FlashParking

Bid Contact	**Julie Thiers** **julie.thiers@flashparking.com** **Ph 925-223-**7108	Address	**3801 South Capital of Texas Highway, Suite 250** **Austin, TX 78704**

Item #	Line Item	Notes	Unit Price	Qty/Unit	Attch.	Docs
PNC2119994R1--01-01	Parking Access and Revenue Control Equipment and Maintenance	**Supplier Product Code:**	**First Offer -**	1 / each	**Y**	**Y**

Supplier Total $0.00

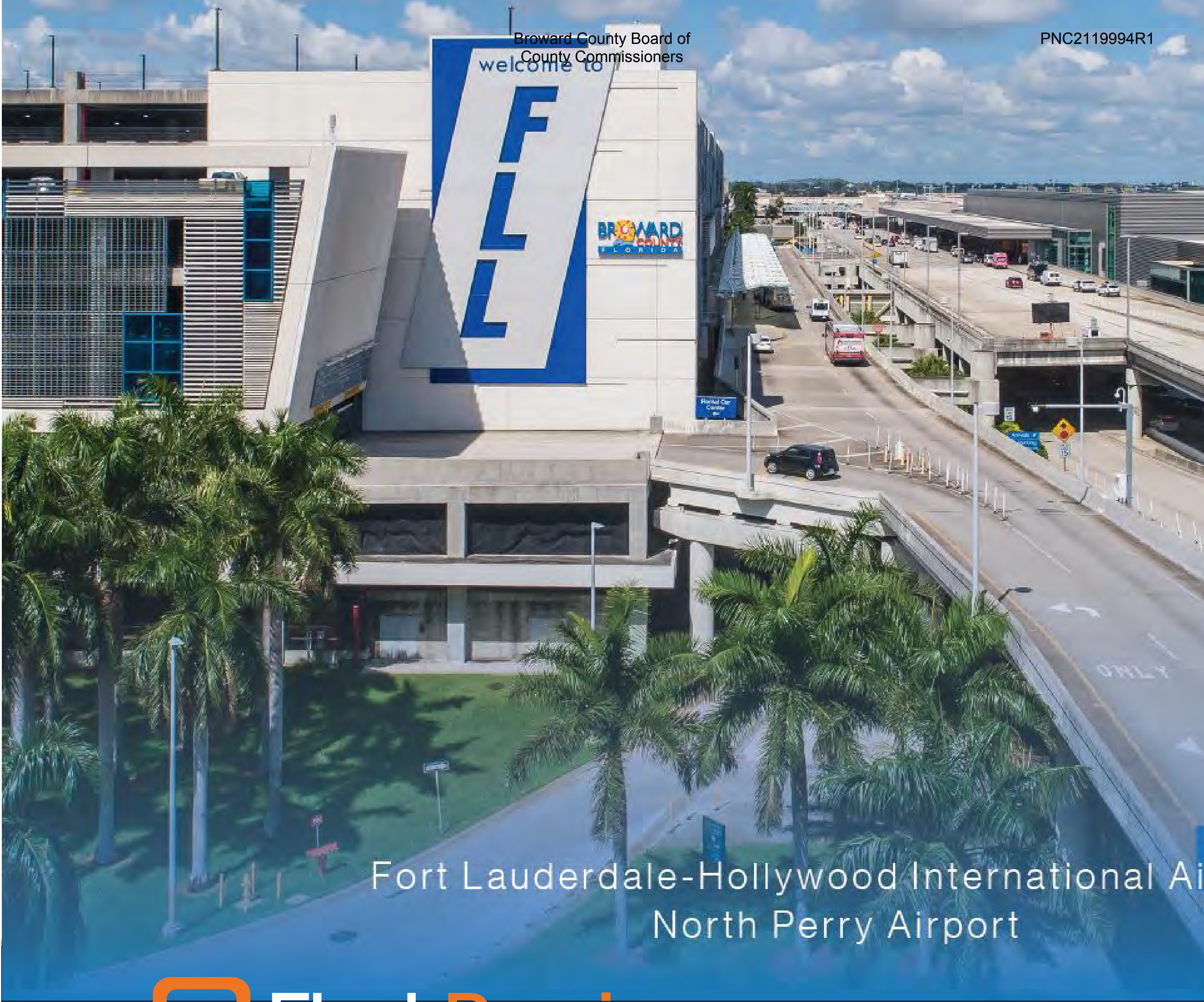
FlashParking

Item: **Parking Access and Revenue Control Equipment and Maintenance**

Attachments

FlashParking-Financials for PNC2119994R1.pdf

FlashParking- RFP Response Ft Lauderdale PNC2119994R1.pdf



FlashPar ing

PNC2119994R1 - Parking Access and Revenue Control Equipment and Maintenance

Fort Lauderdale-Hollywood International Airport

Future-Ready Together

HEADQUARTERS
FlashParking
3801 S. Capital of Texas Highway, Suite 250
Austin, TX 78704

SALES
sales@flashparking.com
800.213.3706

TABLE OF CONTENTS

SECTION I – FLASHPARKING INTRODUCTION/OVERVIEW

SECTION II – METHODOLOGY, PROJECT UNDERSTANDING AND PROPOSED APPROACH

SECTION III – PRICING

SECTION IV – REQUESTED DOCUMENTS & ADDITIONAL INFORMATION

March 5, 2020
Michal Durden & Mark Roberts
Broward County Board of County Commissioners

Subject: FlashParking response to the RFP for PNC2119994R1 Ft. Lauderdale Airport

Dear Mr. Durden & Mr. Roberts,

Thank you for providing FlashParking, Inc. with an opportunity to submit a response to your Request for PARCS at the Ft Lauderdale Airport. As a technology company, it is exciting to see how our advanced parking system would provide Broward County with a future-proof, state of the art PARCS.

When FlashParking was launched in 2011, our founders knew one thing for sure: the world was changing rapidly. So, we built a platform with **reliability** and **adaptability** in mind that featured:

- **Cloud-based** functionality for total reliability, security, and agility
- **Mobile-first** management to meet modern business needs
- **Frictionless access** via Bluetooth, LPR and AVI technology for transients and employees
- **Secure transactional environment**, PCI DSS Level 1 Service Provider
- **Future-ready**, extensible software that supports remote configuration and over-the-air updates
- **Simplified USB-based hardware** comprised of off-the-shelf components for minimum downtime, reduced costs, and easy maintenance

This technology approach has allowed us to **create an operating system** that sits at the **intersection of enhanced 21st century parking, a robust business intelligence engine, and ecosystem of value-driven mobility service partners. Together, these core competencies will allow you to optimize everyday operations, implement dynamic processes, and develop a long-term strategy for thriving in an age of evolving mobility practices.**

Serving over 2,500 locations across the U.S. in a variety of different venues, FlashParking has the experience and the know how to successfully deploy customized solutions for customers. For operations that demand PARCS, valet, events or a combination of the three, we can deliver a comprehensive system that meets requirements and exceeds expectations.

With FlashParking, asset owners and operators can configure a solution that supports the venue's current and future needs with functionalities like:

Current

- Local vendor support or the ability to self-maintain

- Multiple validation options (print, electronic, text, stand-alone kiosk, printer chase tickets) and reporting to bill departments
- Multiple access options including LPR, AVI, Bluetooth, controlled code, validations, RFID and more.
- Barcode reader for reading tickets, validations, and other barcodes

Future Needs

- Dynamic yield management
- Logistics and delivery access points
- Value-added services such as EV charging, cleaning, and servicing
- Integrations with transportation network companies and micromobility technologies.
- Modern mobility services like autonomous vehicle access and eParking reservations

FlashParking was born in the cloud, which means that we have the most experience in the industry working in a true cloud environment. *We do not push data to an on-site server that is connected to the cloud*. Our equipment connects directly to the cloud via an Ethernet line, which means validations, rate pushes, on-line management, payments and reporting are done in real time.
Please call the references we listed, and we would be happy to provide more. Whatever the venue, FlashParking continues to provide world class parking solutions to industry leaders across the United States and we look forward to hearing from you about being your partner.

Again, thank you for your consideration.

Jim DuFon
FlashParking
VP Government Projects
Cell (512) 547-9998
james.dufon@flashparking.com

SECTION I
FLASHPARKING INTRODUCTION/OVERVIEW

FlashParking

PROPOSAL CONTACT INFO

FlashParking

Headquarters

3801 South Capital of Texas Highway, Suite 250 Austin, TX 78704

Main Line

512.402.8960

Sales

sales@flashparking.com

800.213.3706

Support

support@flashparking.com

888.737.7465

Authorized Representative to bind the Offer

Sam Goodner

Chief Strategy Officer

sam.goodner@flashparking.com

Authorized Representative to negotiate on behalf of the Offer

Jim DuFon

VP Government Projects

james.dufon@flashparking.com

BACKGROUND, EXPERIENCE, AND PERSONNEL

Background

Since being launched in 2011, FlashParking has strategically architected a series of solutions that deliver everything from perfect parking at the site and enterprise-levels to connected mobility hubs that meet the needs of modern smart cities.

Our straightforward business strategy starts with listening to our clients, understanding their pain points with legacy infrastructure, and ultimately designing solutions with future-ready technologies that position your operation for success in the mobility ecosystem of today and tomorrow.

We have since installed over 3,000 kiosks and work with most industry leading partners such as the Banner Health, Texas Health Presbyterian Hospital and the Texas Medical Center. In fact, we provide PARCS and/or valet services to over 50 hospitals. We add 25-30 valet and 25-35 PARCS locations per month.

FlashParking's primary solutions supporting our site, enterprise, and smart city solutions are:

FlashValet: Valet and Event Parking Solution

Our inaugural offering, FlashValet is currently servicing thousands of locations across the vertical landscape. Parking operators and asset owners saw such immediate value in our cloud-born platform—which allows for real-time revenue and pricing decisions while delivering a true mobile customer experience—that they demanded we build out innovative solutions for garages and parking lots as well.

FlashPARCS: Parking Access and Revenue Control Solution

FlashPARCS is now running over a 3,000 kiosks and is the solution of choice for industry leaders such as the Texas Medical Center (200 lanes installed in 44 days), City of Las Vegas (running Bluetooth for transients and monthlies), T.F. Green Airport (Providence, RI), Bayside Marketplace, American Airlines Arena, and the Port of Miami to name a few.

Today FlashParking is delivering at enterprise scale counts of 5M+ parkers per month (100K+ w/ our FlashBeacon Bluetooth technology) and is processing over $1B across 3000+ locations.

Our rapid growth stems from our future-ready philosophy that's rooted in three competitive differentiators:

Future-ready Infrastructure

With equipment manufactured and assembled in our production facility in the U.S. and a direct sales and installation model, we control the end-to-end process; thus, creating efficiencies in sales, onboarding, installation, and deployment training.

Unrivaled Cloud Inteligence

Our industry-leading cloud-born software platform and architecture deliver real-time business intelligence with a 360-degree view of operations that provides unrivaled business intelligence for organizations of all sizes and industry spectrums.

World-Class Customer Experience

In an increasingly mobile world, the FlashParking platform delivers comprehensive, innovative, user-friendly technologies like text for retrieval, ticketless parking, mobile payments, frictionless Bluetooth access, loyalty management, and eParking functionality that deliver a world-class customer experience.

The result is FlashParking delivers a smart ecosystem of solutions, products, and seamless integrations that work together to streamline operations for operators, drive revenue for asset owners, as well as improve mobility and enhance the guest experience.

Experience

The following project team has collectively managed, installed and commissioned over 10,000 installations in industries like parking, petroleum, and energy. Each bring a unique and influential perspective to establish a development, installation, implementation and client services plan designed to consider every phase of the project.

Our Implementation Team installs 25-35 new PARCS locations and adds 25-30 new valet locations every month. Utilizing a highly experienced team, being dedicated to customer service, and offering superior products and

software enables us to continue scale without jeopardizing our customer's satisfaction.

Executive Team

Dan Sharplin
Chairman & CEO

A lead investor and FlashParking's Chairman & CEO. Dan is a serial entrepreneur, who founded and led SiteControls, a clean tech startup from concept to industry leadership in the smart grid and energy efficiency space. Managed through to a successful exit via a sale of the Company to Siemens.

Juan Rodriguez
Vice Chairman & Chief Product Officer /Co-Founder

Juan Rodriguez directs the planning, management of product development, and overall strategy of the company.

Sam Goodner

Chief Strategy Officer & Founder/Former CEO of Catapult Systems

A lead investor and FlashParking's Chief Strategy Officer, Sam Goodner is a serial entrepreneur, angel investor, and business coach. Sam is also the founder and former CEO of Catapult Systems, a Microsoft-focused information technology consulting firm, which he sold to a public company in 2014.

Sales/Solutions Engineering

Jim DuFon

VP Government Projects

Jim is an experienced Sales Executive in the Parking Industry. Over the past 9 years at Parkeon and then at FlashParking, he has overseen the sale and installation of over 2,500 kiosks in cities such as Miami, Washington D.C., Austin and Las Vegas.

Jeffrey Johnson

Vice President of Enterprise Projects

Jeff joins FlashParking from Towne Park, where he served on their executive team and rose to the role of Senior Vice President, Operations, Western Group. He was responsible for leading all field operations for the Western United States. He also focused on providing a path for employee enrichment and development and led the client development roadmap. Before joining Towne Park, Jeff was a Director of Rooms Division for Four Seasons Hotels and Resorts. During his 15 years in the hospitality industry, he worked in several executive level leadership roles where he oversaw departments including Guest Services, Housekeeping, and Front Office.

Damon Kessler

Vice President of Stategic Projects

Damon is a 20-year veteran in the parking industry as an Operator, PARCS distributer, and PARCS manufacturer. For the first seven years of his career, Damon oversaw operations and marketing for ABM's Washington market. Drawn to the technology side of the business, Damon moved to the PARC side of the business by joining Protection Technologies (PTI) as a partner. Damon spent ten years overseeing all aspects of the business that provided PARCS solutions for nine Western states. In 2016, Damon led the successful acquisition of PTI by SKIDATA where he remained until 2018. Joining the FlashParking team in early 2019, Damon oversees the sales process for complex and strategic projects. With hundreds of PARCS installations under his supervision, following are just a few marquee projects Damon oversaw: City Creek Center, Cherry Creek Mall, Spokane Airport, Saskatoon Airport, Winnipeg Airport, Edmonton Airport, Washington Convention Center to name a few.

Wade Bettisworth
Vice President of Government & Municipalities

Over the past 23 years, Wade has been entrusted to provide parking and transportation solutions to municipalities, colleges and universities as well as private parking operators. During this time, he has assisted numerous public and private entities in improving the efficiencies of their parking operations. Wade's experience includes consultative customer interface while at T2 Systems, Redflex Traffic Systems and Genetec/AutoVu. During his nine-year tenure with Schlumberger/Parkeon (now known as Flowbird), Wade was instrumental in introducing parking pay stations for on-street use in numerous cities, including Seattle, Portland, Galveston and Park City. Wade joined FlashParking following a successful career at Amano McGann. His successes at Amano McGann include leading the effort to deliver a multi-million-dollar, state of the art parking control system to a consortium led by the city of Sacramento.

Liz Young
Vice President of Strategic Solutions

Liz began her career in PARCS in 1996 and has scaled the ranks from training customers to ultimately managing over 3,000 lanes of equipment. Her extensive involvement working closely with Operators, Manufacturers, Vendors and Customers provides an exclusive insight on the installation process. Her astute understanding of how a downed facility affects the opera on and experience for the end user makes her a customer proponent that will push internally to assure a successful project.

