction processing for its user organizations is generally implicit, rather than explicit. Management's involvement in the daily operations allows them to learn about risks through direct personal involvement with employees and outside parties, thus reducing the need for formalized and structured risk assessment processes.

CONTROL OBJECTIVE AND RELATED CONTROL ACTIVITIES

Integration with Risk Assessment

Along with assessing risks, Passport has identified and put into effect actions needed to address those risks. In order to address risks, control activities have been placed into operation to help ensure that the actions are carried out properly and efficiently. Control activities serve as mechanisms for managing the achievement of those objectives.

Selection and Development of Control Activities Specified by the Service Organization

Control activities are a part of the process by which Passport strives to achieve its business objectives. Passport has applied a risk management approach to the organization in order to select and develop control activities. After relevant risk have been identified and evaluated, controls are established, implemented, monitored, reviewed and improved when necessary to meet the overall objectives of the organization.

Passport's control objectives and related control activities are included in Section 4 (the "Testing Matrices") of this report to eliminate the redundancy that would result from listing the items in this section and repeating them in the Testing Matrices. Although the control objectives and related control activities are included in the Testing Matrices, they are, nevertheless, an integral part of Passport's description of the data center services system.

The description of the service auditor's tests of operating effectiveness and the results of those tests are also presented in the Testing Matrices, adjacent to the service organization's description of control activities. The description of the tests of operating effectiveness and the results of those tests are the responsibility of the service auditor and should be considered information provided by the service auditor.

MONITORING

Passport's management performs monitoring activities in order to continuously assess the quality of internal control over time. Monitoring activities are used to initiate corrective action through personnel meetings, client conference calls, and informal notifications. Monitoring activities are conducted on a continuous basis and necessary corrective actions are taken as required to correct deviations from company policy and procedures.

Management's direct involvement in key operations facilitates identifying significant variances from expectations regarding internal controls. Management immediately evaluates the specific facts and circumstances related to any suspected control breakdowns. 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.

INFORMATION AND COMMUNICATION SYSTEMS

Information Systems

Passport employs an internally developed application, which is hosted on web servers located in a secure demilitarized zone ("DMZ") separate from the internal network. Backend supporting MySQL databases are used to store transaction data and are located on a separate network segment behind a dedicated firewall in the cloud. The Organization utilizes Active Directory for their internal network.

People

Passport staff provides support for the above services in each of the following functional areas:

- Executive management - provides general oversight and strategic planning of operations
- Systems administrators - responsible for effective provisioning, installation/configuration, operation, and maintenance of systems hardware and software relevant to the system
- Systems engineers - serves customers by providing product and service information that includes resolving product and service issues

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 Passport policies and procedures that define how services should be delivered. These are located on the Company's internal shared drive and can be accessed by any Passport team member.

Physical Security and Computer Operation

Passport uses Amazon AWS as a third party cloud computing provider that houses all Passport cardholder data and cloud computing space.

Logical Access

Passport 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, Passport 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 Passport network using an Active Directory user ID and password. Passwords must conform to defined password standards and are enforced through parameter settings in the Active Directory. 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.

Upon hire, employees are assigned to a position in the HR management system. 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 the appropriate security team. 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 Chief Technology Officer (CTO). As part of this process, the CTO reviews access by privileged roles and requests modifications based on this review.

The terminated employees' access is disabled on a timely basis. This terminated employee list is used by the security help desk to delete employee access.

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.

Change Control

Passport 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. Quality assurance testing and User Acceptance Testing (UAT) results are documented and maintained with the associated change request. 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.

Data

Customer data is managed, processed, and stored in accordance with the relevant data protection and other regulations, with specific requirements formally established in customer contracts. Customer data is captured which is utilized by Passport in delivering its Cloud-based Parking Management system.

Significant Events and Conditions

Passport has implemented automated and manual procedures to capture and address significant event and conditions. In addition, detailed monitoring and risk assessment procedures are in place to provide management with detailed information that impacts the Cloud-based Parking Management system. Please see the procedures, monitoring, and risk assessment procedures described in the relevant sections of this report for further details.

Preparation and Delivery of Reports and Data

Passport utilizes the services and procedures described above to capture, prepare, and deliver reports and other information (described in the data section above) to user entities and other parties.

Communication Systems

Communication is an integral component of Passport'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 Passport, information is identified, captured, processed, and reported by various information systems, as well as through conversations with clients, vendors, regulators, and employees.

Upper management is involved with day-to-day operations and is able to provide personnel with an understanding of their individual roles and responsibilities pertaining to internal controls. This includes the extent to which personnel understand how their activities relate to the work of others and the means of reporting exceptions to a higher level within Passport. Management believes that open communication channels help ensure that exceptions are reported and acted on. For that reason, formal communication tools such as organizational charts, employee handbooks, training classes and job descriptions are in place at Passport. Management's communication activities are made electronically, verbally, and through the actions of management.

COMPLEMENTARY USER ENTITY CONTROLS

Passport'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 of the control objectives related to Passport's services to be solely achieved by Passport control procedures. Accordingly, user entities, in conjunction with the services should establish their own internal controls or procedures to complement those of Passport.

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the control objectives 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 maintaining authorized user access to the Passport application and periodically reviewing and updating these users.
2. User entities are responsible for removing user access to the Passport application when terminating an employee.
3. User entities are responsible for using strong password and access codes to access all systems, including, but not limited to the Passport application.
4. User entities are responsible for appropriate design and implementation of security architecture for equipment including firewalls: switch, and router configuration accessing the Passport application.
5. User entities are responsible for having authorized personnel available to report issues and resolve them with Passport personnel.
6. User entities are responsible for immediately notifying Passport of any actual or suspected information security breaches, including compromised user accounts.
7. User entities are responsible for developing their own disaster recovery and business continuity plans that address their inability to access or utilize Passports services.
8. User entities are responsible for reconciling daily transactions and operator reports back to funds deposited within their accounts.
9. User entities are responsible for the accurate setup of service fees after the initial setup of the account.
10. User entities are responsible for complying all laws and regulations with respect to security, availability, maintainability, and integrity.
11. User entities are responsible for understanding and complying with the terms of service and their contractual obligations to Passport.

SECTION 4

TESTING OF CONTROL OBJECTIVES AND RELATED CONTROL ACTIVITIES PROVIDED BY THE SERVICE AUDITOR

GUIDANCE REGARDING INFORMATION PROVIDED BY THE SERVICE AUDITOR

A-lign's examination of the controls of Passport was limited to the control objectives and related control activities specified by the management of Passport and did not encompass all aspects of Passport's operations or operations at user organizations. Our examination was performed in accordance with American Institute of Certified Public Accountants (AICPA) Statement on Standards for Attestation Engagements No. 16 (SSAE 16).

Our examination of the control activities were performed using the following testing methods:

TEST	DESCRIPTION
Inquiry	The service auditor made inquiries of service organization personnel. Inquiries were made to obtain information and representations from the client to determine that the client's knowledge of the control and corroborate policy or procedure information.
Observation	The service auditor observed application of the control activities by client personnel.
Inspection	The service auditor inspected among other items, source documents, reports, system configurations to determine performance of the specified control activity and in some instances the timeliness of the performance of control activities.
Re-performance	The service auditor independently executed procedures or controls that were originally performed by the service organization as part of the entity's internal control.