Implementation & Installation

Casey Ackman
Director of Implementation

For the last 15 years Casey has honed his skills on implementing new projects. Having implemented over 8,000 sites including: Michaels (1,100 sites), LA Fitness (500 sites), Big Lots (1,200 sites), 24 Hour Fitness (300 sites) and Tuesday Morning (500 sites), Casey is able to identify risk factors before they are present to prevent disruption to the project timeline. His professionalism and approach to the implementation of a project ensures a well-developed and accurate implementation plan.

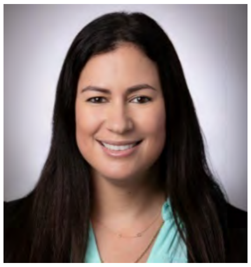
Christine Powers
Onboarding Manager

Christine has managed software onboarding and strategic operation projects for over 15 years. With this experience, the onboarding team is poised to provide a first-class onboarding experience. Christine will be the first point of contact for software configuration and oversee all onboarding projects alongside the onboarding team to ensure FlashParking solutions are set up and ready to go prior to installation.

Matt Braddock
Install Manager

Matt has managed and installed over 150 lanes of equipment for FlashParking, in addition to Pay on Foot Devices, LPR and AVI solutions. Matt is responsible to consult, select and manage sub-contractors across the country to meet his timelines and milestones. He will oversee the on-site crew to ensure a successful completion of the project. Using his degree in Physics, Matt can find out of the box solutions for complex challenges that arise, while onsite. Matt will be on the ground day to day throughout the installation and will be the first point of contact.

Client Services



Dannika FiFi
Vice President of Client Services

Dannika is responsible for managing the customer experience post installation and serves as a trusted advisor with focus on maximizing product benefits and value. Dannika previously served as Senior Support Manager at Q2ebanking, where she was responsible for creating and leading Premier Support for mega tier financial institutions. Prior to her FinTech experience, she served as the Premier Services Manager for the energy management branch of Siemens BT. Dannika holds a master's degree in Technical Communication from Texas State University and a bachelor's degree in Business Management from Sam Houston State University.

Allison Noblitt
Training Manager

Allison began with FlashParking in 2012, after having been a managing editor for a local Tech magazine. Her proficiency for attention to detail and granular understanding of how things come together made her a natural for training on the Flash systems. Since, Allison has earned the esteem of her customers who recognize the extent of her knowledge. She will be a recurring presence onsite for ongoing training. Knowing how to best utilize the system is key to success, therefore training will be emphasized and repeated as necessary for everyone's success.

John Durham

Support Manager

John has managed support teams of up to 30 agents and has a keen understanding for the impact of quick resolution and clear communication. With his extensive experience and support, our installation team knows that they are in good hands and will receive speedy responses to ensure a timely installation. John will participate in Project calls to safeguard the installation process and keep the Support Team in the know of every phase, to be able to assist when needed

Vendor Reference Verification Form

Broward County Solicitation No. and Title:

Solicitation PNC2119994R1 Parking Access and Control Equipment

Reference for: FlashParking, Inc.

Organization/Firm Name providing reference:

The City of Las Vegas

Contact Name: Brandy Stanley Title Parking Services Mgr Reference date:

Contact Email: bstanley@lasvegasnevada.gov Contact Phone: 702-229-6863

Name of Referenced Project: Parking Access & Revenue Control equipment

Contract No. 180323-GL Date Services Provided: 10/1/18 to 9/30/23 Project Amount: 1.7 million

Vendor's role in Project: ☒ Prime Vendor ☐ Subconsultant/Subcontractor

Would you use this vendor again? ☒ Yes ☐ No If No, please specify in Additional Comments (below).

Description of services provided by Vendor:

Installation, Commissioning and ongoing service for 5 parking garage systems

Please rate your experience with the referenced Vendor:	**Needs Improvement**	**Satisfactory**	**Excellent**	**Not Applicable**
1. Vendor's Quality of Service				
a. Responsive	☐	☒	☐	☐
b. Accuracy	☐	☐	☒	☐
c. Deliverables	☐	☐	☒	☐
2. Vendor's Organization:				
a. Staff expertise	☐	☒	☐	☐
b. Professionalism	☐	☐	☒	☐
c. Turnover	☐	☐	☒	☐
3. Timeliness of:				
a. Project	☐	☐	☒	☐
b. Deliverables	☐	☐	☒	☐
4. Project completed within budget	☐	☐	☒	☐
5. Cooperation with:				
a. Your Firm	☐	☐	☒	☐
b. Subcontractor(s)/Subconsultant(s)	☐	☐	☐	☒
c. Regulatory Agency(ies)	☐	☐	☐	☒

Additional Comments: (provide on additional sheet if needed) ***ADDITIONAL REFERENCES AVAILABLE UPON REQUEST.**

THIS SECTION FOR COUNTY USE ONLY

Verified via: ____EMAIL ____VERBAL Verified by: ______________________________ Division: ______________ Date: ____________

All information provided to Broward County is subject to verification. Vendor acknowledges that inaccurate, untruthful, or incorrect statements made in support of this response may be used by the County as a basis for rejection, rescission of the award, or termination of the contract and may also serve as the basis for debarment of Vendor pursuant to Section 21.119 of the Broward County Procurement Code.

SECTION II

METHODOLOGY, PROJECT UNDERSTANDING AND PROPOSED APPROACH

FlashParking

OVERVIEW OF STRATEGIC SOLUTIONS FOR SITE LEVEL, ENTERPRISE, AND SMART CITIES

FlashParking's cloud-based platform has made it possible to strategically architect solutions to deliver everything from perfect parking at the site-level all the way up to connected mobility hubs for Smart Cities.

STRATEGIC SOLUTIONS

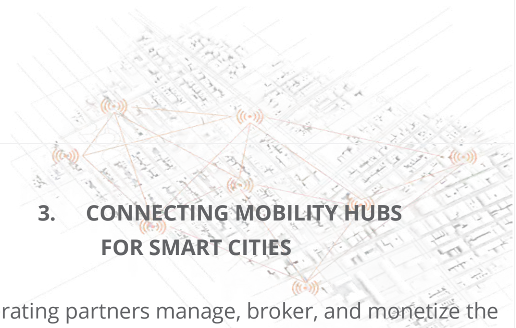
1. PERFECTING THE PARKING EXPERIENCE AT THE SITE LEVEL

Flashparking's industry-leading, future-ready infrastructure has perfected the parking experience at the site level (garages, surface lots, valet stands).

2. DELIVERING EXCELLENCE ACROSS YOUR ENNTERPRISE PORTFOLIO

While competitors retrofit outdated solutions, FlashParking's "cloud-first" approach is delivering cost-efficiencies, easy upkeep, redundancies, and scalability for enterprise operations, from portfolio-wide down to the site-level.

Our cloud-based systems deliver unprecedented business intelligence that maximizes asset value and enables urban mobility.



3. CONNECTING MOBILITY HUBS FOR SMART CITIES

As our operating partners manage, broker, and monetize the evolution of traditional parking assets (garages and lots), our technology layer is the only solution that can enable new transactions via a secure, real-time engine, with frictionless movement of all vehicle types.

At scale, with the right demand-side data via consumer app integrations, FlashParking's connected MobilityHub represents a practical solution to urban congestion, facilitating an efficient mobility ecosystem.

CORE DIFFERENTIATORS

These 3 Differentiators Drive All Our Solutions...

Future-ready Infrastructure

Unrivaled Cloud Intelligence & Security

World-Class Customer Experience

RESULTS & IMPACT

4.2 BILLION
Transactions Processed

100+ MILLION
Vehicles Parked

5.1 MILLION
Parkers per Month on Average

$1+ BILLION
Processed Annually

3,000+
Customer Locations

"We chose Flashparking and LAZ Parking to not only help us modernize our facilities and delivera best-in-class parking experience for our patients, visitors, and employees but also to help TMC better respond to the evolving mobility ecosystem."
--Shawn W. Cloonan, COO, TMC

44 days
200-lane PARCS installation at Texas Medical Center—the world's largest medical complex—in just 44 days!

30,000
Parking Spaces

39
Garages & Surface Lots

10 million
People Served Annually

61%
Drop in Support Calls

"As a business who has the ability to influence urban mobility significantly, it was imperative for us to work with a technology partner that could help us innovate to solve the growing congestion issues facing urban populations. Partnering with FlashParking will allow cities, like our hometown of Philadelphia, to benefit from the real-time data and business intelligence that can help win the war on congestion."
--Robert Zuritsky, CEO of Parkway Corporation

1. PERFECTING PARKING AT THE SITE LEVEL

FlashParking's industry-leading parking technology platform has perfected the parking experience at the site level for garages, surface lots, and/or valet stands. Our three competitive differentiators—future-ready infrastructure, unrivaled intelligence and security, and world-class customer experiences—deliver unique features and benefits that position FlashParking as the best platform for your needs today and into the future.

FEATURES	BENEFITS	VALUES (CORE DIFFERENTIATORS)
Plug-and-play, USB-Based System (PARCS)	□ Upgrade components individually as new technology emerges → gain new capabilities without replacing the entire machine □ Easy to perform DIY maintenance and replace components as needed → minimal downtime and no maintenance technician required	 **FUTURE-READY INFRASTRUCTURE** A forward-looking philosophy that reduces the long-term costs of updating with new technologies, upgrading as needs change, and driving innovation and industry leadership
Built for the cloud platform	□ Ability to scale operations up or down as needs change □ No on-site software programming required – kiosks are ready to use upon arrival □ Can mirror programming on any new kiosk □ Can adjust software configuration across system of kiosks □ Remote software updates performed automatically for zero downtime	
Direct business model	□ Unmatched installation times □ Direct sales □ Customization capabilities □ Collapsed supply chain allows for customer feedback to influence product development	
Data analytics	□ Price dynamically based on supply and demand □ Data-based decision making and strategy □ Drive revenues □ Maximizes asset value	 **UNRIVALED CLOUD INTELLIGENCE & SECURITY** Powerful business intelligence offers deep, broad ecosystem visibility that powers operational efficiency
Cloud-based software	□ Anytime, anywhere access □ Unified platform across portfolio □ System-wide visibility	
PCI DSS Level 1 Service Provider	□ Ability to process over 300,000 credit card transactions each year safely and securely □ Reduced risk of a credit card data breach □ FlashParking assumes 99% of the responsibility in maintaining compliance	
Open API software	□ Ability to interface with consumer-facing apps □ Integrations with third-party products platforms, and services	
PARCS and valet on one platform	□ Seamless user experience □ Maximized space utilization □ Increased visibility reduces revenue leakage	
Software development kit	□ Empowers partners to connect FlashParking programs to existing or new apps	

Cutting-edge user-facing technology	□ Deliver innovative features today that will become expectations tomorrow (i.e. mobile payments, Bluetooth access) □ Intuitive user interface for easy-of-use □ Constantly exceeding expectations □ Increased customer loyalty	**WORLD-CLASS CUSTOMER EXPERIENCE** Deliver benefits of innovative technologies to delight users, drive loyalty, and stay ahead of competitors

2. DELIVERING EXCELLENCE ACROSS AN ENTERPRISE PORTAFOLIO

Threats of Enterprise Organizations

The current model of managing an entire asset portfolio of parking assets with multiple parking technology systems poses many threats to large enterprise organizations including:

1) Disparate, Non-cloud-based parking systems
2) No Real-time Visibility and Reporting
3) Exorbitant Compliance and Hardware Costs
4) Rigid, Antiquated Technology
5) A Rapidly Evolving Ecosystem.

All these threats dissipate when you unify your enterprise portfolio under a unified parking technology system.

The Industry's Only Cloud-based Platform Delivers Enterprise Excellence

However, enterprise portfolios cannot operate on legacy infrastructure. On-premise servers, time-consuming maintenance, and unreliable hardware leaves parking assets isolated and costly. While competitors retrofit outdated solutions, FlashParking's "cloud-first" platform is delivering cost-efficiencies, easy upkeep, redundancies, and unlimited scalability for large enterprises and smart cities. Our competitive differentiators allow us to deliver enterprise excellence via our:

Future-ready Infrastructure

□ Extensible hardware
□ Self-service USB-based components
□ No special technician preventative maintenance requirements
□ Networked mobility hubs – built for the cloud. Not hosted in the cloud.
□ Standard open API framework allows for ease of integrations

Unrivaled Cloud Intelligence & Security

□ Managed PCI compliance – The parking provider outsources 98% of the PCI duties to the Level 1 Service provider.
□ Unified software package (surface/garage/valet on one platform)
□ Business intelligence with a 360-degree view of entire enterprise portfolios from single to multi-site view
□ Yield management engine
□ Mobile-first allows customers to manage entire operations from the palm of their hands

World-Class Customer Experiences

□ Frictionless access via proprietary, patent-pending Bluetooth beacon technology

- An iOS and Android Software Development Kit allowing operations to embed frictionless access in consumer facing applications

3. CONNECTING MOBILITY HUBS FOR SMART CITIES

The Mobility Challenge

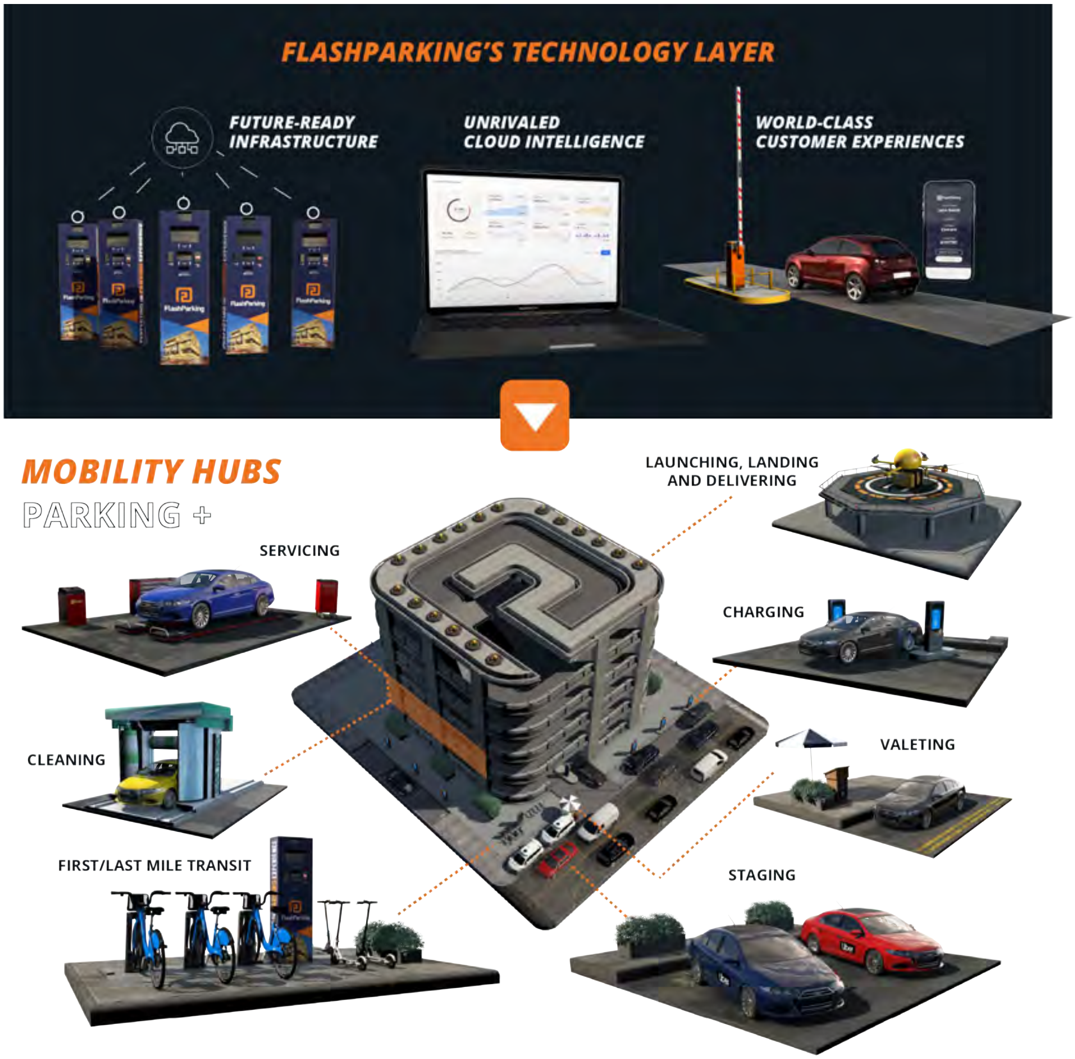
It is the threat presented by increasing urbanization, increasing vehicle miles traveled, and congestion within deteriorating infrastructures causing emissions and clutter to rise, productivity to drop, and public health concerns and costs to society as result. It is a challenge facing individuals, communities, and businesses like you.

The Solution

As the mobility ecosystem evolves to accommodate new market entrants like Transportation Network Companies (TNCs), eScooters, eBikes, UAV (drone) deliveries, electric vehicles, and self-driving cars, traditional parking assets will need to preemptively act to maintain their relevance. By networking traditional parking assets into the mobility ecosystem to serve a broader set of needs, operators and asset owners will be able to stake a sustainable position within the mobility ecosystem and establish mutually-beneficial business relationships—all while supporting societal welfare.

Turning Isolated Parking Assets into Connected Mobility Hubs

FlashParking's platform delivers the mobility infrastructure our cities need to turn parking garages turn into connected mobility hubs that can support all these flashy mobility technologies. With the mobility infrastructure in place, asset owners and operators can manage these connected mobility hubs, actually offer scooters and autonomous vehicles a place to live, and ultimately have that real impact on congestion and emissions.


FLASHPARKING'S TECHNOLOGY LAYER
FUTURE-READY INFRASTRUCTURE
UNRIVALED CLOUD INTELLIGENCE
WORLD-CLASS CUSTOMER EXPERIENCES
MOBILITY HUBS
PARKING +
SERVICING
CLEANING
FIRST/LAST MILE TRANSIT
LAUNCHING, LANDING AND DELIVERING
CHARGING
VALETING
STAGING

FlashParking

The total simple
approach to
parking

Executive Summary

After reviewing the RFP, we believe that FlashParking would be an ideal partner for Broward County at the Fort Lauderdale airport. FlashParking installs 15-20 new systems each month, mainly replacing antiquated systems. Our cloud-based system enables FlashParking to provide software updates, rate changes, real time reporting and maintain PCI compliance remotely.

FlashPARCS can be installed with minimal disruption to your current operations. FlashParking can install the new system at the facility within two weeks. FlashParking staff would remain on-site for 5 days after installation to confirm the system is fully functional and to answer any additional questions that may arise. The installation can be started within 6-7 weeks of receiving a signed agreement and Purchase Order. We have completed complicated installations at locations such as the Texas Medical Center and TF Green airport without disrupting the operation. Additionally, our quote includes replacing the existing LPR, AVI and gate equipment. With that said, we would be open to inspect the existing equipment and only replace what we cannot reuse, thus saving the County money.

While FlashParking does not have a local office, our partner, Burroughs Inc. has four offices within the Ft Lauderdale/Miami area where Flash factory trained technicians would reside at. FlashParking will also actively pursue local businesses to assist with the installation of all equipment with the goal of achieving the 21% CBE requirement.

We understand that there are other PARCS providers but based on the requirements in the RFP, not only will our PARCS equipment satisfy your current requirements, we future proof your investment via our ongoing Research and Development. You can have the assurance that your PARCS solution will solve your parking needs for years.

Thank you for the opportunity to submit this proposal and please do not hesitate to ask if you have any additional questions or need us to clarify any component.

PROPOSED SOLUTION: FLASHPARCS

Overview

FlashParking offers the most advanced cloud-based PARCS solution for any venue type and size. From overnight hotel parking and monthly parking in office buildings to complex mixed-use developments that offer robust validations and event parking, FlashPARCS allows you to manage and maximize your operation from a desktop, tablet, or mobile phone.

With FlashPARCS you can expect:

- A single platform that offers 360-degree, holistic view of operations across an entire asset portfolio down to the individual site-level.
- Real-time, cloud-based intelligence to help deliver a superior, mobile-first customer experience.
- A robust electronic validation system that offers six different methods of validating
- The ability to change rates and other key operational tasks from your mobile phone in real-time.
- Over 160 standard reports are available in the administrative portal with on-demand and scheduled reporting capabilities; our open API architecture can push data directly to Business Intelligence dashboards for ease-of-use and powerful analytics.
- Open API framework that offers seamless integrations with a variety of third-party applications, including: Hotel PMS systems, eParking Reservation systems, and more.
- Streamlined implementation and installation process managed by our own Installation team from end to end.
- Entry/Exit Smart Station is highly customizable. Whether it will be used to manage transients or monthlies, the software package is configured before shipment.
- All peripherals on the Smart Station are part of a plug-and-play (USB-based) system and can be swapped out in the existing machine as new technology emerges.
- A FlashCare Maintenance Kit contains replacements for major components so operators can quickly replace parts in a matter of minutes with minimal downtime

Highly Configurable to Meet Your Needs

Managing access and revenue can be a complex endeavor when you're handling multiple parker types and configuration needs. That is why we have an extensive list of additional features and functionalities available as configurable add-ons to ensure your PARCS solution meets your requirements and provides the services that matter to your parkers.

Display:

- **Multi-lingual module:** Smart Stations can be configured with multiple language options.
- **Display current rate on entry kiosk:** Display parking rates on entry kiosk
- **Digital rate display via monitor:** Display parking rates on digital display
- **Digital operations queue monitor:** Display equipment notification

Access & Revenue:

- **Access and Revenue Control:** Software allows for complex calculated rates, late fees, lost tickets, eValidations, and eParking Access.

- **Ticketless access via credit card and mobile number:** Instead of a paper ticket, transients can use a credit card or mobile number as their ticket.
- **Interactive Voice Recognition (IVR) System for Monthly Parkers:** Registered parkers can gain entry and exit in a parking facility by calling from their registered mobile phone, reducing call for help volumes.
- **Third-party access control module (AVI, LPR and others):** FlashParking offers integrations with a wide range of products; this module enables ongoing support for API integrations.
- **FlashParking mobile app module (BLE):** Our mobile app provides access control for monthly parkers via Bluetooth access.

Payment:

- **Credit card (with EMV chip payment option):** EMV chips or Magstripes can be accepted by a secure credit card reader.
- **Cash acceptance module (BNR and Exact Change Only):** This module offers the ability for our Smart Stations to accept cash bills; there are two cash acceptance options: Bill Note Recycler machine or an Exact Change Only machine.
- **Handheld Mobile Cashier:** An ideal feature for events, payments processed by a mobile device will allow guests to pre-pay upon entry or post-pay at the exit.
- **Validations:** Secure access for customers, clients, and merchants to validate electronic or printed validations from any browser, or via Mobile App or via Text – for unlimited users and departments.
- **Pay-on-Foot/Vehicle Retrieval Kiosk:** Provide your guests with the ability to pay in advance as well as request their car from a standalone unit.

Management:

- **Online monthly parker module:** This module allows for auto online enrollment, auto-billing/invoicing, and credit card payment.
- **Validations (printed or electronic):** Secure access for customers, clients, and merchants to validate electronic or printed validations from any browser, or via mobile app or via text — for unlimited users and departments.
- **Analytics and business intelligence solutions:** Access smart, intuitive data analytics and reports to stay on top of your operations 24/7
- **Advance portal for customer service module:** This module includes advance functionality for remote management of parking facilities.
- **On-demand based pricing module:** This module allows for an operator of asset owner to optimize garage rates based upon garage occupancy.

Other Features:

- **Contract/Monthly parker management (via AVI, Prox, LPR, etc.):** Monthly parking can be simplified with technologies like Prox cards, Automatic Vehicle Identification (AVI), and License Plate Recognition (LPR) that reduce interaction with kiosks.
- **Third-party call center solution including Parker Video Intercom two-way video support:** FlashParking's Smart Stations support call center options including Commend, Umojo, and Parker Video Intercom two-way intercoms for premium customer service offerings.
- **eParking Online Reservation modules:** FlashParking is integrated with all major eParking online reservation systems, allowing you to connect with the eParking vendor of your choice.
- **PARCS to valet:** Increase revenue and garage occupancy with the by seamlessly converting your transient parkers into valet parkers.

- **Access zones and access restrictions:** Restricted areas can be created with additional points of access, easily controlled by prox cards or guards, beyond the initial gate entry.
- **Reversible lanes:** Since our Smart Stations can be configured for entry or exit, lanes can be set-up to perform an entry or exit role at different times.
- **Enforcement Integration:** FlashParking through our open API sends data to Enforcement, after a parker has made an entry input on the Multi-Meter FlashParking kiosk configured as Pay by Plate or Pay by Space. Once transaction is complete info is sent to Enforcement in real-time through API. Enforcement app will take over enforcement duties at this point.

(FlashPARCS Solution Overview)

SOFTWARE PLATFORM

Overview

With FlashParking's highly configurable cloud-based platform, built using Microsoft Azure Cloud Services, clients can capitalize on a dynamic, "future-proof" system, that will expand and support new capabilities as technology and customer demand evolves. We've essentially taken the cloud computing success seen in other industries and applied it to the parking industry to enable a more effective way of operating parking operations, improving the bottom line and delivering world class customer experiences.

(FlashCloud product sheet)

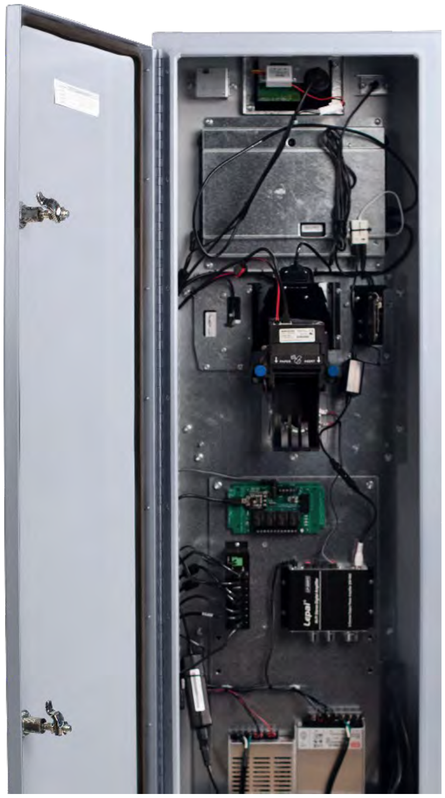
HARDWARE

Overview

Our design brief for building hardware products to run the FlashParking platform was to create next generation PARCS equipment that would eliminate and minimize issues that legacy PARCS systems suffer from. All our Smart Station form factors combine all the essential elements needed to manage parking access and revenue control into a streamlined kiosk. The system is designed with the guiding principle of "fewer moving parts = less chance for a breakdown." Replacing or upgrading individual components can be done in a matter of minutes in a USB-based, plug-and play hardware system.

With our equipment manufactured and assembled in our production facility in the U.S. and a direct sales and installation model, we control the end-to-end process; thus, creating efficiencies, in sales, onboarding, installation, deployment, and training.

Additionally, for enterprise and Smart City operations, FlashParking's infrastructure is deployed rapidly, maintained easily, and delivers incredible value and cost efficiencies over time with future-ready architecture.



Products

Smart Stations: The Smart Station is a Bluetooth-enabled, cloud-based kiosk with flexible software configurations, seamless integrations, and easy DIY maintenance guarantees maximum uptime. Bringing all the essential elements needed to manage parking access and revenue control into a single elegant unit, our physical kiosk is identical for entry or exit, pay-on-foot, or multi-space kiosk. The software platform is simply configured prior to shipping making the installation process efficient.

- ***Entry/Exit Smart Station:*** The Entry/Exit kiosk is highly customizable to meet the unique demands of your facility. Whether it will be used to manage transient and/or monthlies, the software package is simply configured for each machine's role in the venue. The Entry/Exit come standard with credit card reader, barcode scanner, ticket spitter, RFID reader, LCD display and IoT controller, and a Bluetooth technology reader. *(Entry/Exit Smart Station product sheet)*

- ***Pay-on-Foot Smart Station:*** The Pay-on-Foot Smart Station can be configured for PARCS, valet, or both. The POF Smart Station can be set up anywhere often in a garage or lobby as an additional payment station. For valet operations, the Valet POF/Vehicle Retrieval Smart Station allows for guests to request their vehicle and pay. *(Pay-on-Foot Smart Station product sheet)*

- ***Multi-Space Smart Station:*** The Multi-Space Smart Station can be configured as either a Pay-&-Display, Pay-by-Plate, or Pay-by-Space kiosk. The flexible configuration ensures the best set up based on venue dynamics and customer experience demands. *(Multi-Space Smart Station product sheet)*

Mini Smart Station: A streamlined version of our full-sized, cloud-based Smart Station is available in the following configurations for eParking Reservations, Monthly Parkers, and PARCS kiosk. monthly parker access via Bluetooth beacon technology, RFID/Prox card reader and features a scanner that reads QR and barcodes.

- ***Level 1 – Monthly Mini Smart Station:*** We know how important monthly and contract parkers are to your business; monthlies are often the steady lifeblood of your operations. Your parking solution should be able to meet their demands. With that understanding, we developed our Monthly Parking Mini-Smart Station to harness the power of our cloud-based parking platform, provide state-of-the-art Bluetooth access with FlashBeacon, and read over 65 types of RFID/prox cards. The Monthly Parking Mini-Smart Station can stand on its own or can work with legacy PARCS equipment. *(Monthly Mini Smart Station product sheet)*

- ***Level 2 – eParking Mini Smart Station:*** Today's parkers are increasingly sophisticated, with many looking to make their parking experience as frictionless as possible. Finding and pre-paying for parking via parking reservation solutions is becoming the method of choice for tech savvy consumers. Your parking solution should be able to meet their demands. With that understanding, we developed our eParking Reservation Mini-Smart Station to harness the power of our cloud-based parking platform, provide state-of-the-art Bluetooth access with FlashBeacon, as well as read and accept mobile or printed tickets. *(Monthly Mini Smart Station product sheet)*

- ***Level 3 – PARCS Mini Smart Station:*** Designed to give your customers the best parking experience possible, our PARCS Mini-Smart Station solution suite is highly configurable to meet the specific needs of the venue today and can be easily reconfigured in the future as those needs evolve. You will no longer need to buy totally new equipment as needs change, a simple re-configuration of the unit is all that is required. The PARCS Mini

Smart Station can be configured for these scenarios: entry/exit, pay-on-foot, self-validator, pedestrian access, valet access control, or valet POF/retrieval. *(Monthly Mini Smart Station product sheet)*

Wall Mount Smart Station: The Wall Mount Smart Station brings together all the functionality enjoyed in our full-sized Smart Station, but in a compact unit. This fully functional unit is perfect for tight spaces: it can be bolted on to a garage wall or mounted on a pedestal; it is also ideal for a venue looking for a pedestrian access kiosk. The Wall Mount Smart Station is available in the following configurations: Entry/Exit, Pay-on-Foot, Multi-Space Meter, Pedestrian Access, and/or as a Self-Validation machine. *(Wall Mount Smart Station product sheet)*

Cash Acceptance: The cash machine was designed as an add-on component to our Smart Station. It's built to provide all the cash-handling ability of a human cashier with increased security and cash management benefits. FlashParking's Cash Machine comes in two variations: exact change bill acceptor or Bill Note Recycler (BNR), which includes up to a 4-denomination recycling capability. *(Cash Machine with Bill Note Recycler product sheet)*

Gates: FlashParking is a proud partner with Magnetic, whose Access Barriers are both highly reliable and boast the fastest vend times. Magnetic's Access Pro series barriers are optimized solutions for access control at car parks, residential buildings, company grounds, port facilities and other secured areas with lane widths up to 20 ft. At the heart of the Access series is the innovative MHTM drive that is distinguished by its energy efficiency, lack of maintenance and long service life; the Access series is designed for 10 million opening and closing cycles. *(Magnetic Gate product sheet)*

Frictionless Access: Frictionless access, a.k.a. automatic vehicle identification (AVI), is no longer a luxury—it is quickly becoming the standard for monthly parkers. Parkers want to be able to come and go without having to roll down their car window, which is why FlashParking offers full integrations with TransCore, Survision's License Plate Recognition (LPR) system, as well as our own proprietary Bluetooth access option. Depending upon your venue and operational needs we have a frictionless access option that will take your monthly parking to the next level.