In determining whether a SSAE 16 report meets the user auditor's objectives, the user auditor should perform the following procedures:

- Understand the aspects of the service organization's controls that may affect the processing of the user organization's transactions;
- Understand the flow of significant transactions through the service organization;
- Determine whether the control objectives are relevant to the user organization's financial statement assertions;
- Determine whether the service organization's controls are suitably designed to prevent or detect processing errors that could result in material misstatements in the user organization's financial statements and determine whether they have been implemented.

CONTROL AREA 1 INFORMATION SECURITY

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that system information, once entered into the system, is protected from unauthorized or unintentional use, modification, addition or deletion.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
1.1	Formal information security policies and procedures are in place and communicated to all users with access to the systems.	<p>Inspected information security policies and procedures to determine that formal information security policies and procedures were in place.</p> <p>Inspected the training materials and training attendance form to determine that periodic education and training was provided to the users related to the company policies and procedures.</p> <p>Inspected completed Acknowledgement forms for a sample of new hired during the audit period to determine that formal information security policies and procedures were communicated to all the users with access to the systems.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p>
1.2	SSH access is executed via public key authentication, enabling the avoidance of using shared passwords and allows Passport to restrict access to only users with private keys.	<p>Inspected SSH access via public key authentication configuration to determine that individual authentication through passwords was enforced.</p> <p>Inspected the user directory to determine that authentication was restricted to authorized users.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>
1.3	Administrator access is restricted to authorized user accounts and in line with their job function.	<p>Inspected a list of administrators to determine that administrator access was restricted to authorized user accounts and in line with their job function.</p> <p>Inspected the authorized user list to determine that users had appropriate access to the database based on the job responsibilities.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>
1.4	Users are required to authenticate via a user account and password before being granted access to the system.	Observed the log-on process to determine that users were required to authenticate via a user account and password before being granted access to the system.	No exceptions noted.

CONTROL AREA 1 INFORMATION SECURITY

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that system information, once entered into the system, is protected from unauthorized or unintentional use, modification, addition or deletion.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
1.5	Access to system requires a documented approval by authorized parties specifying required privileges.	<p>Inspected the SSH key user authentication to determine that users were required to authenticate via a user account and password before being granted access to the system.</p> <p>Inquired of Brad Powers, Chief Technology Officer (CTO) regarding the utilization of the authorization form for user access to determine that access to system required a documented approval by authorized parties specifying required privileges.</p> <p>Inspected New Hire Policy within the Security Policy obtained from Brad Powers, Chief Technology Officer (CTO) to determine that utilization of an Authorization Form for User Access was required for all new hires prior to gaining access to the system.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p>
1.6	Access to the system is revoked as a component of the termination process.	<p>Inspected new hire authorization forms for a samples of new hires to determine that access to system required a documented approval by authorized parties specifying required privileges.</p> <p>Inquired of Brad Powers, Chief Technology Officer (CTO) regarding user access revocation to determine that access to the system was revoked as a component of the termination process.</p> <p>Inspected user access revocation policy and procedures within the information policy to determine that policy and procedures existed to revoke user's access as a component of the termination process.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>

CONTROL AREA 1 INFORMATION SECURITY

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that system information, once entered into the system, is protected from unauthorized or unintentional use, modification, addition or deletion.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
1.7	Anti-virus software is installed on production servers to detect and prevent the transmission of data or files that contain virus signatures recognized by the anti-virus software.	Inspected user access revocation confirmation for a sample of terminated employees to determine that access to the system was revoked as a component of the termination process.	No exceptions noted.
1.8	Procedures exist to identify, report, and act upon system confidentiality and security breaches and other incidents.	<p>Inspected anti-virus software configuration on a sample of production servers to determine that anti-virus software was installed on production servers to detect and prevent the transmission of data or files that contain virus signatures recognized by the anti-virus software.</p> <p>Inspected anti-virus update settings for a sample of production servers to determine that anti-virus software was up to date.</p> <p>Inquired of Brad Powers, Chief Technology Officer (CTO) regarding system confidentiality and security to determine that procedures existed to identify, report, and act upon system confidentiality and security breaches and other incidents.</p> <p>Inspected evidence of recurring daily security review calendar invitation to determine that procedures existed to identify, report, and act upon system confidentiality and security breaches and other incidents.</p> <p>Inspected evidence of a daily security review summary to determine that procedures exist to identify, report, and act upon system confidentiality and security breaches and other incidents.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p>

CONTROL AREA 1 INFORMATION SECURITY

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that system information, once entered into the system, is protected from unauthorized or unintentional use, modification, addition or deletion.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
1.9	System components and software are protected from known vulnerabilities through installation of the latest vendor-supplied security patches.	Inspected configuration of security monitoring software to determine that system components and software were protected from known vulnerabilities through installation of the latest vendor-supplied security patches.	No exceptions noted.
1.10	Firewalls are installed on the Passport Systems and applications. Management periodically reviews the firewall settings to ensure access is limited appropriately.	<p>Inspected firewall settings for a sample of servers to determine that firewalls were installed on the Passport Systems and applications.</p> <p>Inspected evidence of management's review of firewall settings to determine firewalls were installed on the Passport Systems and applications and that management reviewed the firewall settings to ensure access was limited appropriately.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>

CONTROL AREA 2 APPLICATION CHANGE CONTROL

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that unauthorized changes are not made to production application systems.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
2.1	Formal application change control policies and procedures are in place and communicated to all users with access to the systems.	<p>Inspected application change control policies and procedures to determine that formal application change control policies and procedures were in place.</p> <p>Inspected the training materials and training attendance form to determine that periodic education and training was provided to the users related to the application change control policies and procedures.</p> <p>Inspected completed Acknowledgement forms for a sample of new hired during the audit period to determine that formal application change control policies and procedures were in place and communicated to all users with access to the systems.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p>
2.2	A change management software is utilized to maintain and control infrastructure application changes, and the associated reporting and logging functions.	<p>Inquired the Chief Technology Officer (CTO) Brad Powers to determine that a change management software was utilized to maintain and control infrastructure and application logging changes, and the associated reporting and logging functions.</p> <p>Inspected a sample of change tickets to determine that a change management software was utilized to maintain and control infrastructure and application changes, and the associated reporting and logging functions.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>
2.3	Documented change request are reviewed and prioritized by management based on business needs and resource availability, and assigned to personnel for action.	Inquired Chief Technology Officer (CTO) Brad Powers to determine documented change requests were completed for infrastructure projects and reviewed and prioritized by management based on business needs and resource availability, and assigned to personnel for action.	No exceptions noted.