FlashBeacon: Bluetooth Beacon Technology: All FlashParking Smart and Mini-Smart Stations come standard with FlashBeacon, our proprietary frictionless Bluetooth beacon technology. This technology is different the traditional Bluetooth technology available to speakers and mobile ready devices. The FlashParking Bluetooth beacon transmits a directional signal 8 FT in the direction of a single lane. The technology is designed to target the mobile device of the guest seated in the driver's seat. The beacon works like an AVI scanner in the sense that it pulses a signal in the entrance or exit lane of the garage. It is constantly searching for the credentials of a tenant to be able to grant access. This process works like a traditional AVI windshield tag, but instead uses a mobile device. The parker would just need to download the FlashParking app to be able gain access to the garage via Bluetooth. It's that simple. *(FlashBeacon product sheet)*

TransCore: A leader in AVI, TransCore's wireless, RFID-based system ensures the highest level of security, while providing hands-free convenience and sustainability. TransCore is perfect for facilities that are looking for an AVI-option that is integrated with toll-tags.

LPR: FlashParking is fully integrated with Survision's License Plate Recognition system. Survision is an effective, cost-efficient and scale-able license plate recognition. It is offered as a Software-as-a-Service (SaaS). Survision's cloud-based architecture means that there is no infrastructure to install or maintain – just supply the images and access the data – in real-time.

Monitors: FlashParking offers an assortment of digital monitors that help keep your customers informed in real-time. From a simple garage occupancy sign to an outdoor, dynamic digital rate sign, to a vehicle retrieval sign that keeps valet customers informed wait time for their car–our monitors can be set-up for both indoor and outdoor venues. Need a garage occupancy sign outdoors? No problem, all our monitors can be installed for indoor and outdoor purposes. Also, our digital rates signs can be hung horizontally as well as vertically for best user interaction.

AUDIT AND REVENUE CONTROLS

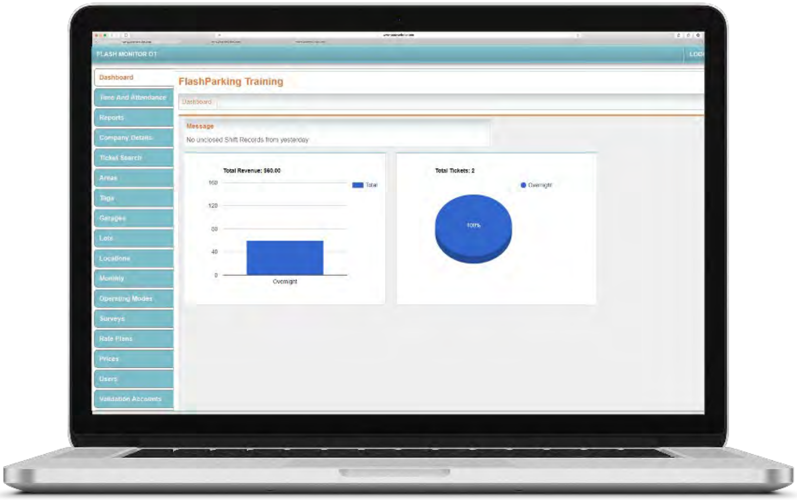
FlashParking is a technology company. Our cloud-based solution gives you complete control over your system. You can change a rate in seconds, shut down transient parkers so that you maintain room for monthly parkers or monitor your activity via our hundred plus reports.

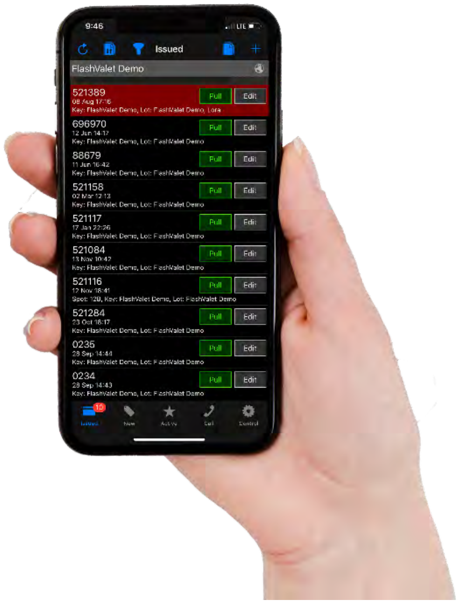
Audit Controls & Tools

Everything that happens in the FlashPARCS system, whether at the kiosk, cashier or valet is electronically tracked and reported on. Additionally, every user has their own log in with a unique password, so their activity is tracked and controlled. Here are just a few of the many audit controls we have in place:

- Cashier controls – everything that happens in the system is tracked.
- Electronic journals – Yes, the cash machine keeps an electronic journal.
- System security – Alarms and unique locks are part of the system security.
- Separate locks for cashboxes – Yes, there are separate locks for the cashboxes on the BNR.
- Unique logins – Each user will have a unique login and passcodes, which are managed by the Admin.
- Alarms for unauthorized access – Yes, alarms sound if there is unauthorized access.
- Car presence required for transaction – Yes, a car must be present for a transaction to take place.

FlashPARCS Management App
Manage operations via phone or browser anytime, anywhere, including rate changes, credit card payments, electronic validations, and much more. Our FlashPARCS Management App will allow to monitor and manage operations in real-time, so they can make the best operation and business decisions possible.





REPORTING

Overview

With FlashCloud's reporting suite operators and asset owners can access detailed reports anytime, anywhere via the FlashCloud for minute-by-minute insights on key performance indicators that enable operational efficiency and smart business strategies.

Our comprehensive Admin Portal houses a reporting suite that offers insight into key metrics and calculations like occupancy per hour, tickets issued, rates, transaction details, payments, validations, kiosk summaries, and monthly parking activity. Reports are available in PDF and XXLS formats and can be called on demand anytime, from anywhere, or schedule to arrive in your inbox routinely.

FlashPARCS has over 100 on-line reports that are available to any user via Administration Rights. These reports can be accessed through any connected device. Several reports can be scheduled to be delivered to an email address every day. The reports cover everything that happens via the FlashPARCS equipment, including Counts, General Totals, Detailed Transaction Reports, Card Holder Reports, etc. Examples of reports are available upon request.

Total Visibility

With over 100 reports to choose from, you'll be equipped with intelligence on every facet of your operation. FlashParking's integrated platform allows for combination reports that can merge PARCS and valet data into one seamless summary. Data points can also be pushed to other individuals or programs via API for total visibility.

Popular Recommended Reports Include

- **Location Summary Hotel**
  Not just for hotels, this comprehensive report provides an executive-level summary of tickets processed per price per kiosk. It also provides a payment summary broken down by tender type and includes a sub-report that provides the number of vehicles processed per fee.

- **Location Transaction Detail**
  For a closer look at transactions, details including ticket number, arrival, departure, duration, and payment information can be found in this report. At the end of the report is the total amount transacted as well as an average duration and coupon summary.

- **Contact Center Detail**
  This report provides information on support calls made through any kiosk in the system.

- **FlashPARCS Vend Exceptions**
  For details on each time the "vend" function was used in the mobile app or when the gate was vended via a support call, this report will provide the source of the command, the kiosk on which it was performed, the time, and any notes associated with the action.

- **Location Issued Ticket Detail**
  Run this report for a detailed list of all transient tickets that were issued for a selected time period per kiosk.

- **Occupancy Per Hour (PARCS)**
  This report provides the number of vehicles that entered and exited per hour, along with a running total and identifies the peak hours.
- **Electronic Payments**
  The Electronic Payments report provides details for each credit card transaction and breaks down subtotals per credit card type.

- **eValidation by Date and Validator**
  All electronic and printed validations are provided in this report alongside the duration of stay, discount amount (for billing back), and amount paid. Subtotals for the validation usage per validator are also included.

- **Kiosk Summary**
  Similar to the Location Summary Hotel, this report details transactions but separates them out by individual kiosk.

Intelligent Decision Making

Using data to make strategic business decisions will boost efficiency and revenue. For instance: tracking the patterns of transient and monthly parkers allows you to maximize occupancy and revenue by filling underutilized spaces; recognizing the average duration of a stay can inform pricing decisions as well as offer valuable customer data to your tenants.

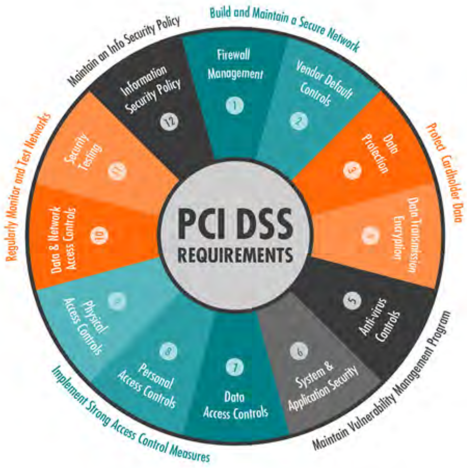
(FlashParking Reports Overview)

PCI COMPLIANCE

PCI DSS Certified

We are committed to delivering PCI DSS compliant technology that takes the burden away from you. As a PCI-DSS Level 1 Service Provider (the highest level of PCI compliance and cyber security available), we deliver a processing system that can handle millions of transactions daily in a reliable and safe environment. Today, we process over 5 million transactions per month through our ,000 plus locations.

Our cloud-based platform means that there are no on-site servers to maintain. Adopting a cloud-based approach to your operations allows you to shift the burden of upkeep, maintenance, and compliance of the system to us, leaving you to focus on your core competencies.


Build and Maintain a Secure Network
Protect Cardholder Data
Maintain Vulnerability Management Program
Implement Strong Access Control Measures
Regularly Monitor and Test Networks
Maintain an Info Security Policy
Firewall Management 1
Vendor Default Controls 2
Data Protection 3
Data Transmission Encryption 4
Anti-virus Controls 5
System & Application Security 6
Data Access Controls 7
Personal Access Controls 8
Physical Access Controls 9
Data & Network Access Controls 10
Security Testing 11
Information Security Policy 12
PCI DSS REQUIREMENTS

In fact, we handle 98% of the PCI duties by taking on the technical burden, so you can stay focused on running your operation, not on fixing and updating machines. The result is instant and on-going complete PCI compliance. The means you don't need to worry about not being compliant, requiring patches, paying for costly monthly or yearly updates or having a server go down. *(FlashParking's PCI Approach; In-depth Encryption and Data Flow document; Letter of Attestation)*

PROJECT PLAN AND INSTALL TIMELINE

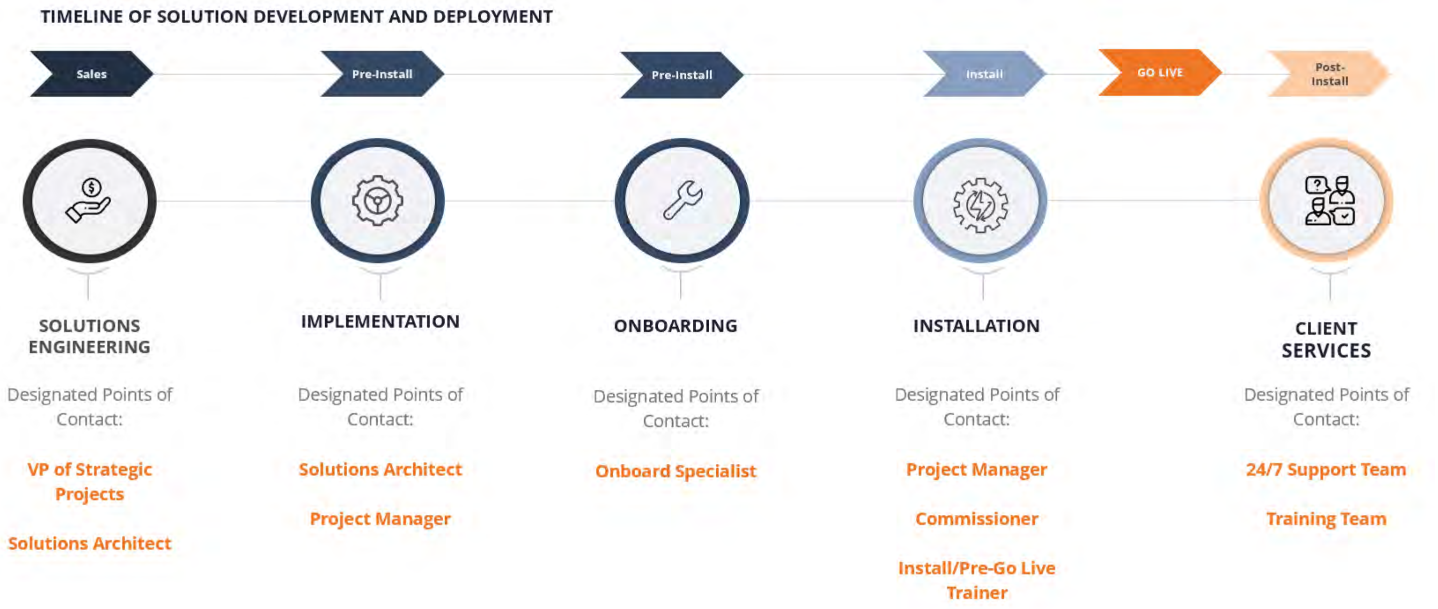
FlashParking has successfully completed difficult installations at high volume locations such as the Texas Medical Center (200 lanes in 44 days), T.F. Green Airport, City of Las Vegas, Aspen Airport, Port of Miami, and Presbyterian Hospital in Dallas to name a few.

Our Implementation and Installation Teams have spent endless cycles on simplifying and optimizing the deployment process. Considering down time, flow and customer experience, our Flash team will have you back up and collecting revenue faster than anyone else.

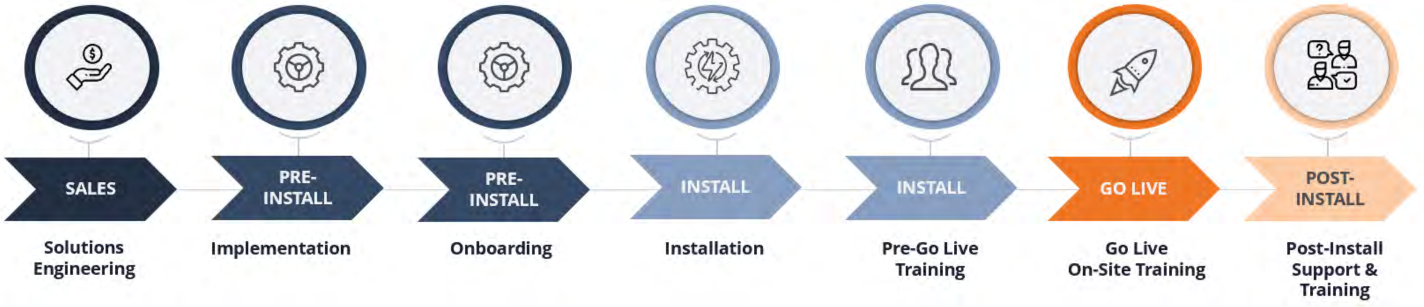
Post-install, our Client Services Team (comprised of support and training) takes customer care and service very seriously. That is why we survey our customers after installation, every support interaction, and quarter. We track the feedback utilizing the Net Promoter Score method. Our dedication to customer satisfaction is one reason we have a high success rates with our installations.

Over the next couple of pages, we will outline our approach to development and deployment to building and deploying your custom enterprise solution from start to finish.

1. Organizational Chart



2. Development & Deployment Overview Approach



SALES: FlashParking's sales/solutions engineering team works with the client to create a Theory of Operations document that identifies equipment/solution needs.

PRE-INSTALL: There are two parts to this phase: Implementation and Onboarding. During Implementation, a Project Manager works closely with the client on installation planning, equipment purchasing, and solution training. During Onboarding, a specialist gathers info and key deliverables from the client to properly build out the backend of the solution. As the Implementation and Onboarding wrap up…it's go time!

INSTALL: During the installation, a commissioner oversees and manages the FlashParking's operations team as they install the solution and communicate daily with key internal and external stakeholders to ensure a seamless, smooth roll out. Towards the end of the install, a FlashParking representative will connect with customer to schedule online and on-site training (if purchased).

GO LIVE: Systems are a go! Customers have the option of booking a Go Live Trainer to train during the initial Go Live phase. As the Go Live phase comes to an end, a transition kick-off call introduces the client to client services and account management teams.

POST-INSTALL: Our support and training team are always a phone call away. Each team will provide providing assistance in training and support escalation ensuring that the client is getting the most value out of the FlashParking platform.

3. Development & Deployment Detailed Approach

Sales/Solutions Engineering Phase

- Our Sales and Solutions Engineering Team will work closely with stakeholders to plot and create the best solution to address operational needs and wants. Our Solutions Architect gathers site data to fill out a Theory of Operations (TOO) for each site and identifies equipment needed to complete the solution. The Sales Team will put together a comprehensive deal for review. Once contract is signed and 50% deposit is received, the Implementation phase kicks off.

Pre-Install Phase

- **Implementation**
  We will dedicate a seasoned Project Manager to handle all logistics related to the implementation phase to ensure a smooth transition. During this phase the Solutions Architect and the Project Manager collectively work together and set a weekly communication rhythm with internal and external stakeholders to discuss theory of operations and identify site-specific requirements and development needs.

- **Onboarding**
  An important part of the implementation phase is onboarding. For each venue, an Onboard Specialist creates an onboarding project in Task Ray with key milestones and deliverables prior to the installation, followed by a configuration kick-off call that informs client of next steps in customizing their FlashParking Solutions. The Onboard Specialist gathers and coordinates site-specific onboarding deliverables and identifies any development needs for the Development Team.

- **Pre-Install Training**
  We are proud to offer a tiered training that kicks-off with our Pre-install Trainer conducting a pre-install webinar. To help train the customer on how to use FlashParking solutions, the trainer lays out the Training Webinar agenda that includes reporting, validations, rate structures, monthlies, and more. If additional help is needed, the trainer is available to do onsite Go Live training (if purchased) to address specific concerns. Towards the end of the Pre-Install Phase, a Commissioner is assigned to kick-off the Installation phase.

(FlashPARCS Training Manual)

Install Phase

□ Installation

At the start of the Installation phase, your Project Manager will conduct an external kickoff call with internal and external stakeholders to discuss timeline and hardware installation requirements. Your Project Manager generates and maintains the installation schedule at both the portfolio and site-levels as well as oversees equipment testing. During the roll-out, your on-site Commissioner provides on-site service and support and oversees the testing plan.

□ Testing Plan

Our goal is to get your facility up and running as quickly, but as efficiently as possible. To accomplish this, we have structured different levels of testing and counter checks. This thorough and vigorous setup ensures that when your equipment is installed and turned on you are ready to start collecting revenue.

□ Install/Go-live Training

If purchased, your Go-Live Trainer, will provide onsite support during Go Live to assist with operational issues. Based on the complexity of a venue, the trainer remains onsite for a pre-defined period.

Post-Install Phase

□ Post-Install Training

FlashParking also provides commentary virtual training sessions. Property owners and site managers can book I hour, personalized session with our master trainers on their time by using our booking website. The training session can also be recorded so the information can be shared throughout management team. Our trainers can help with generating custom reports, managing validation accounts, implementing new software rules in your operation or onboarding a new team member. FlashParking committed to providing ongoing support to all our locations in effort to create the perfect customer parking experience.

Trainers are also available for additional in-person training (fee applicable).

□ Support Team

Once the project is live, FlashParking will deliver continuous 24/7 support to your location at no additional charge. This includes service calls to our support centers in Austin, TX and the Dominican Republic who can resolve software issues remotely. Follow up visits from our regional sales managers to share best practices for mix use properties with the local operations team.

□ Maintenance

We have an innovative approach to servicing our FlashPARCS equipment. Our kiosks are designed to be maintained by on-site support staff, therefore alleviating expensive and quite often delayed service calls. The kiosks are modular, meaning any part can be replaced within seconds and utilizing only a screwdriver. This is a similar service model to existing On-Street equipment providers such as Calle and Parkeon. Our equipment is always on-line; therefore, we ping each unit every 15 seconds for a heartbeat, which means we know almost immediately if anything ever malfunctions. We then send a notification to on-site staff so that they can address any issue immediately. There is no need to wait for an expensive technician to schedule a service call the next business day. “Maintenance Kits” are available so staff can have immediate access to a replacement part; the Kit contains a replacement part for all the major components in the kiosk. ***(Maintenance Model handout, FlashParking’s FlashCare maintenance kit)***

IN CONCLUSION SUMMARY

- Based on the requirements detailed in your RFP, we believe FlashPARCS is a perfect solution for Ft. Lauderdale Airport's Parking Access and Revenue Control Equipment and Maintenance. As a technology company, we offer the most advanced PARCS solution in the industry. Not only will our PARCS equipment satisfy you current requirement, we continue to research better ways to improve your operations via new technologies, software development and equipment enhancements.

SECTION III
PRICING

FlashParking

FlashParking

Proposal for:

Ft Lauderdale Airport

Prepared For:
Broward County
Ft Lauderdale Airport 115 South Andrews Ave
Fort Lauderdale, FL 33301
United States

Created By:
James DuFon
FlashParking, Inc.
(800) 213-3706
james.dufon@flashparking.com

FlashParking

Customer Quote

FlashParking, Inc.

The total simple approach to parking

3801 S. Capital of Texas Highway, Suite 250
AustinTX78704
USA
Phone: (800) 213-3706
Email: sales@flashparking.com

Quote Nbr:	Q-13193-1
Date:	3/2/2020 3:19 PM
Expires On:	4/1/2020
Prepared By:	James DuFon james.dufon@flashparking.com

Bill To
Broward County
115 South Andrewes Ave
Room 212
Fort Lauderdale, Florida 33301
United States

Ship To
Ft Lauderdale Airport
115 South Andrews Ave
Fort Lauderdale, FL 33301
United States

FlashPARCS - Hardware

Product	Description	Unit Price	Qty	Discount	SubTotal
FlashPARCS Smart Station Entry	Ruggedized parking station with: - Interactive-customizable touch display - Ticket dispenser - Credit card acceptance - Barcode scanner - RFID reader - Intercom with mic and speaker	$15,000.00	19	$0	$285,000.00
FlashPARCS Smart Station Exit	Ruggedized parking station with: - Interactive-customizable touch display - Receipt dispenser - Credit card acceptance - Barcode scanner - RFID reader - Intercom with mic and speaker	$15,000.00	27	$0	$405,000.00
Mini-Smart Station for Monthly Parkers ONLY with RFID + Intercom	Provides access control for monthly parkers via: - Proximity card reading - Bluetooth Access Includes: - LCD Display - RFID reader - BLE Technology (Bluetooth Low Energy) - Intercom	$2,900.00	15	$0	$43,500.00
FlashPARCS - Pay on Foot Smart Station - Credit Card Only	Provide your guests with the ability to pay in advance. Ruggedized pay station with: - Interactive-customizable touch display - Credit card acceptance - Receipt dispenser - Barcode scanner - Intercom with mic, speaker and camera	$15,000.00	15	$0	$225,000.00

Product	Description	Unit Price	Qty	Discount	SubTotal
Cash Machine with Bill Recycler	Cash Machine: - High first-time insertion Acceptance rate - Advanced sensor technology scans both sides of the billâ€”optimizing recognition - Self-centering transport guides that automatically adjust to and perfectly align bills â€” even when fed at an angle - Single Hardware Platform to reduce support and operation cost - Accepts, stacks and outputs cash - Customer friendly, high speed and high security acceptance - Escrows bills to deliver same cash back to customers - Pays out in bundles of up to 15 bank notes - Lockable, removable and durable cashbox - Electronic memory to record cash loading RECYCLING UNITS -Does not accept coins or dispense coins	$18,750.00	3	$0	$56,250.00
Spare Cash Box for Bill Recycler	- Lockable, removable and durable cashbox	$750.00	1	$0	$750.00
EMV Kit (Chip Card Reader)	Includes EMV reader + NFC The SCR200 is a Windcave EMV compliant Secure Card Reader (SCR). Supports Magnetic Stripe, ICC (chip card), and Contactless (NFC) payment types (via contactless receiver). **The SCR200 is ONLY compatible with Windcave Merchant accounts	$1,500.00	61	$0	$91,500.00
FlashPARCS Network Kit	Includes a network kit with a primary line and 4G/LTE backup for full connectivity network redundancy and network security.	$2,500.00	1	$0	$2,500.00
FlashCare Kit PLUS	Includes: - FlashCare Kit with replacement parts for all major components for FlashPARCS Smart Station: > Rugged tablet > Ticket/receipt thermal printer > Barcode scanner > Magnetic credit card reader > RFID proximity card reader > Relay board > Central USB-peripheral hub > 12V (a.) & 24V (b.) power Supplies - Includes mini smart station controller and display	$8,000.00	1	$0	$8,000.00

Product	Description	Unit Price	Qty	Discount	SubTotal
Transcore Reader with mounting Kit	Includes: - Reader Entry or Exit - Reader Integration to FlashPARCS - Integration to FlashPARCS Monthly Parker Management Module - Cypress Board for Transcore compatibility - Wiegan Board to USB - Delay Relay	$6,000.00	19	$0	$114,000.00
License Plate Recognition (LPR) Solution	**1 camera per lane Micropak, power and fixation accessories, commissioning with a skills transfer.** Features: -ALL-INTEGRATED: License Plate Recognition camera is carried out entirely in the camera -EASY TO INSTALL: The camera automatically adjusts its filming and lighting parameters in order to be able to provide an optimal performance regardless of the conditions. The camera settings compression, frequency,...) can be carried out remotely. -HIGH SPEED: Supports vehicle speeds up to 155 miles/ hour -IP67 CASING For Indoor and Outdoor installations -VIDEO STREAM provided in real time (Standard RTSP streaming) FAST: 60 frames per second The Micropak camera • Is optimal for recognition distance 10-33ft • includes 4 strong power pulsed IR (850nm) or White Light LEDs and HD 1.3MPixels Black&White optic • perfectly works in Free Running (no trigger) mode or software/ hardware trigger • doesn’t need any server	$111,250.00	1	$0	$111,250.00

Product	Description	Unit Price	Qty	Discount	SubTotal
Parking.Pro Magnetic Parking barrier	- Specifically designed for high volume parking applications - Opening / closing times starting at 1.3 sec - High functionality - Only 35 W of power consumption (Magnetic.Parking) - Safe control unit according to EN 13849 - 10 million opening and closing cycles	$3,750.00	61	$0	$228,750.00
FlashPARCS Magnetic Gate Care Kit for straight gate arm barrier boom kit	Kits include complete gate arm with grey sections, T30 & T40 Torx wrenches	$450.00	1	$0	$450.00
				FlashPARCS - Hardware TOTAL:	$1,571,950.00

FlashPARCS - Services

Product	Description	Unit Price	Qty	Discount	SubTotal
EMV Gateway setup		$3,000.00	1	$0	$3,000.00
Bond Fee	Travel + Expenses	$0.00	1	$0	$25,640.00
License Plate Recognition Setup	Includes: > Configuration, Setup, Testing and Commissioning.	$0.00	1	$0	$0.00
				FlashPARCS - Services TOTAL:	$28,640.00

Shipping and Handling

Product	Description	Unit Price	Discount	SubTotal
Shipping and Handling-160 Units		$250.00	$0	$40,000.00
			Shipping and Handling TOTAL:	$40,000.00

Implementation

Product	Description	Unit Price	Discount	SubTotal
Implementation-15 Days	Setup, Configuration, Commissioning & On-Line training	$900.00	$0.00	$13,500.00
			Implementation TOTAL:	$13,500.00

Travel and Expenses

Product	Description	Unit Price	Discount	SubTotal
Travel and Expenses-15 Days	Travel & Expenses	$1,250.00	$0.00	$18,750.00
			Travel and Expenses TOTAL:	$18,750.00

FlashPARCS - Services

Product	Description	Details	Discount	SubTotal
FlashPARCS Extended Warranty	Purchase of additional 12 months warranty on all parts for each FlashPARCS Smart Station from the date of installation in addition to standard warranty.	76 Stations - 1 Year	$49,665.00	$0.00
			FlashPARCS - Services TOTAL:	$0.00

Installation

Product	Description	SubTotal
Smart Station Installation	Includes: - Data: ethernet cables from switch to kiosk with (1)# conduit recessed connection to each Smart Station. - Smart Station Kiosk Installations. Includes bolts & washers & shims as needed. - Existing equipment removal and disposal (when applicable) *Permits when applicable (Pass Through plus Service Fees) TBD.	$154,237.50
Automatic Vehicle Identification (AVI) Installation	*Permits (Pass Through plus Service Fees) TBD.	$7,771.50
Gate Installation	Includes: - Gate & boom installations done in conjunction with Smart Station installations. - Arming and closing loop channels from gates channels to be scored in conjunction with work (when applicable). *Permits (Pass Through plus Service Fees) TBD.	$53,434.50
Custom Installation and Setup	LPR Installation Tie into existing electronic signage and ParkAssist system Misc. installation expenses	$55,000.00
	Installation TOTAL:	$270,443.50

FlashPARCS - Software

Product	Description	Discount	SubTotal
FlashPARCS Software License - 5 Years	-Software upgrades for life of Software (includes all PCI upgrades). No surprise fees. -Cloud Born Multi Tenant System -24/7 Online support + online training -Mobile first tech. Change rates, vend gates, real time reporting suite from anywhere. -Scheduled reporting that can be customized and sent to X users.	$54,120.00	$191,880.00

Product	Description	Discount	SubTotal
Cash Acceptance Module - 5 Years	Offers the ability to accept cash bills.	$1,320.00	$4,680.00
Advance Portal for Customer Support Module - 5 Years	Includes advance functionality for remote management of parking facilities.	$1,320.00	$4,680.00
Validation Module - 5 Years	Electronic or Printed validations from any browser, or via Mobile App or via Text - for unlimited users & departments.	$1,980.00	$7,020.00
Access via Credit Card and Mobile Number - 5 Years	Parkers have the option to access parking facility via Credit Card or by entering Mobile Number.	$1,980.00	$7,020.00
eParking Online Reservation - 5 Years	FlashParking is integrated with all major eParking Online Reservations.	$1,320.00	$4,680.00
Onscreen Kiosk Banner Advertising - 5 Years	Digital banner adds can be presented onscreen at Entry, Exit or Pay on Foot Smart Stations.	$660.00	$2,340.00
Monthly Parkers Access via Mobile Phone (IVR) - 5 Years	Registered parkers can access parking facility by calling from their registered mobile phone. Thus reducing call for help volumes.	$1,320.00	$4,680.00
Multi-Lingual Module - 5 Years	Smart Stations can be configured with multiple language options.	$1,320.00	$4,680.00
FlashPARCS License Plate Recognition (LPR) Module - 5 Years	Enables use of FlashPARCS LPR cameras (various configurations available).	$1,980.00	$7,020.00
AVI Module - 5 Years	Allows for seamless integration and support for interface between AVI’s and FlashPARCS	$1,320.00	$4,680.00
Custom Software - 5 Years	Software for Valet Stands at Terminals 1, 2 & 3 Hardware is not included and will be determined by operator	$0.00	$36,000.00
		FlashPARCS - Software TOTAL:	$279,360.00

FlashPARCS - Managed Services

Product	Description	Unit Price	Qty	Discount	SubTotal
Managed Network Services with 4G/ LTE Back-up	for Term of Software Fee	Included	76	$0	$0.00
Real-time Reporting Suite	for Term of Software Fee	Included	76	$0	$0.00
24/7 Phone and Online Support	for Term of Software Fee	Included	76	$0	$0.00
Ongoing PCI compliance + Software Updates and general soflware patches	for Term of Software Fee	Included	76	$0	$0.00
Mobile App Module (for managing parking operations)	for Term of Software Fee	Included	76	$0	$0.00
FlashPARCS Warranty Standard	Warranty for the initial 12 months on all parts for each FlashPARCS Smart Station from the date of installation.	$750.00	79	$59,250	$0.00
				FlashPARCS - Managed Services TOTAL:	$0.00

Quote Summary

Product Type	Subtotal
FlashPARCS - Hardware	$1,571,950.00
FlashPARCS - Shipping	$40,000.00
FlashPARCS - Services	$60,890.00
Installation	$270,443.50
FlashPARCS - Software	$279,360.00
FlashPARCS - Managed Services	$0.00
Total	**$2,222,643.50**

****Taxes not included**

DISCLAIMERS

FlashPARCS equipment

- Equipment orders are subject to a 50% deposit payment at time of signing to ensure timely delivery of project. FlashParking reserves the right to charge a cancellation fee of 20% of the total of the contract to be paid immediately at time of cancellation.