CONTROL AREA 2 APPLICATION CHANGE CONTROL

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that unauthorized changes are not made to production application systems.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected a sample of change tickets to determine documented change request was completed for infrastructure projects and reviewed and prioritized by management based on business needs and resource availability, and assigned to personnel for action.	No exceptions noted.
2.4	Development/test environments exist and are separate from the production environment.	Inspected evidence of the development and test environments to determine that development/test environments exist and were separate from the production environment.	No exceptions noted.
2.5	Application and other infrastructure changes are authorized, tested, and approved for implementation prior to actual implementation.	Inspected a sample of change tickets to determine that application and other infrastructure changes were authorized, tested, and approved for implementation prior to actual implementation.	No exceptions noted.
2.6	Access to implement changes to production environment is limited to authorized individuals.	Inspected list of users with access to promote changes to production to determine that access to promote changes to production was limited to appropriate personnel.	No exceptions noted.
2.7	Production changes are appropriately logged and monitored on a daily basis.	<p>Inquired of Chief Technology Officer (CTO) Brad Powers regarding the daily review of the system monitoring log to determine that changes promoted to production were appropriately logged and monitored.</p> <p>Inspected evidence of a daily review of the system monitoring log to determine that changes promoted to production were appropriately logged and monitored on a daily basis.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>

CONTROL AREA 3 SERVICE FEE IMPLEMENTATION

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that service fees are initially implemented accurately according to client instructions.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
3.1	Access to set up service fees are limited to authorized personnel.	<p>Inquired of Chief Technology Officer regarding the user access list with authorities to setup service fees to determine access was limited to authorized users, based on job responsibilities.</p> <p>Inspected user access list with authorities to determine that access to set up service fees were limited to authorized personnel, based on job responsibilities.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>
3.2	An Implementation Checklist is completed as part of the initial implementation of service fees for new customers.	<p>Inquired of Chief Technology Officer regarding the new customers' setup to determine the checklist was completed, including the accurate setup of service fees for new customers' setup.</p> <p>Inspected new customer implementation checklists for a sample of new customer's setup to determine the checklist was completed, including the accurate setup of service fees.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>
3.3	Customer sign-off of new customer setup, including accurate service fees implementation, is received prior to customer account go-live.	<p>Inquired of Chief Technology Officer regarding the new customers' setup to determine that customers reviewed and approved the account setup prior to the account go-live.</p> <p>Inspected customer sign-offs within the new customer implementation checklist for a sample of new customers' setup to determine that customers reviewed and approved the account setup prior to the account go-live.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>

CONTROL AREA 4 WALLETS LOADING

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that parker wallets are loaded accurately and timely.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
4.1	Parker wallets are automatically and accurately loaded to the system.	<p>Inquired of Chief Technology Officer (CTO) regarding parker wallets to determine that parker wallets were automatically and accurately loaded to the system.</p> <p>Inspected a sample of wallet loading transactions to determine that parker wallets were automatically and accurately loaded to the system.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>
4.2	Notification of parker charges are communicated to the parker prior to the transaction processing.	<p>Inspected system configuration from the production system to determine that the system was configured to notify charges to the parker prior to transaction processing.</p> <p>Inspected a sample of parker charge notification obtained from Chief Technology Officer (CTO), to determine that notification of parker charges were communicated to the parker prior to transaction processing.</p> <p>Inspected a sample of parker charge notifications to determine that notification of wallet updating was communicated to the parker prior to being charged.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p>
4.3	Access to make changes to parker wallets is limited to authorized personnel.	Inspected administrative accounts with authorities to make changes to parker wallets to determine that access to make changes to the parker wallets was limited to authorized personnel.	No exceptions noted.

CONTROL AREA 5 TRANSACTION PROCESSING

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that transactions are updated accurately in parker wallets.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
5.1	An implementation checklist is maintained for each new customer setup. As part of the customer setup, test transactions are processed to ensure customer wallets are loaded accurately. Customers confirm transactions have been processed in the wallet accurately.	<p>Inquired of Chief Technology Officer (CTO) regarding the new customer setup process to determine that an implementation checklist was maintained for each new customer setup. As part of the customer setup, test transactions were processed to ensure customer wallets were loaded accurately. Customers confirmed transactions had been processed in the wallet accurately.</p> <p>Inspected new customer implementation checklists for a sample of new customers' to determine the checklist was maintained for each new customer setup and that test transactions were processed to ensure customer wallets were loaded accurately. Customers confirmed transactions had been processed in the wallet accurately.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>
5.2	Errors in transaction processing are recorded real time. A review of any errors is performed on a daily basis by the Technology team. Errors are reviewed and resolved.	<p>Inspected a daily error log to determine that errors in transaction processing were reviewed and resolved throughout the day.</p> <p>Inspected a sample of error log/resolution tickets to determine that errors in transaction were recorded, reviewed and resolved timely.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>
5.3	Access to make changes to the parker wallets is limited to authorized personnel.	Inspected the user access listing for those users with authorities to make changes to parker wallets to determine that access to make changes to the parker wallets was limited to authorized personnel.	No exceptions noted.

CONTROL AREA 5 TRANSACTION PROCESSING

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that transactions are updated accurately in parker wallets.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
5.4	Parker wallets changes follow the Passport change management process.	<p>Inquired of the Chief Technology Officer (CTO) regarding the parker wallets changes to determine that parker wallets changes followed Passport change management process.</p> <p>Inspected a sample of parker wallets changes to determine that parker wallets changes followed Passport change management process.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>

CONTROL AREA 6 OPERATOR REPORTING

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that operator reports reflect parker activity and financial transactions.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
6.1	An implementation checklist is maintained for each new customer setup. Customers confirm operator reports reflect accurate parker activity and financial transactions.	<p>Inquired of Chief Technology Officer regarding the new customers' setup to determine that the checklist was maintained for customer setup and that report was confirmed by the customers to reflect the accurate parker activity and the financial transactions.</p> <p>Inspected the new customer implementation checklist for a sample of new customers to determine the checklist was maintained for each new customer setup and that it was part of the customer setup process.</p> <p>Inspected the implementation checklist for a sample of new customers' setup to determine that new customers confirmed operator reports reflected accurate parker activity and financial transactions.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p>
6.2	Errors in reporting are researched and resolved by the Passport Support team.	Inspected a sample of error log/resolution tickets to determine that errors in reporting were recorded, reviewed and resolved timely.	No exceptions noted.
6.3	Access to make changes to the operator reports is limited to appropriate personnel.	<p>Inquired of the Chief Technology Officer (CTO) regarding privileged users' access necessary to make changes to the operator reports to determine that access to make changes to the operator reports was limited to appropriate personnel.</p> <p>Inspected user access accounts with authorities to make changes to operator wallets to determine that access to make changes to the operator wallets was limited to authorized personnel.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>

CONTROL AREA 6 OPERATOR REPORTING

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that operator reports reflect parker activity and financial transactions.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
6.4	Operator reports changes follow the Passport change management process.	<p>Inquired of the Chief Technology Officer (CTO) regarding the operator reports changes to determine that operator reports changes followed the Passport change management process.</p> <p>Inspected a sample of operator reports changes to determine that operator reports changes followed the Passport change management process.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>



A-ALIGN



Passport
Type 2 SSAE 16
2015



Passport

**REPORT ON MANAGEMENT'S DESCRIPTION OF PASSPORT'S SYSTEM AND
THE SUITABILITY OF THE DESIGN AND OPERATING
EFFECTIVENESS OF CONTROLS**