- The remaining 50% will be invoiced upon successful installation and commissioning of the FlashPARCS equipment, or within two months of equipment receipt by Customer if Customer delays the installation, whichever comes first.

Delivery Lead Time

- Smart Stations and Magnetic Barrier Gates delivered and installed on average within 3-4 weeks for standard installations of 10 units or less - from time of contract signature (contingent upon credit approval and good standing of existing accounts receivable).

Excludes orders with LED Barriers, Custom Wrapping for Smart Stations, LPR Cameras, AVI Readers or any other third-party equipment as these may have longer lead times from manufacturer.

Cash Machine

- Cash Machine can be delivered and installed on average within 6- 8 weeks for standard installations of 10 units or less - from time of contract signature, and after 50% deposit payment is received.

- Bill acceptor manufacturer provides a limited warranty on its equipment that covers all mechanical and electrical components, but excludes parts subject to wear and tear, for a period of two years for parts and RTF (return to factory or authorized service center) labor warranty.

Standard Installation

- Internet connectivity and electricity is required and is to be provided by venue or parking operator.
- Installation quote is based on the information provided by client. All other requirements not provided by the client before installation are subject to review, and additional fees may be assessed to cover the work.
- Assumes a concrete surface on each lane, that the concrete is in good enough condition to install the saw cut loop, it has no major cracks and is not post tension construction. If the location is post tension construction then please inform install team during the kickoff process to send a concrete contractor to perform a surface penetration scan to ensure it is safe to make the cut for the loop, additional fees will apply.
- All work installation services to be performed during normal business hours, Monday through Friday, excluding holidays, by non-union labor.
- Reusing or running one ethernet cable from the network demarcation point to the FlashPARCS Smart Station Kiosk using existing pathway or conduit **
- Mounting FlashPARCS network kit with back-up LTE in each lot or garage (will be pre-configured prior to shipping)
- Removing old entry (ticket/spitter) or exit (exit verifier) machine
- Removing old gate (when applicable)
- Cutting, installing & calibrating new arming and safety loops
- Connecting both loops to the gate
- Bolting down the Smart Station kiosk (they immediately get their configuration from the cloud infrastructure upon powering-up)
- Bolting down gate
- Running 3 pairs of cables from the Smart Station Kiosk to gate for (a) gate vend, (b) arming loop detection, and (c) closing loop detection
- Clean up: placing old machine and gate in a designated area within the facility (Old Equipment disposal not included)
- Testing all components: getting a ticket, and every entry or exit method including real credit card payment transaction, microphone & speakers (placing a support call), barcode scanner, proximity card reader, Bluetooth access, vending gate and loop detection
- Extending or re-routing existing electrical power lines to new SmartStation Kiosk and gate **

***** Not to exceed 15 feet***

****** Old Equipment disposal not included in price***

Exclusions:

- All utility company charges, deposits and fees if any; Repairs for unforeseen underground utilities that may become damaged during installation of underground conduits; Performance and Payment Bonds. All other requirements if any are extra and are subject to review; (All Permit and Inspections are a Pass Through - plus Service Fees if applicable).

LPR Cameras

- LPR (License Plate Recognition) Cameras can be delivered and installed on average within 8-10 weeks for standard installations of 10 units or less - from time of contract signature, and after 50% deposit payment is received.

Transcore Reader

- Products are warranted by TransCore to Purchaser against defects in workmanship and material for one (1) year after the date of installation. Warranty service will be provided in the United States at a repair facility designated by TransCore. Transportation costs to and from the repair facility shall be paid by Purchaser.

Gates

- Gates manufacturer provides a limited warranty on its barriers that covers all mechanical and electrical components, but excludes parts subject to wear and tear, for a period of two years from the date of first use provided that the operating instructions have been complied with, no unauthorized servicing of machine components has taken place, and that no mechanical damage to the machines is evident.

* For EMV transactions *Client requires to open an account with Payment Express. FlashParking is not responsible for Merchant and Gateway fees associated with EMV transactions.*

* FlashPARCS Mobile Payments ($0.35 per mobile payment transaction).

*Onsite support available upon request. Fees and response time varies by region.
* All prices are exclusive of taxes, shipping, installation, electrical or civil work, and any other item non specified in this quote unless otherwise clearly stated in the proposal.

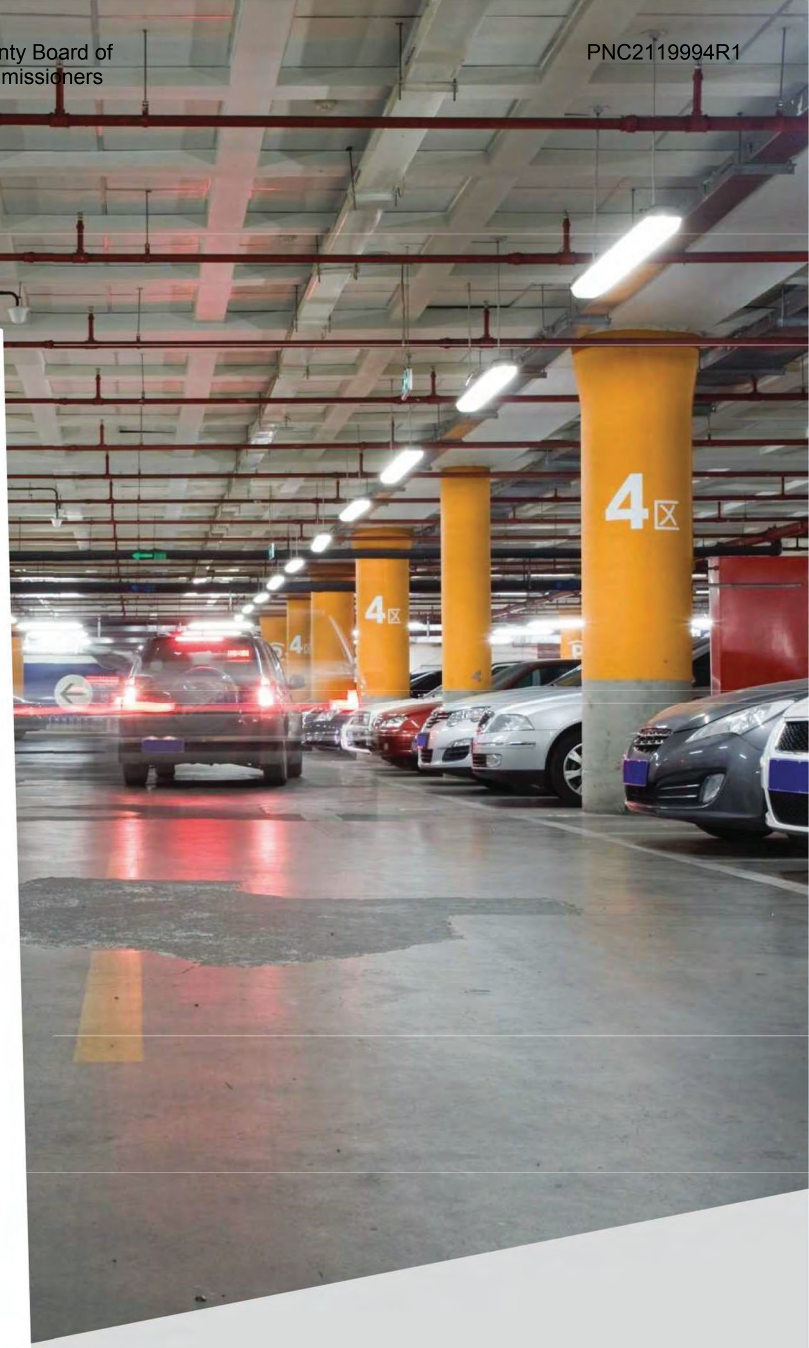
Equipment Service Options:

A) Self-Served with 24/7 Remote Hands FlashParking Support Team: FlashParking designed its solutions with simplicity and efficiency as the driving tenets. We supply every customer with a FlashCare maintenance kit containing all the replacements components needed for every machine and gate supplied by FlashParking. Should any of them fail, the client can easily remove the failed part and insert the replacement part with assistance from our remote hands 24/7 support team.

B) Remote/Smart Hands Support: Should you chose not to use our *Self-Served with 24/7 Remote Hands FlashParking Support* option. FlashParking employs an extensive network of highly vetted, independent repair technicians under the following terms below:

Regions	Mon-Fri	Mon-Fri (all day Sat)	Sundays and Holidays
	8:00 am–4:00 pm	4:00 pm–8:00 am	All day
AK, CA, HI, NY, TX, WA & Puerto Rico	$177.80	$267.40	$357.00
AZ, CO, OR & PA	$141.68	$212.52	$283.36
Everywhere else (US only)	$130.20	$195.30	$260.40
Plus Travel	$110/per trip		

Billing is in whole hours only (every fractional hour is billed as an hour). Response time varies by market. On average it can be within 4-6 hours.



SECTION IV

REQUESTED DOCUMENTS & ADDITIONAL INFORMATION

FlashParking

Enterprise Technology Services
Vendor Security Questionnaire (VSQ)
(For RFPs and Sole Source/Only Reasonable Source as applicable)

The Vendor Security Questionnaire's (VSQ) purpose is to assess your organization's security policies and/or system protocol and to identify any security vulnerabilities. Each responding vendor will be required to complete and submit the VSQ (for applicable solution – services, hardware, and/or software). If not included with the proposal submittal at the time of the solicitation opening deadline, the proposing vendor will be required to complete and submit the VSQ within three business days of County's request.

If a response requires additional information, the Vendor should attach a written detailed response; each response should be numbered to match the question number. The County will review Vendor's VSQ response and any security concerns will be addressed during Evaluation Committee Meetings or negotiations. Unresolved security concerns shall be considered by the committee as part of its final evaluation and may lead to impasse during negotiations.

The questionnaire is divided into the following areas: **Section 1: Software-as-a-Service/Hosting/Application Development/Managed and Professional Services**; **Section 2: Software**; and **Section 3: Hardware.** Each section(s) should be completed as applicable to your organization's proposed product and/or service. If applicable, failure to complete the questionnaire may deem a vendor non-responsible. The questionnaire should be submitted with your proposal. Vendor should immediately inform the assigned Purchasing Agent of any changes in vendor's responses after submittal.

Vendor Name:	Flashparking
Vendor Type (Manufacturer, Reseller, Other? If Other, specify.):	Manufacture
Technical Contact Name / Email Address:	Jim DuFon, james.dufon@flashparking.com
Product Name / Description:	FlashParcs
Solicitation Number and Title (If applicable):	PNC2119994R1 - Parking Access and Revenue Control Equipment and Maintenance

For each applicable section, complete the matrix by using the dropdown option to select YES or NO. Use "Comments" section to provide as much explanation as possible to clearly support your response. Additional pages may be attached to provide further detail, but any attachments should be referenced in "Comments" section. **Select "N/A" if a question within a given section is not applicable. IMPORTANT:** Vendors must complete ATTESTATION SECTION at bottom of form using digital signature or pdf. Unsigned forms or incomplete forms will be returned.

SECTION 1: SOFTWARE-AS-A-SERVICE (SaaS) / HOSTING / APPLICATION DEVELOPMENT / MANAGED AND PROFESSIONAL SERVICES

No.	Area	Question	Vendor Response	
			YES/NO	Comments
1	**REQUIRED:** Will your organization provide **SOFTWARE-AS-A-SERVICE (SaaS)**?		Yes	
2	**REQUIRED:** Will your organization provide **HOSTING SERVICES**?		Yes	
3	**REQUIRED:** Will your organization provide **APPLICATION DEVELOPMENT SERVICES**?		Yes	This is dependant on scope
4	**REQUIRED:** Will your organization provide **MANAGED OR PROFESSIONAL SERVICES (UNSUPERVISED BY COUNTY PERSONNEL)?** (Note: "Managed or Professional Services" used herein refers to unsupervised (by County personnel) installation, configuration, and maintenance or monitoring of systems, applications or infrastructure related to your organization's proposed solution.)		Yes	
STOP: If you selected NO for Questions 1 through 4 above, **PROCEED TO SECTION 2.**				
5	**Supporting Documentation**	Provide the following: a) Workflow diagram of stored or transmitted information (for SaaS and Hosting Services only)		This requires a signed nda
6		b) Security / Network Architecture diagram (for SaaS and Hosting Services only)	attached	
7		c) Secure Coding standard (for Application Development Services only)		To provide upon award, with clarification of request
8		d) Application Security Program standard (for Application Development Services only)		To provide upon award, with clarification of request

9	**Audit Reporting Requirements**	Does your organization have a current Service Organization Controls (SOC) II, Type II report, inclusive of all five Trust Service Principles (Security, Availability, Processing Integrity, Confidentiality, and Privacy?). (Note: For any SaaS or hosted application, the SOC report should be for the organization or application specifically, not the datacenter only.)	Yes	This is managed my Microsoft Azure
10	**Payment Card Industry (PCI) environments - Applicable only if Organization or its third party partner processes or collects credit card information.**	Does your organization have a current Payment Card Industry (PCI) certification (e.g., Attestation of Compliance (AOC), Self-Assessment Questionnaire (SAQ))?	Yes	
11		Will the product or solution process or collect credit card information?	No	
12		Does your organization maintain a file integrity monitoring program to ensure critical file system changes are monitored and approved with respect to Confidential County data?	No	
13	**Electronic Protected Health Information (ePHI) - Applicable only if Organization has access to or will be hosting or storing County ePHI.**	Has your organization had a Risk Assessment performed in the past 5 years by an external auditor in conjunction with the HIPAA Security rule?	No	
14		Does your organization maintain current HIPAA specific policies and procedures in conjunction with the HIPAA Security Rule?	No	
15		Does your organization have a designated HIPAA Security and Privacy Officer(s)?	No	
16		Does your organization provide HIPAA Security training to your employees at time of hire and at least annually thereafter?	No	
	Roles & Responsibilities	Has your organization appointed a central point of contact for security coordination?	Yes	
18		Does your organization have an expected timeframe to respond to initial contact for security related issues? Provide timeframe.	No	
19		Does your organization define the priority level of an issue (e.g., minor vs. major, 0-4 scale, etc.)? Describe.	No	
20		Does your organization have an expected Service Level Agreement (SLA) to implement changes needed to fix security issues according to priority level? Describe.	Yes	
21	**Federated Identity Management and Web Services Integration**	Does your organization's product have Single Sign-on (SSO) and Federated Identity Enablement integration options (e.g., support for standards like SAML v2 and OAuth 2.0, active directory)? Describe.	No	
22		Does your organization use web services and/or data import/export functions (e.g., API, FTP)? Describe.	Yes	

23	**External Parties**	Will third parties, such as IT service providers have access to the County's data that is stored or transmitted by your organization?	No	
24		Does your organization have Disaster Recovery and Continuity of Operations plans where third-party dependencies are concerned?	Yes	Managed by MS Azure
25		Does your organization outsourcing any aspect of the service to a third party?	No	
26		Does your organization utilize any off-shore resources for development? Provide location(s).	No	
27		Does your organization outsource or build the application in-house?		All development is in-house
28		Does your organization share customer data with or enable direct access by any third-party?	No	
29		Will any third party vendors process, access, transmit or store any County data?	No	
30		Does all third party vendors contractually comply with your organization's security standards for data processing?	NA	
31		Does your organization regularly audit your critical vendors? Describe.	NA	
32	**Information Security Policy & Procedures**	Does your organization have documented standard policies and procedures for security and compliance?	Yes	Managed by MS Azure
	Risk Assessment	Does your organization have a process that addresses: (a) the identification and measurement of potential risks with mitigating controls (measures taken to reduce risk), and (b) the acceptance or transfer (e.g. insurance policies, warranties, etc.) of the remaining (residual) risk after mitigation steps have been applied?	Yes	
34	**Regulatory Compliance**	Is the product or solution currently certified by any security standards? (e.g., PCI-DSS, HIPAA). Provide proof of compliance documentation.		
35		Does your organization have a documented process to identify new laws and regulations with IT security implications (e.g., FIPA, new state breach notification requirements, monitoring newsletters, webinars, security or regulatory forums, etc.)?	Yes	
36		Has your organization experienced a legally reportable data breach within the past 5 years?	No	
37		Does your organization have procedures for preservation of electronic records and audit logs in case of litigation hold?	Yes	Customer data is available for the life of the system.
38	**During Employment – Training, Education &**	Have employees and third party vendors received formal information security awareness training? Provide frequency.	Yes	
39		Have your organization's security policies and procedures been communicated to your employees?	Yes	
40		Are periodic security reminders provided to your organization's employees?	Yes	

41	**Background Checks**	Does your organization perform background checks (e.g., credential verification, criminal history, credit history) to examine and assess an employee’s or third party vendor’s work and criminal history?	Yes	
42		Are individuals who would have access to the County's data subjected to periodic follow-up background checks?	Yes	
43	**Prior to Employment - Terms and Conditions of Employment**	Are employees and third party vendors required to sign a non-disclosure agreement (e.g., non-disclosure and/or confidentiality form upon initial employment)?	Yes	
44		If so, are employees and third party vendors required to sign the non-disclosure agreement annually?	No	
	Termination or Change in Employment	Does your organization require that all equipment of any terminated employee or third party vendor is returned and that his/her user ID is disabled in all systems and badges and/or keys are returned?	Yes	
46		Upon transfer, is existing access reviewed for relevance for employees and third party vendors?	No	
47	**Secure Areas**	Does your organization have effective physical access controls (e.g., door locks, badge /electronic key ID and access controls) in place that prevent unauthorized access to facilities and a facility security plan?	Yes	
48		Do personnel abide by a clean desk policy and lock workstation screens prior to leaving work areas?	Yes	
49		Does your organization have a contingency plan in place to handle emergency access to facilities?	Yes	
50		Are physical access controls authorized? Describe who is responsible for managing and ensuring that only appropriate persons have keys or codes to the facility and to locations within the facility with secure data.	Yes	
51		Are there policies and procedures to document repairs and modifications to physical components of the facility that are related to security?	Yes	
52		Are employees or third party vendors permitted access to customer environments from your physical locations only?	No	
53	**Application and Information Access Control - Confidential System Isolation**	Are systems and networks that host, process, and/or transfer Confidential information "protected" (i.e., isolated, logically or physically separated) from other systems and/or networks?	Yes	
54		Are internal and external networks separated by firewalls with access policies and rules?	Yes	
55		Can your organization restrict access to the solution to and from the County's network in a "deny all, permit by exception" configuration (i.e. whitelist County IP addresses only)?	Yes	

56	**Data Security**	Are development, test, and production environments separated from operational, IT environments to protect production (actively used) applications from inadvertent changes or disruption?	Yes	
57		Does your organization apply database and application logical segregation of customer data?	Yes	
58		Is there a standard approach for protecting network devices to prevent unauthorized access/network related attacks and data-theft (e.g. firewall between public and private networks, internal VLAN, firewall separation, separate WLAN network, secure portal, multi-tenancy, virtualization, shared storage, etc.)?	Yes	
59		Are employees allowed to connect to customer environments remotely (e.g., working from home, public Wi-Fi access)?	NA	Flashparking is a cloud based enviroment which allows access through any computer or mobile device.
60		Is there a remote access policy? Provide documentation.	NA	
61		Does your organization have protections in place for ensuring secure remote access (e.g., up-to-date antivirus, posture assessment, VPN enforcement, split tunneling)?	Yes	
62		Will your organization restrict inbound and outbound traffic to the County network to a “deny all, permit by exception” configuration?	Yes	
63		Is this a multi-tenant solution?	Yes	
64		Will County’s data be co-mingled with any other multi-tenant customer?	No	
65		Will County’s data be processed, accessed, transmitted or stored through an off shore environment (e.g., Outside continental U.S, Alaska, Hawaii)?	No	
66	**Audit Logging**	Does the software or solution perform audit logging? Describe.	Yes	
67		Does the software or solution allow for the configuration of audit log retention for a minimum of 90 days or more?	Yes	
68		Does the software track events for user activity (e.g., failed/successful logins, privileged access)? Describe.	No	
69	**Encryption**	Does your organization provide a means to encrypt County Confidential information in transit? Describe controls that are in place to protect Confidential information when transferred (e.g., encryption).	Yes	Only Credit Card data is encrypte
70		Does your organization use a secure VPN connection with third parties and/or IT vendors for email encryption?	NA	
71		Does your organization provide a means to encrypt data at rest (e.g., AES)?	No	

72	**Vulnerability Assessment and Remediation**	Does your organization perform periodic vulnerability scans on your IT systems, networks, and supporting security systems? Provide frequency.	No	
73		Are internal or third party vulnerability assessments automated?	No	
74		Does your organization have a security patch management cycle in place to address identified vulnerabilities?	Yes	Managed by MS Azure
75		Does your organization provide disclosure of vulnerabilities found in your environment and remediation timelines?	Yes	
76		Does your organization notify customer of applicable patches?		
77	**Security Monitoring**	Are third party connections to your network monitored and reviewed to confirm only authorized access and appropriate usage (e.g., with VPN logs, server event logs, system, application and data access logging, automated alerts, regular/periodic review of logs or reports)?	NA	
78		Does your organization monitor your systems and networks for security events? Describe monitoring (e.g., server and networking equipment logs such as servers, routers, switches, wireless APs, monitored regularly).	Yes	
79		Does your organization periodically review system activity? Provide frequency.	No	Not unless alerted
80	**Identity & Access Management**	Does your organization have a formal access authorization process based on "least privilege" (i.e. employees are granted the least amount of access possible to perform their assigned duties) and "need to know" (e.g., access permissions granted based upon the legitimate business need of the user to access the information, role-based permissions, limited access based on specific responsibilities, network access request form)?	Yes	
81		Are systems and applications configured to restrict access only to authorized individuals (e.g. use of unique IDs and passwords, minimum password length, password complexity, log-in history, lockout, password change, expiration)?	Yes	
82		Is there a list maintained of authorized users with general access and administrative access (e.g., active directory user lists within a Confidential application, a spreadsheet of users, a human resources file)?	Yes	
83		Does your organization maintain a list of "accepted mobile devices" (e.g., smart phones, cell phones) exist and are these devices tracked and managed (e.g., Mobile Device Management)?	No	Customer provides MDM
84		Is a Data Loss Prevention (DLP) in place to prevent the unauthorized distribution of Confidential information?	Yes	
85		Is software installation for desktops, laptops, and servers restricted to administrative users only?	NA	

86		Does software or system have automatic logoff for session inactivity?	Yes	
87		Is access to source application code restricted? Describe how and provide a list of authorized users maintained and updated.	Yes	
88		Are user IDs for your system uniquely identifiable?	Yes	
89		Does your organization have any shared accounts? Describe.	No	
90		Will your organization allow remote access from third party vendors to the County network, with immediate deactivation after use?	No	
91		Can service accounts be configured to run as non-privileged user (i.e. non-Domain Admin)?	NA	
92		Is Multi-Factor Authentication (MFA) required for employees/contractors for remote access to production systems?	No	
93	**Entitlement Reviews**	Does your organization have a process to review user accounts and related access (e.g., manual process of reviewing system accounts to user accounts in AD for both users and privileged access, such as admins, developers, etc.)?	No	
94	**Antivirus**	Is antivirus software installed and running on your computers and supporting systems (e.g., desktops, servers, gateways, etc.)?		
95		Is this antivirus product centrally managed (e.g., is the antivirus monitored to verify all endpoints have functional agents, agents are up to date with the latest signatures, etc.)? Explain your policies and procedures for management of antivirus software.	NA	
96		Does your organization have a process for detecting and reporting malicious software?	NA	Not required on the front end
97	**Network Defense and Host Intrusion Prevention Systems**	Does your organization have any Intrusion Protection System (IPS) in place for your environment?	Yes	Managed by MS Azure
98		Does your organization install personal firewall software on any mobile or employee-owned device?	No	
99	**Media Handling**	Does your organization have procedures to protect documents and computer media (e.g., tapes, disks, hard drives, etc.) from unauthorized disclosure, modification, removal, and destruction?	NA	
100		Is Confidential data encrypted (e.g., data at rest) when stored on laptop, desktop, and server hard drives, flash drives, backup tapes)?	NA	
101	**Secure Disposal**	Are there security procedures (e.g., use of secure wiping, NIST 800-88, etc.) for the decommissioning (replacement) of IT equipment and IT storage devices which contain or process Confidential information?	No	

102	**Separation of Duties**	Are duties separated (e.g., front desk duties separated from accounting, data analysts access separated from IT support), where appropriate, to reduce the opportunity for unauthorized modification, unintentional modification, or misuse of your IT assets?	NA	
103	**Change Management**	Do formal testing and change management procedures exist for networks, systems, desktops, software releases, deployments, and software vulnerability during patching activities, changes to the system, changes to the workstations and servers with appropriate testing, notification, and approval, etc.?	Yes	
104	**Incident Management**	In the event of a major security incident or data breach, do you provide the County a third party digital forensics/incident report?	No	MS Azure may have to ability to produce this
105		Does your organization identify, respond to, and mitigate suspected or known security incidents (e.g., incident form completed as a response to each incident)?	Yes	
106		Does your organization have a formal incident response and data breach notification plan and team?	Yes	Managed by MS Azure
107		Is evidence properly collected and maintained during the investigation of a security incident (e.g., employing chain of custody and other computer forensic methodologies that are monitored by internal and/or external parties)?	No	
108		Are incidents identified, investigated, and reported according to applicable legal requirements?	Yes	
109		Are incidents escalated and communicated? Describe.	Yes	
110		Do you have a contingency plan in place to handle emergency access to the software?	No	
111	**Disaster Recovery Plan & Backups**	Does your organization have a mechanism to back up critical IT systems and Confidential data? Describe.	Yes	Managed by MS Azure
112		Does your organization periodically test your backup/restoration plan by restoring from backup media?	Yes	Managed by MS Azure
113		Does your organization have a disaster recovery plan?	Yes	Managed by MS Azure
114		Are disaster recovery plans updated and tested at least annually?	Yes	Managed by MS Azure
115		Do any single points of failure exist which would disrupt functionality of the product or service?	No	
116	**Product Security Development Lifecycle**	Does your organization have any product pre-release security threat modeling in place (e.g., secure coding practice, security architecture review, penetration testing)?	No	
117		Does your organization maintain end-of-life-schedule for the software product?	No	
118		Is the product engineered as a multi-tier architecture design?	Yes	
119		Is the product or service within 3 year end of life?	No	

120	**Crypto Materials and Key Management**	Does your organization have a centralized key management program in place (e.g., any Public Key Infrastructure (PKI), Hardware Security Module (HSM)-based or not, etc.) to issue certificates needed for products and cloud service infrastructure?	Yes	

121	**Application Development - This section is applicable only if Organization is providing Application Development Services.**	Do your organization's development and testing teams receive training specific to application security? Describe.	Yes	
122		Does your organization follow application security and coding standards and utilize a development framework?	Yes	
123		Does your organization's development team use a development framework? List development languages and framework.	Yes	
124		Will the County receive a copy of the source code?	No	
125		Does your organization review security at each phase of the software development life cycle?	Yes	
126		Does your organization use an industry standard methodology for conducting security testing? Describe.	Yes	
127		Does your organization use an independent 3rd party for periodic security penetration testing?	Yes	Managed by MS Azure
128		Does your organization use automated tools for security testing or code reviews?	Yes	
129		Does your organization perform security testing based on industry standards (e.g. OWASP Top 10, SANS Top 25)?	Yes	Managed by MS Azure
130		Does your organization use SAST and DAST tools to scan code for vulnerabilities prior to production deployment?	Yes	
131		Does your organization perform peer code reviews on source code prior to production deployment?	Yes	
132		Does your organization remediate all vulnerabilities identified prior to production deployment?	Yes	
133		Does your organization have a security methodology for continuous maintenance of the application and applicable components?	Yes	

SECTION 2: SOFTWARE INSTALLED LOCALLY IN COUNTY'S NETWORK

No.	Area	Question	Vendor Response	
			YES/NO	Comments
1	**REQUIRED:** Will your organization provide **SOFTWARE INSTALLED LOCALLY IN COUNTY NETWORK**?		NO	
	STOP: If you selected NO for Question 1, **PROCEED TO SECTION 3.**			
2	**Reseller**	Will your organization act as a reseller to provide software to the County? If so, provide manufacturer documentation regarding the security controls of the software and a secure configuration document.		
3	**Supporting Documentation**	Provide the following: a) Hardware and Software requirements (i.e. Operating System, CPUs, RAM)		
4		b) Network connectivity requirements		
5	**Software Installation Requirements**	Can the application and service accounts used to run the application be configured to run as non-privileged users (e.g. non-Local Administrator rights)		
6		Does software require admin rights to be installed? Describe the level of administrative access the software will need on the County domain.		
7		Is remote access required for installation and support? Describe.		
8		Can the software be installed on and operated in a virtualized environment?		
9	**Third Party Software Requirements**	Is third party software (e.g., Java, Adobe) required to be installed for your software to work? Provide software and minimum version.		
10		Will the software remain compatible with all updates and new releases of required third party software?		
11		Are there contingencies where key third-party dependencies are concerned?		
12	**Secure Software Design/Testing**	Is the software currently certified by any security standards? (e.g., PCI-DSS). Provide standards.		
13		Is security testing performed on product to identify security vulnerabilities (e.g., injection, buffer overflows)?		
14		Has the software been developed following secure programming standards like those in the OWASP Developer Guide?		
15		Is your organization outsourcing any aspect of the service to a third party?		