**Pursuant to Statement on Standards for Attestation Engagements No. 16
(SSAE 16) Type 2**

January 1, 2015 Through November 30, 2015

Table of Contents

SECTION 1 INDEPENDENT SERVICE AUDITOR’S REPORT	2
SECTION 2 PASSPORT’S ASSERTION	5
SECTION 3 DESCRIPTION OF THE SYSTEM PROVIDED BY THE SERVICE ORGANIZATION	8
OVERVIEW OF OPERATIONS	9
Company Background	9
Description of Services Provided	9
CONTROL ENVIRONMENT	10
Integrity and Ethical Values	10
Commitment to Competence	11
Executive Participation	11
Management’s Philosophy and Operating Style	11
Organizational Structure and Assignment of Authority and Responsibility	11
Human Resources Policies and Practices	12
RISK ASSESSMENT	12
CONTROL OBJECTIVE AND RELATED CONTROL ACTIVITIES	13
MONITORING	13
INFORMATION AND COMMUNICATION SYSTEMS	13
Information Systems	13
Communication Systems	15
COMPLEMENTARY USER ENTITY CONTROLS	16
SECTION 4 TESTING OF CONTROL OBJECTIVES AND RELATED CONTROL ACTIVITIES PROVIDED BY THE SERVICE AUDITOR	17
GUIDANCE REGARDING INFORMATION PROVIDED BY THE SERVICE AUDITOR	18
INFORMATION SECURITY	19
APPLICATION CHANGE CONTROL	23
SERVICE FEE IMPLEMENTATION	25
WALLET LOADING	26
TRANSACTION PROCESSING	27
OPERATOR REPORTING	29

SECTION 1
INDEPENDENT SERVICE AUDITOR'S REPORT



**INDEPENDENT SERVICE AUDITOR'S REPORT
ON A DESCRIPTION OF PASSPORT'S SYSTEM AND
THE SUITABILITY OF THE DESIGN AND OPERATING EFFECTIVENESS OF CONTROLS**

To Passport:

We have examined Passport's (or 'the Company') description of its Mobile Pay Transaction System at its Charlotte, North Carolina location for processing user entities' transactions for the period January 1, 2015 through November 30, 2015, and the suitability of the design and operating effectiveness of controls to achieve the related control objectives stated in the description. The description indicates that certain control objectives specified in the description can be achieved only if complementary user entity controls contemplated in the design of Passport's controls are suitably designed and operating effectively, along with related controls at the service organization. We have not evaluated the suitability of the design and operating effectiveness of such complementary user entity controls.

Passport uses Twilio for IVR and SMS Communication, Amazon AWS for third party cloud computing provider, and Authorize.net for payment gateway service provider ("subservice organizations"). The description in Section 3 includes only the controls and related control objectives of Passport and excludes the control objectives and related controls of the subservice organizations. Our examination did not extend to controls of the subservice organizations.

In Section 2 of this report, Passport has provided an assertion about the fairness of the presentation of the description and suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description. Passport is responsible for preparing the description and for the assertion, including the completeness, accuracy, and method of presentation of the description and the assertion, providing the services covered by the description, specifying the control objectives and stating them in the description, identifying the risks that threaten the achievement of the control objectives, selecting the criteria, and designing, implementing, and documenting controls to achieve the related control objectives stated in the description.

Our responsibility is to express an opinion on the fairness of the presentation of the description and on the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description, based on our examination. We conducted our examination 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 fairly presented and the controls were suitably designed and operating effectively to achieve the related control objectives stated in the description for the period January 1, 2015 through November 30, 2015.

An examination of a description of a service organization's system and the suitability of the design and operating effectiveness of the service organization's controls to achieve the related control objectives stated in the description involves performing procedures to obtain evidence about the fairness of the presentation of the description and the suitability of the design and operating effectiveness of those controls to achieve the related control objectives stated in the description. Our procedures included assessing the risks that the description is not fairly presented and that the controls were not suitably designed or operating effectively to achieve the related control objectives stated in the description. Our procedures also included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the related control objectives stated in the description were achieved. An examination engagement of this type also includes evaluating the overall presentation of the description and the suitability of the control objectives stated therein, and the suitability of the criteria specified by the service organization and described in Section 2. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Because of their nature, controls at a service organization may not prevent, or detect and correct, all errors or omissions in processing or reporting transactions. Also, the projection to the future of any evaluation of the fairness of the presentation of the description, or conclusions about the suitability of the design or operating effectiveness of the controls to achieve the related control objectives is subject to the risk that controls at a service organization may become inadequate or fail.

In our opinion, in all material respects, based on the criteria described in Passport's assertion in Section 2 of this report,

- the description fairly presents the system that was designed and implemented for the period January 1, 2015 through November 30, 2015.
- the controls related to the control objectives stated in the description were suitably designed to provide reasonable assurance that the control objectives would be achieved if the controls operated effectively for the period January 1, 2015 through November 30, 2015 and user entities applied the complementary user entity controls contemplated in the design of Passport's controls for the period January 1, 2015 through November 30, 2015.
- the controls tested, which together with the complementary user entity controls referred to in the scope paragraph of this report, if operating effectively, were those necessary to provide reasonable assurance that the control objectives stated in the description were achieved, operated effectively for the period January 1, 2015 through November 30, 2015.

The specific controls tested and the nature, timing, and results of those tests are listed in Section 4.

This report, including the description of tests of controls and results thereof in Section 4, is intended solely for the information and use of Passport, user entities of Passport's system during some or all of the period January 1, 2015 through November 30, 2015, and the independent auditors of such user entities, who have a sufficient understanding to consider it, along with other information including information about controls implemented by user entities themselves, when assessing the risks of material misstatements of user entities' financial statements. This report is not intended to be and should not be used by anyone other than these specified parties.



January 12, 2016
Tampa, Florida

SECTION 2
PASSPORT'S ASSERTION




Passport's Assertion

January 12, 2016

We have prepared the description of Passport's Mobile Pay Transaction System for user entities of the system during some or all of the period January 1, 2015 through November 30, 2015, and their user auditors who have a sufficient understanding to consider it, along with other information, including information about controls implemented by user entities of the system themselves, when assessing the risks of material misstatements of user entities' financial statements. We confirm, to the best of our knowledge and belief, that:

- a. The description fairly presents the Mobile Pay Transaction System made available to user entities of the system during some or all of the period January 1, 2015 through November 30, 2015 for processing their transactions. The criteria we used in making this assertion were that the description:
 - i. presents how the system made available to user entities of the system was designed and implemented to process relevant transactions, including:
 - (1) The types of services provided including, as appropriate, the classes of transactions processed.
 - (2) The procedures, within both automated and manual systems, by which services are provided, including, as appropriate, procedures by which transactions are initiated, authorized, recorded, processed, corrected as necessary, and transferred to reports and other information prepared for user entities.
 - (3) The related accounting records, supporting information, and specific accounts that are used to initiate, authorize, record, process, and report transactions; this includes the correction of incorrect information and how information is transferred to the reports and other information prepared for user entities.
 - (4) How the system captures significant events and conditions, other than transactions.
 - (5) The process used to prepare reports and other information for user entities.
 - (6) The specified control objectives and controls designed to achieve those objectives, including as applicable, complementary user entity controls contemplated in the design of the service organization's controls.
 - (7) Other aspects of our control environment, risk assessment process, information and communication systems (including related business processes), control activities, and monitoring controls that are relevant to processing and reporting transactions of user entities of the system.
 - ii. does not omit or distort information relevant to the scope of the Mobile Pay Transaction System, while acknowledging that the description is prepared to meet the common needs of broad range of user entities of the system and the independent auditors of those user entities, and may not, therefore, include every aspect of the Mobile Pay Transaction System that each individual user entity of the system and its auditor may consider important in its own particular environment.

- b. The description includes relevant details of changes to the service organization's system during the period covered by the description when the description covers a period of time.
- c. The controls related to the control objectives stated in the description were suitably designed and operated effectively for the period January 1, 2015 through November 30, 2015 to achieve those control objectives. The criteria we used in making this assertion were that:
 - i. the risks that threaten the achievement of the control objectives stated in the description have been identified by the service organization;
 - ii. the controls identified in the description would, if operating as described, provide reasonable assurance that those risks would not prevent the control objectives stated in the description from being achieved; and
 - iii. the controls were consistently applied as designed, including whether manual controls were applied by individuals who have the appropriate competence and authority.



Bob Youakim
Managing Partner
Passport

SECTION 3
DESCRIPTION OF THE SYSTEM PROVIDED
BY THE SERVICE ORGANIZATION

OVERVIEW OF OPERATIONS

Company Background

Passport (or the “Company”) is a private company, headquartered in Charlotte, North Carolina. Passport offers a fully integrated cloud-based parking management and payment solution to its customers through the Internet and mobile application. The Passport mobile application provides the ability to pay for parking from a mobile phone. Payments are accepted through e-commerce via the Internet or mobile devices, including phone and text orders. The system also provides the ability for validation at checkout. The application also provides parking validation functionality allowing parking management companies to create custom parking validations, manage their funds, and monitor any activity. Parking management companies gain total control of all parking activity with real-time reporting and logs of each transaction.

Description of Services Provided

Passport offers a fully integrated cloud-based parking management and payment solution to its customers through the Internet and mobile application.

Business Role with Payment Cards

Passport receives card-not-present orders through their hosted online website and mobile ordering application. Customers “parkers” input payment card data at the time of account registration. Upon completion of the registration process, customers pay for their parking with the stored payment card data and are not required to submit new payment data each time they pay for parking. Passport provides a secure application payment interface for the customer registration process. Passport receives the payment information through the web or mobile interface.

Passport also provides text and interactive voice response (“IVR”) system interfaces as well. The pay via text process allows you to pay via texting the zone and space number to a phone number. This starts the parking booking process with credit card you have on file. The pay via voice process asks for zone number and space number and allows customer to change their credit card information via an IVR.

Passport uses service provided by Twilio, Amazon AWS, and Authorize.Net for the following services. Passport uses Twilio for IVR and SMS communication. Passport uses the services of Amazon AWS as a third party cloud computing provider that houses all Passport cardholder data and cloud computing space. Authorize.Net is a payment gateway service provider allowing merchants to accept credit card and electronic check payments through their Web site and over an IP (Internet Protocol) connection. This description does not include the control objectives and related controls of the Subservice Organizations.

Service Fee Implementation

Passport’s business customers utilize the online and mobile parking application to provide parking payment solutions to parkers. Business customers must set up an account with Passport to offer the online and mobile services for the parking locations owned by the business customers. As part of the account setup process, Passport completes an Implementation Checklist which includes details regarding the parking locations, spaces, times, and service fees. Service fees depend on the location, space, and time of the park. Rates can fluctuate to reflect current events, early park discounts, premium parking locations, standard rates, among other things. The Implementation Checklist is utilized to ensure the variables in the setup of the account, and the related service fees, are accurate. Confirmation of the accurate setup of new customer accounts, which includes the accurate service fee implementation, is received prior to customer account go-live. Access to make changes to the customer service fees is limited to authorized personnel within Passport. Business customers also have the ability to set up service fees after the initial account setup process.

Wallet Loading

Passport offers parkers the ability to purchase a wallet. A wallet allows the parker to pay a specific dollar amount which is credited to their wallet. Each time the parker purchases a space to park, the transaction amount for that space is deducted from the wallet. Notification of parker charges are communicated to the parker prior to the transaction processing. As part of the account setup process, Passport processes test transactions through the account. Test transactions are reviewed to ensure they are processed through the parker wallets accurately and timely. Test transactions are a step within the Implementation Checklist prior to the go-live date. Access to make changes to parker wallets is limited to authorized personnel within Passport.

Transaction Processing and Operator Reporting

Passport provides operator reports and transaction details of all parker activity to the business customers for their respective parking locations. Operator reports and the related transaction details are available to business customers on a real-time basis. Business customers can access their reports through their accounts with Passport. These reports are utilized by business customers to reconcile charges to their accounts and the funds posted to their bank accounts. Funds are posted to the business customer's bank accounts on a daily basis. During the account setup process, business customers are involved in reconciling test transactions. Errors in reporting, whether it is during the account setup process or during live processing of transactions, are communicated to Passport and researched and resolved by the Support team. Passport also monitors transaction processing on a daily basis. Errors are posted real time and are recorded on a log. The log is reviewed by members of the Support team on a daily basis. If errors have occurred, they are reviewed and resolved the same day.

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 the Organization's control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior is the product of Company'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:

- Organizational policy statements and codes of conduct are documented and communicate entity values and behavioral standards to personnel. The employee policy and procedures manual contains organizational policy statements and codes of conduct to which employees are required to adhere
- Policies and procedures require that employees sign an acknowledgment form indicating that 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. Credit checks are performed for back office employees as a component of the hiring process

Commitment to Competence

Company'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
- A training program has been developed to maintain the skill level of personnel in certain positions

Executive Participation

The Company's executives have the ultimate responsibility for overseeing the business policies of the service organization. The executive team, composed of internal business partners, meets to discuss matters pertinent to the Company's operations and to review financial results.

Management's Philosophy and Operating Style

Company'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
- Management meetings are held on a regular basis to discuss major initiatives and issues that impact the business as a whole. It is expected that management members are prepared to provide clear and concise updates

Organizational Structure and Assignment of Authority and Responsibility

The Company's organizational structure provides the framework within which activities for achieving objectives are planned, executed, controlled and monitored. The organizational structure described below details the departments of the service organization that provide Mobile Payment Services for its clients. The structure provides for an adequate segregation of duties as well as clearly defined areas of responsibility.

Department	Description
Information Technology	The Information Technology ("IT") Staff is responsible for activities associated with developing, maintaining and supporting critical data processing systems. The organizational structure of the Information Technology staff provides segregation of duties between client services, systems programming, application programming, computer operations, physical and logical security access and documentation
Operations	The Operations Staff is responsible for day-to-day collection activities, hiring, training, and quality assurance. The Operations Staff is also responsible for setting and sustaining client and the service organization's goals
Administrative	The Administrative Staff is responsible for receiving, identifying, posting and depositing all payments received each day in a timely and accurate manner. The Administrative Staff also documents all incoming correspondence. They also ensure that all required licensing is obtained and current

Human Resources Policies and Practices

Company'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, from the collectors who contact the individuals to the management team who ensures the service organization is operating at maximum efficiency.

Upon being hired, new employees are issued an employee packet documenting various procedural and administrative matters, which is then discussed during the new hire orientation program. Human Resources creates and ensures adherence to policies, which include but are not limited to Employment, Non-Disclosure, Employee Status, Timekeeping and Payroll, Work Conditions and Hours, Employee Conduct and Disciplinary Action, and Employee Benefit Programs. Employees sign off on policies which include but are not limited to Employee Conduct and Work Rules, Company Privacy Policy, and Collection Regulations and Rules of Conduct.

Management checks trustworthiness and reliability for all personnel prior to employment through pre-screening procedures. Standard pre-screening interviews and testing are conducted by the in-house recruiting department. Background investigations are performed by the recruiter through an FCRA-regulated vendor.

In addition, the Human Resources department administers the Information Security/Privacy Policies for all employees, which addresses the sensitivity of customer information and how the service organization safeguards this information. Employees are required to sign acknowledgement forms, which are kept in the Personnel files maintained by the Company.

Company Management follows a standard exit procedure for all personnel leaving employment or changing job roles or location. This procedure includes notifying the relevant management team, communicating official termination procedures, notifying the IT department to review all relevant access within the systems, returning all company property, including company books, materials, keys, ID badges, computers, cell phones, and any other company owned items.

RISK ASSESSMENT

Passport has placed into operation a risk assessment process to identify and manage risks that could affect the organization's ability to provide reliable transaction processing for user organizations. This process requires management to identify significant risks in their areas of responsibility and to implement appropriate measures to address those risks.

Risks that are considered during management's risk assessment activities include the following:

- Changes in operating environment
- New personnel
- New or revamped information systems
- Rapid growth
- New technology
- New accounting pronouncements

Management's recognition of risks that could affect the organization's ability to provide reliable transaction processing for its user organizations is generally implicit, rather than explicit. Management's involvement in the daily operations allows them to learn about risks through direct personal involvement with employees and outside parties, thus reducing the need for formalized and structured risk assessment processes.

CONTROL OBJECTIVE AND RELATED CONTROL ACTIVITIES

Integration with Risk Assessment

Along with assessing risks, Passport has identified and put into effect actions needed to address those risks. In order to address risks, control activities have been placed into operation to help ensure that the actions are carried out properly and efficiently. Control activities serve as mechanisms for managing the achievement of those objectives.

Selection and Development of Control Activities Specified by the Service Organization

Control activities are a part of the process by which Passport strives to achieve its business objectives. Passport has applied a risk management approach to the organization in order to select and develop control activities. After relevant risk have been identified and evaluated, controls are established, implemented, monitored, reviewed and improved when necessary to meet the overall objectives of the organization.

Passport's control objectives and related control activities are included in Section 4 (the "Testing Matrices") of this report to eliminate the redundancy that would result from listing the items in this section and repeating them in the Testing Matrices. Although the control objectives and related control activities are included in the Testing Matrices, they are, nevertheless, an integral part of Passport's description of the data center services system.

The description of the service auditor's tests of operating effectiveness and the results of those tests are also presented in the Testing Matrices, adjacent to the service organization's description of control activities. The description of the tests of operating effectiveness and the results of those tests are the responsibility of the service auditor and should be considered information provided by the service auditor.

MONITORING

Passport's management performs monitoring activities in order to continuously assess the quality of internal control over time. Monitoring activities are used to initiate corrective action through personnel meetings, client conference calls, and informal notifications. Monitoring activities are conducted on a continuous basis and necessary corrective actions are taken as required to correct deviations from company policy and procedures.

Management's direct involvement in key operations facilitates identifying significant variances from expectations regarding internal controls. Management immediately evaluates the specific facts and circumstances related to any suspected control breakdowns. 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.

INFORMATION AND COMMUNICATION SYSTEMS

Information Systems

Passport employs an internally developed application, which is hosted on web servers located in a secure demilitarized zone ("DMZ") separate from the internal network. Backend supporting MySQL databases are used to store transaction data and are located on a separate network segment behind a dedicated firewall in the cloud. The Organization utilizes Active Directory for their internal network.

People

Passport staff provides support for the above services in each of the following functional areas:

- Executive management - provides general oversight and strategic planning of operations
- Systems administrators - responsible for effective provisioning, installation/configuration, operation, and maintenance of systems hardware and software relevant to the system
- Systems engineers - serves customers by providing product and service information that includes resolving product and service issues

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 Passport policies and procedures that define how services should be delivered. These are located on the Company's internal shared drive and can be accessed by any Passport team member.

Physical Security and Computer Operation

Passport uses Amazon AWS as a third party cloud computing provider that houses all Passport cardholder data and cloud computing space.

Logical Access

Passport 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, Passport 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 Passport network using an Active Directory user ID and password. Passwords must conform to defined password standards and are enforced through parameter settings in the Active Directory. 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.

Upon hire, employees are assigned to a position in the HR management system. 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 the appropriate security team. 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 Chief Technology Officer (CTO). As part of this process, the CTO reviews access by privileged roles and requests modifications based on this review.

The terminated employees' access is disabled on a timely basis. This terminated employee list is used by the security help desk to delete employee access.

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.

Change Control

Passport 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. Quality assurance testing and User Acceptance Testing (UAT) results are documented and maintained with the associated change request. 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.

Data

Customer data is managed, processed, and stored in accordance with the relevant data protection and other regulations, with specific requirements formally established in customer contracts. Customer data is captured which is utilized by Passport in delivering its Cloud-based Parking Management system.

Significant Events and Conditions

Passport has implemented automated and manual procedures to capture and address significant event and conditions. In addition, detailed monitoring and risk assessment procedures are in place to provide management with detailed information that impacts the Cloud-based Parking Management system. Please see the procedures, monitoring, and risk assessment procedures described in the relevant sections of this report for further details.

Preparation and Delivery of Reports and Data

Passport utilizes the services and procedures described above to capture, prepare, and deliver reports and other information (described in the data section above) to user entities and other parties.

Communication Systems

Communication is an integral component of Passport'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 Passport, information is identified, captured, processed, and reported by various information systems, as well as through conversations with clients, vendors, regulators, and employees.

Upper management is involved with day-to-day operations and is able to provide personnel with an understanding of their individual roles and responsibilities pertaining to internal controls. This includes the extent to which personnel understand how their activities relate to the work of others and the means of reporting exceptions to a higher level within Passport. Management believes that open communication channels help ensure that exceptions are reported and acted on. For that reason, formal communication tools such as organizational charts, employee handbooks, training classes and job descriptions are in place at Passport. Management's communication activities are made electronically, verbally, and through the actions of management.

COMPLEMENTARY USER ENTITY CONTROLS

Passport'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 of the control objectives related to Passport's services to be solely achieved by Passport control procedures. Accordingly, user entities, in conjunction with the services should establish their own internal controls or procedures to complement those of Passport.

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the control objectives 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 maintaining authorized user access to the Passport application and periodically reviewing and updating these users.
2. User entities are responsible for removing user access to the Passport application when terminating an employee.
3. User entities are responsible for using strong password and access codes to access all systems, including, but not limited to the Passport application.
4. User entities are responsible for appropriate design and implementation of security architecture for equipment including firewalls: switch, and router configuration accessing the Passport application.
5. User entities are responsible for having authorized personnel available to report issues and resolve them with Passport personnel.
6. User entities are responsible for immediately notifying Passport of any actual or suspected information security breaches, including compromised user accounts.
7. User entities are responsible for developing their own disaster recovery and business continuity plans that address their inability to access or utilize Passports services.
8. User entities are responsible for reconciling daily transactions and operator reports back to funds deposited within their accounts.
9. User entities are responsible for the accurate setup of service fees after the initial setup of the account.
10. User entities are responsible for complying all laws and regulations with respect to security, availability, maintainability, and integrity.
11. User entities are responsible for understanding and complying with the terms of service and their contractual obligations to Passport.

SECTION 4

TESTING OF CONTROL OBJECTIVES AND RELATED CONTROL ACTIVITIES PROVIDED BY THE SERVICE AUDITOR

GUIDANCE REGARDING INFORMATION PROVIDED BY THE SERVICE AUDITOR

A-lign's examination of the controls of Passport was limited to the control objectives and related control activities specified by the management of Passport and did not encompass all aspects of Passport's operations or operations at user organizations. Our examination was performed in accordance with American Institute of Certified Public Accountants (AICPA) Statement on Standards for Attestation Engagements No. 16 (SSAE 16).

Our examination of the control activities were performed using the following testing methods:

TEST	DESCRIPTION
Inquiry	The service auditor made inquiries of service organization personnel. Inquiries were made to obtain information and representations from the client to determine that the client's knowledge of the control and corroborate policy or procedure information.
Observation	The service auditor observed application of the control activities by client personnel.
Inspection	The service auditor inspected among other items, source documents, reports, system configurations to determine performance of the specified control activity and in some instances the timeliness of the performance of control activities.
Re-performance	The service auditor independently executed procedures or controls that were originally performed by the service organization as part of the entity's internal control.

In determining whether a SSAE 16 report meets the user auditor's objectives, the user auditor should perform the following procedures:

- Understand the aspects of the service organization's controls that may affect the processing of the user organization's transactions;
- Understand the flow of significant transactions through the service organization;
- Determine whether the control objectives are relevant to the user organization's financial statement assertions;
- Determine whether the service organization's controls are suitably designed to prevent or detect processing errors that could result in material misstatements in the user organization's financial statements and determine whether they have been implemented.

CONTROL AREA 1 INFORMATION SECURITY

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that system information, once entered into the system, is protected from unauthorized or unintentional use, modification, addition or deletion.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
1.1	Formal information security policies and procedures are in place and communicated to all users with access to the systems.	<p>Inspected information security policies and procedures to determine that formal information security policies and procedures were in place.</p> <p>Inspected the training materials and training attendance form to determine that periodic education and training was provided to the users related to the company policies and procedures.</p> <p>Inspected completed Acknowledgement forms for a sample of new hired during the audit period to determine that formal information security policies and procedures were communicated to all the users with access to the systems.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p>
1.2	SSH access is executed via public key authentication, enabling the avoidance of using shared passwords and allows Passport to restrict access to only users with private keys.	<p>Inspected SSH access via public key authentication configuration to determine that individual authentication through passwords was enforced.</p> <p>Inspected the user directory to determine that authentication was restricted to authorized users.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>
1.3	Administrator access is restricted to authorized user accounts and in line with their job function.	<p>Inspected a list of administrators to determine that administrator access was restricted to authorized user accounts and in line with their job function.</p> <p>Inspected the authorized user list to determine that users had appropriate access to the database based on the job responsibilities.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>
1.4	Users are required to authenticate via a user account and password before being granted access to the system.	Observed the log-on process to determine that users were required to authenticate via a user account and password before being granted access to the system.	No exceptions noted.

CONTROL AREA 1 INFORMATION SECURITY

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that system information, once entered into the system, is protected from unauthorized or unintentional use, modification, addition or deletion.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
1.5	Access to system requires a documented approval by authorized parties specifying required privileges.	<p>Inspected the SSH key user authentication to determine that users were required to authenticate via a user account and password before being granted access to the system.</p> <p>Inquired of Brad Powers, Chief Technology Officer (CTO) regarding the utilization of the authorization form for user access to determine that access to system required a documented approval by authorized parties specifying required privileges.</p> <p>Inspected New Hire Policy within the Security Policy obtained from Brad Powers, Chief Technology Officer (CTO) to determine that utilization of an Authorization Form for User Access was required for all new hires prior to gaining access to the system.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p>
1.6	Access to the system is revoked as a component of the termination process.	<p>Inspected new hire authorization forms for a samples of new hires to determine that access to system required a documented approval by authorized parties specifying required privileges.</p> <p>Inquired of Brad Powers, Chief Technology Officer (CTO) regarding user access revocation to determine that access to the system was revoked as a component of the termination process.</p> <p>Inspected user access revocation policy and procedures within the information policy to determine that policy and procedures existed to revoke user's access as a component of the termination process.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>

CONTROL AREA 1 INFORMATION SECURITY

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that system information, once entered into the system, is protected from unauthorized or unintentional use, modification, addition or deletion.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
1.7	Anti-virus software is installed on production servers to detect and prevent the transmission of data or files that contain virus signatures recognized by the anti-virus software.	Inspected user access revocation confirmation for a sample of terminated employees to determine that access to the system was revoked as a component of the termination process.	No exceptions noted.
1.8	Procedures exist to identify, report, and act upon system confidentiality and security breaches and other incidents.	<p>Inspected anti-virus software configuration on a sample of production servers to determine that anti-virus software was installed on production servers to detect and prevent the transmission of data or files that contain virus signatures recognized by the anti-virus software.</p> <p>Inspected anti-virus update settings for a sample of production servers to determine that anti-virus software was up to date.</p> <p>Inquired of Brad Powers, Chief Technology Officer (CTO) regarding system confidentiality and security to determine that procedures existed to identify, report, and act upon system confidentiality and security breaches and other incidents.</p> <p>Inspected evidence of recurring daily security review calendar invitation to determine that procedures existed to identify, report, and act upon system confidentiality and security breaches and other incidents.</p> <p>Inspected evidence of a daily security review summary to determine that procedures exist to identify, report, and act upon system confidentiality and security breaches and other incidents.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p>

CONTROL AREA 1 INFORMATION SECURITY

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that system information, once entered into the system, is protected from unauthorized or unintentional use, modification, addition or deletion.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
1.9	System components and software are protected from known vulnerabilities through installation of the latest vendor-supplied security patches.	Inspected configuration of security monitoring software to determine that system components and software were protected from known vulnerabilities through installation of the latest vendor-supplied security patches.	No exceptions noted.
1.10	Firewalls are installed on the Passport Systems and applications. Management periodically reviews the firewall settings to ensure access is limited appropriately.	<p>Inspected firewall settings for a sample of servers to determine that firewalls were installed on the Passport Systems and applications.</p> <p>Inspected evidence of management's review of firewall settings to determine firewalls were installed on the Passport Systems and applications and that management reviewed the firewall settings to ensure access was limited appropriately.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>

CONTROL AREA 2 APPLICATION CHANGE CONTROL

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that unauthorized changes are not made to production application systems.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
2.1	Formal application change control policies and procedures are in place and communicated to all users with access to the systems.	<p>Inspected application change control policies and procedures to determine that formal application change control policies and procedures were in place.</p> <p>Inspected the training materials and training attendance form to determine that periodic education and training was provided to the users related to the application change control policies and procedures.</p> <p>Inspected completed Acknowledgement forms for a sample of new hired during the audit period to determine that formal application change control policies and procedures were in place and communicated to all users with access to the systems.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p>
2.2	A change management software is utilized to maintain and control infrastructure application changes, and the associated reporting and logging functions.	<p>Inquired the Chief Technology Officer (CTO) Brad Powers to determine that a change management software was utilized to maintain and control infrastructure and application logging changes, and the associated reporting and logging functions.</p> <p>Inspected a sample of change tickets to determine that a change management software was utilized to maintain and control infrastructure and application changes, and the associated reporting and logging functions.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>
2.3	Documented change request are reviewed and prioritized by management based on business needs and resource availability, and assigned to personnel for action.	Inquired Chief Technology Officer (CTO) Brad Powers to determine documented change requests were completed for infrastructure projects and reviewed and prioritized by management based on business needs and resource availability, and assigned to personnel for action.	No exceptions noted.

CONTROL AREA 2 APPLICATION CHANGE CONTROL

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that unauthorized changes are not made to production application systems.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected a sample of change tickets to determine documented change request was completed for infrastructure projects and reviewed and prioritized by management based on business needs and resource availability, and assigned to personnel for action.	No exceptions noted.
2.4	Development/test environments exist and are separate from the production environment.	Inspected evidence of the development and test environments to determine that development/test environments exist and were separate from the production environment.	No exceptions noted.
2.5	Application and other infrastructure changes are authorized, tested, and approved for implementation prior to actual implementation.	Inspected a sample of change tickets to determine that application and other infrastructure changes were authorized, tested, and approved for implementation prior to actual implementation.	No exceptions noted.
2.6	Access to implement changes to production environment is limited to authorized individuals.	Inspected list of users with access to promote changes to production to determine that access to promote changes to production was limited to appropriate personnel.	No exceptions noted.
2.7	Production changes are appropriately logged and monitored on a daily basis.	<p>Inquired of Chief Technology Officer (CTO) Brad Powers regarding the daily review of the system monitoring log to determine that changes promoted to production were appropriately logged and monitored.</p> <p>Inspected evidence of a daily review of the system monitoring log to determine that changes promoted to production were appropriately logged and monitored on a daily basis.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>

CONTROL AREA 3 SERVICE FEE IMPLEMENTATION

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that service fees are initially implemented accurately according to client instructions.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
3.1	Access to set up service fees are limited to authorized personnel.	<p>Inquired of Chief Technology Officer regarding the user access list with authorities to setup service fees to determine access was limited to authorized users, based on job responsibilities.</p> <p>Inspected user access list with authorities to determine that access to set up service fees were limited to authorized personnel, based on job responsibilities.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>
3.2	An Implementation Checklist is completed as part of the initial implementation of service fees for new customers.	<p>Inquired of Chief Technology Officer regarding the new customers' setup to determine the checklist was completed, including the accurate setup of service fees for new customers' setup.</p> <p>Inspected new customer implementation checklists for a sample of new customer's setup to determine the checklist was completed, including the accurate setup of service fees.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>
3.3	Customer sign-off of new customer setup, including accurate service fees implementation, is received prior to customer account go-live.	<p>Inquired of Chief Technology Officer regarding the new customers' setup to determine that customers reviewed and approved the account setup prior to the account go-live.</p> <p>Inspected customer sign-offs within the new customer implementation checklist for a sample of new customers' setup to determine that customers reviewed and approved the account setup prior to the account go-live.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>

CONTROL AREA 4 WALLETS LOADING

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that parker wallets are loaded accurately and timely.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
4.1	Parker wallets are automatically and accurately loaded to the system.	Inquired of Chief Technology Officer (CTO) regarding parker wallets to determine that parker wallets were automatically and accurately loaded to the system.	No exceptions noted.
		Inspected a sample of wallet loading transactions to determine that parker wallets were automatically and accurately loaded to the system.	No exceptions noted.
4.2	Notification of parker charges are communicated to the parker prior to the transaction processing.	Inspected system configuration from the production system to determine that the system was configured to notify charges to the parker prior to transaction processing.	No exceptions noted.
		Inspected a sample of parker charge notification obtained from Chief Technology Officer (CTO), to determine that notification of parker charges were communicated to the parker prior to transaction processing.	No exceptions noted.
		Inspected a sample of parker charge notifications to determine that notification of wallet updating was communicated to the parker prior to being charged.	No exceptions noted.
4.3	Access to make changes to parker wallets is limited to authorized personnel.	Inspected administrative accounts with authorities to make changes to parker wallets to determine that access to make changes to the parker wallets was limited to authorized personnel.	No exceptions noted.

CONTROL AREA 5 TRANSACTION PROCESSING

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that transactions are updated accurately in parker wallets.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
5.1	An implementation checklist is maintained for each new customer setup. As part of the customer setup, test transactions are processed to ensure customer wallets are loaded accurately. Customers confirm transactions have been processed in the wallet accurately.	<p>Inquired of Chief Technology Officer (CTO) regarding the new customer setup process to determine that an implementation checklist was maintained for each new customer setup. As part of the customer setup, test transactions were processed to ensure customer wallets were loaded accurately. Customers confirmed transactions had been processed in the wallet accurately.</p> <p>Inspected new customer implementation checklists for a sample of new customers' to determine the checklist was maintained for each new customer setup and that test transactions were processed to ensure customer wallets were loaded accurately. Customers confirmed transactions had been processed in the wallet accurately.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>
5.2	Errors in transaction processing are recorded real time. A review of any errors is performed on a daily basis by the Technology team. Errors are reviewed and resolved.	<p>Inspected a daily error log to determine that errors in transaction processing were reviewed and resolved throughout the day.</p> <p>Inspected a sample of error log/resolution tickets to determine that errors in transaction were recorded, reviewed and resolved timely.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>
5.3	Access to make changes to the parker wallets is limited to authorized personnel.	Inspected the user access listing for those users with authorities to make changes to parker wallets to determine that access to make changes to the parker wallets was limited to authorized personnel.	No exceptions noted.

CONTROL AREA 5 TRANSACTION PROCESSING

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that transactions are updated accurately in parker wallets.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
5.4	Parker wallets changes follow the Passport change management process.	<p>Inquired of the Chief Technology Officer (CTO) regarding the parker wallets changes to determine that parker wallets changes followed Passport change management process.</p> <p>Inspected a sample of parker wallets changes to determine that parker wallets changes followed Passport change management process.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>

CONTROL AREA 6 OPERATOR REPORTING

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that operator reports reflect parker activity and financial transactions.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
6.1	An implementation checklist is maintained for each new customer setup. Customers confirm operator reports reflect accurate parker activity and financial transactions.	<p>Inquired of Chief Technology Officer regarding the new customers' setup to determine that the checklist was maintained for customer setup and that report was confirmed by the customers to reflect the accurate parker activity and the financial transactions.</p> <p>Inspected the new customer implementation checklist for a sample of new customers to determine the checklist was maintained for each new customer setup and that it was part of the customer setup process.</p> <p>Inspected the implementation checklist for a sample of new customers' setup to determine that new customers confirmed operator reports reflected accurate parker activity and financial transactions.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p>
6.2	Errors in reporting are researched and resolved by the Passport Support team.	Inspected a sample of error log/resolution tickets to determine that errors in reporting were recorded, reviewed and resolved timely.	No exceptions noted.
6.3	Access to make changes to the operator reports is limited to appropriate personnel.	<p>Inquired of the Chief Technology Officer (CTO) regarding privileged users' access necessary to make changes to the operator reports to determine that access to make changes to the operator reports was limited to appropriate personnel.</p> <p>Inspected user access accounts with authorities to make changes to operator wallets to determine that access to make changes to the operator wallets was limited to authorized personnel.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>

CONTROL AREA 6 OPERATOR REPORTING

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that operator reports reflect parker activity and financial transactions.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
6.4	Operator reports changes follow the Passport change management process.	<p>Inquired of the Chief Technology Officer (CTO) regarding the operator reports changes to determine that operator reports changes followed the Passport change management process.</p> <p>Inspected a sample of operator reports changes to determine that operator reports changes followed the Passport change management process.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>