16		Is the product engineered as a multi-tier architecture design?		
17		Does your organization have capability to respond to and update product for any unforeseen new regulatory requirements?		
18	**Audit Logging**	Does software or solution perform audit logging? Describe.		
19		Does software or solution allow for the configuration of audit log retention for a minimum of 90 days or more?		
20		Does software have audit reporting capabilities (e.g., user activity, privileged access)? Describe.		
21	**Security Updates/Patching**	Does software have a security patch process? Describe your software security patch process, frequency of security patch releases, and how security vulnerabilities are identified.		
22		Does your organization support electronic delivery of digitally signed upgrades?		
23	**Secure Configuration / Installation** **(i.e. PA-DSS configuration)**	Does software allow for secure configuration and installation (e.g., OS hardening, disabling unnecessary services, antivirus compatibility)?		
24		Will software or solution process or collect credit card information?		
25	**Software Upgrade Cycles**	Does software have upgrade cycles? Identify those cycles.		
26	**Confidential Data**	Does software restrict confidential data (e.g., Social Security Number or Date of Birth) from being used as a primary identifier?		
27		Does software have documentation showing where all confidential data is stored in the application?		
28		Does product or solution collect Confidential data (e.g., Social Security Number, Date of Birth, Credit Card information)?		
29	**Encryption**	Does software support encryption of data in motion (e.g., SSL)?		
30		Does software support encryption of data at rest (e.g., column-level encryption, etc.)?		
31		Does software have built-in encryption controls? List controls.		
32	**Authentication**	Does product have Single Sign-on (SSO) and Federated Identity Enablement integration options (e.g., support for standards like SAML v2 and OAuth 2.0, active directory, etc.)? Describe.		
33	**Roles and Responsibilities**	Does software provide role-based access control?		
34		Is a service account required for this software?		
35		If so, does the service account require admin rights?		
36	**Product Security Development Lifecycle**	Does organization have any product pre-release security threat modeling in place (e.g., secure coding practice, security architecture review, penetration testing, etc.)?		
37		Does your organization maintain end-of-life-schedule for the software product?		
38		Is product or service within 3 year end of life?		

39	**Regulatory Compliance**	Is the software or solution currently certified by any security standards (e.g., PCI-DSS, HIPAA)? Provide proof of compliance documentation.		

SECTION 3: HARDWARE

No.	Area	Description	Vendor Response	
			YES/NO	Comments
1	**REQUIRED:** Will your organization provide **HARDWARE**?		Yes	
	STOP: If you selected NO to Question 1, **PROCEED TO SECTION 4.**			
2	**Reseller**	Will your organization act as a reseller to provide hardware products to the County? If so, provide manufacturer documentation regarding the supply chain security controls around the hardware and a secure configuration document.	No	Flashparking manufactures hardware in house
3	**Secure Hardware Design/Testing**	Are there physical security features used to prevent tampering of the hardware? Identify features.	Yes	
4		Is security testing performed on product to identify security vulnerabilities (e.g., injection, buffer overflows)?	Yes	
5		Do you take security measures during the manufacturing of the hardware? Describe.	Yes	
6	**Security Updates/Patching**	Is your hardware scanned to detect any vulnerabilities or backdoors within the firmware?	NA	
7		Has the operating system installed on the hardware been scanned for vulnerabilities?	Yes	
8		Is your firmware upgraded to remediate vulnerabilities? Provide frequency.	NA	
9		If a new vulnerability is identified, is there a documented timeframe for updates/releases? Provide frequency.	NA	
10	**Identity & Access Management**	Are remote control features embedded for the manufacturer's support or ability to remotely access? Describe.	Yes	Logmein
11		Do backdoors exist that can lead to unauthorized access? Describe.	No	

12		Do default accounts exist? List all default accounts.	No	
13		Can default accounts and passwords be changed by Broward County?	No	
14		Can service accounts be configured to run as non-privileged user (i.e. non-Domain Admin)?	Ni	
15	**Confidential Data**	Does the product or solution collect Confidential data (e.g., Social Security Number, Date of Birth, Credit Card information)?	No	
16	**Roles and Responsibilities**	Is a service account required for this hardware?	No	
17		If so, does the service account require admin rights?		
18	**Product Security Development Lifecycle**	Is an end-of-life schedule maintained for the hardware?	No	
19		Is product or service within 3 year end of life?	No	
20	**Media Handling**	Does your organization have a secure data wipe and data destruction program for proper drive disposal (e.g., Certificate of destruction, electronic media purging)? Describe.	NA	No data is stored locally on the hardware
21	**Regulatory Compliance**	Is the hardware currently certified by any security standards? (e.g., PCI-DSS, HIPAA). Provide proof of compliance documentation.	Yes	Hardware is a component of our fully compliant level 1 pci certification
22		Will product or solution process or collect credit card information?	Yes	We process credit transactions but never store or pass that data through our syste. CCs are encrypted at the head.
23		Does your organization have a process to identify new laws and regulations with IT security implications?	No	

SECTION 4: ATTESTATION SECTION - AL VENDORS MUST FULLY COMPLeTE AND SIGN THIS SECTION.

I possess the authority to sign and act as an agent on behalf of this organization. I have read the above questionnaire in its entirety and responded in a truthful manner to the best of my ability.

Vendor Name:	FlashParking, Inc
Printed Representative Name:	Sam Goodner
Printed Representative Title:	Chief Strategy Officer
Signature:	
Date:	3/5/2020

PNC2119994R1, Parking Access and Revenue Control Equipment and Maintenance

Name of Firm:

PCI Responsibility Matrix

		Responsibility of				
Requirement	**Requirement Text**	**N/A**	**Provider/ Vendor**	**County**	**Joint**	**Notes**
1.1	Establish and implement firewall and router configuration standards that include the following:				X	
1.1.1	A formal process for approving and testing all network connections and changes to the firewall and router configurations				X	
1.1.2	Current diagram that identifies all networks, network devices, and system components, with all connections between the CDE and other networks, including any wireless networks				X	
1.1.3	Current diagram that shows all cardholder data flows across systems and networks	X				
1.1.4	Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone				X	
1.1.5	Description of groups, roles, and responsibilities for management of network components				X	
1.1.6	Documentation and business justification for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure.				X	
1.1.7	Requirement to review firewall and router rule sets at least every six months	X				
1.2	Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder				X	

PCI Responsibility Matrix

		Responsibility of				
Requirement	**Requirement Text**	**N/A**	**Provider/ Vendor**	**County**	**Joint**	**Notes**
	data environment. Note: An "untrusted network" is any network that is external to the networks belonging to the entity under review, and/or which is out of the entity's ability to control or manage.				X	
1.2.1	Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic.				X	
1.2.2	Secure and synchronize router configuration files.	X				
1.2.3	Install perimeter firewalls between all wireless networks and the cardholder data environment, and configure these firewalls to deny or, if traffic is necessary for business purposes, permit only authorized traffic between the wireless environment and the cardholder data environment.				X	
1.3	Prohibit direct public access between the Internet and any system component in the cardholder data environment.				X	
1.3.1	Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.				X	
1.3.2	Limit inbound Internet traffic to IP addresses within the DMZ.				X	
1.3.3	Implement anti-spoofing measures to detect and block forged source IP addresses from entering the network.				X	

PCI Responsibility Matrix

		Responsibility of				
Requirement	**Requirement Text**	**N/A**	**Provider/ Vendor**	**County**	**Joint**	**Notes**
	(For example, block traffic originating from the Internet with an internal source address.)				X	
1.3.4	Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet.				X	
1.3.5	Permit only "established" connections into the network.				X	
1.3.6	Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks.	X				
1.3.7	Do not disclose private IP addresses and routing information to unauthorized parties. Note: Methods to obscure IP addressing may include, but are not limited to: • Network Address Translation (NAT) • Placing servers containing cardholder data behind proxy servers/firewalls, • Removal or filtering of route advertisements for private networks that employ registered addressing • Internal use of RFC1918 address space instead of registered addresses.				X	
1.4	Install personal firewall software equivalent functionality on any portable computing devices (including company and/or employee-owned) that connect to the Internet when outside the network (for example, laptops used by employees), and which are also used to access			X		

PCI Responsibility Matrix

		Responsibility of				
Requirement	Requirement Text	N/A	Provider/ Vendor	County	Joint	Notes
	the CDE. Firewall (or equivalent) configurations include: • Specific configuration settings are defined for personal firewall software. • Personal firewall software (or equivalent functionality) is actively running. • Personal firewall (or equivalent functionality) is not alterable by users of mobile and/or employee-owned devices.			X		
1.5	Ensure that security policies and operational procedures for managing firewalls are documented, in use, and known to all affected parties.				X	
2.1	Always change vendor-supplied defaults and remove or disable unnecessary default accounts before installing a system on the network. This applies to ALL default passwords, including but not limited to those used by operating systems, software that provides security services, application and system accounts, point-of-sale (POS) terminals, Simple Network Management Protocol (SNMP) community strings, etc.).				X	
2.1.1	For wireless environments connected to the cardholder data environment or transmitting cardholder data, change ALL wireless vendor defaults at installation, including but not limited to default wireless encryption keys, passwords, and SNMP community strings.				X	

PCI Responsibility Matrix

		Responsibility of				
Requirement	**Requirement Text**	**N/A**	**Provider/ Vendor**	**County**	**Joint**	**Notes**
2.2	Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards. Sources of industry-accepted system hardening standards may include, but are not limited to: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) Institute • National Institute of Standards Technology (NIST).				X	
2.2.1	Implement only one primary function per server to prevent functions that require different security levels from co-existing on the same server. (For example, web servers, database servers, and DNS should be implemented on separate servers.) Note: Where virtualization technologies are in use, implement only one primary function per virtual system component.				X	
2.2.2	Enable only necessary services, protocols, daemons, etc., as required for the function of the system.				X	

PNC2119994R1, Parking Access and Revenue Control Equipment and Maintenance

PCI Responsibility Matrix

		Responsibility of				
Requirement	**Requirement Text**	**N/A**	**Provider/ Vendor**	**County**	**Joint**	**Notes**
2.2.3	Implement additional security features for any required services, protocols, or daemons that are considered to be insecure.				X	
2.2.4	Configure system security parameters to prevent misuse.				X	
2.2.5	Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.				X	
2.3	Encrypt all non-console administrative access using strong cryptography.				X	
2.4	Maintain an inventory of system components that are in scope for PCI DSS.				X	
2.5	Ensure that security policies and operational procedures for managing vendor defaults and other security parameters are documented, in use, and known to all affected parties.				X	
2.6	Shared hosting providers must protect each entity's hosted environment and cardholder data. These providers must meet specific requirements as detailed in Appendix A: Additional PCI DSS Requirements for Shared Hosting Providers.				X	
3.1	Keep cardholder data storage to a minimum by implementing data retention and disposal policies, procedures and processes that include at least the following for all cardholder data (CHD) storage: • Limiting data storage amount and retention time to that which is required for legal,	X				

PCI Responsibility Matrix

		Responsibility of				
Requirement	**Requirement Text**	**N/A**	**Provider/ Vendor**	**County**	**Joint**	**Notes**
	regulatory, and business requirements • Processes for secure deletion of data when no longer needed • Specific retention requirements for cardholder data • A quarterly process for identifying and securely deleting stored cardholder data that exceeds defined retention.	X				
3.2	Do not store sensitive authentication data after authorization (even if encrypted). If sensitive authentication data is received, render all data unrecoverable upon completion of the authorization process. *It is permissible for issuers and companies that support issuing services to store sensitive authentication data if:* *• There is a business justification and* *• The data is stored secur*ely. Sensitive authentication data includes the data as cited in the following Requirements 3.2.1 through 3.2.3:		X			
3.2.1	Do not store the full contents of any track (from the magnetic stripe located on the back of a card, equivalent data contained on a chip, or elsewhere) after authorization. This data is alternatively called full track, track, track 1, track 2, and magnetic-stripe data. *Note: In the normal course of business, the*					

PCI Responsibility Matrix

		Responsibility of				
Requirement	**Requirement Text**	**N/A**	**Provider/ Vendor**	**County**	**Joint**	**Notes**
	following data elements from the magnetic stripe may need to be retained: *• The cardholder's name* *• Primary account number (PAN)* *• Expiration date* *• Service code* *To minimize risk, store only these data elements as needed for business.*		X			
3.2.2	Do not store the card verification code or value (three-digit or four-digit number printed on the front or back of a payment card used to verify card-not-present transactions) after authorization.	X				
3.2.3	Do not store the personal identification number (PIN) or the encrypted PIN block after authorization.		X			
3.3	Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed), such that only personnel with a legitimate business need can see more than the first six/last four digits of the PAN. Note: This requirement does not supersede stricter requirements in place for displays of cardholder data—for example, legal or payment card brand requirements for point- of-sale (POS) receipts.	X				
3.4	Render PAN unreadable anywhere it is stored (including on portable digital media, backup	X				

PCI Responsibility Matrix

		Responsibility of				
Requirement	**Requirement Text**	**N/A**	**Provider/ Vendor**	**County**	**Joint**	**Notes**
	media, and in logs) by using any of the following approaches: • One-way hashes based on strong cryptography, (hash must be of the entire PAN) • Truncation (hashing cannot be used to replace the truncated segment of PAN) • Index tokens and pads (pads must be securely stored) • Strong cryptography with associated key-management processes and procedures. Note: It is a relatively trivial effort for a malicious individual to reconstruct original PAN data if they have access to both the truncated and hashed version of a PAN. Where hashed and truncated versions of the same PAN are present in an entity's environment, additional controls should be in place to ensure that the hashed and truncated versions cannot be correlated to reconstruct the original PAN.					
3.4.1	If disk encryption is used (rather than file or column-level database encryption), logical access must be managed separately and independently of native operating system authentication and access control mechanisms (for example, by not using local user account databases or general network login credentials). Decryption keys must not be associated with user accounts. *Note: This requirement applies in addition to all*	X				

PCI Responsibility Matrix

		Responsibility of				
Requirement	**Requirement Text**	**N/A**	**Provider/ Vendor**	**County**	**Joint**	**Notes**
	other PCI DSS encryption and key-management requirements.					
3.5	Document and implement procedures to protect keys used to secure stored cardholder data against disclosure and misuse: *Note: This requirement applies to keys used to encrypt stored cardholder data, and also applies to key-encrypting keys used to protect data-encrypting keys—such key- encrypting keys must be at least as strong as the data-encrypting key.*		X			
3.5.1	Additional requirement for service providers only: Maintain a documented description of the cryptographic architecture that includes: • Details of all algorithms, protocols, and keys used for the protection of cardholder data, including key strength and expiry date • Description of the key usage for each key. • Inventory of any HSMs and other SCDs used for key management		X			
3.5.2	Restrict access to cryptographic keys to the fewest number of custodians necessary.		X			
3.5.3	Store secret and private keys used to encrypt/decrypt cardholder data in one (or more) of the following forms at all times: • Encrypted with a key-encrypting key that is at least as strong as the data-encrypting key, and that is stored separately from the data-encrypting key				X	

PCI Responsibility Matrix

		Responsibility of				
Requirement	**Requirement Text**	**N/A**	**Provider/ Vendor**	**County**	**Joint**	**Notes**
	• Within a secure cryptographic device (such as a hardware (host) security module (HSM) or PTS-approved point-of-interaction device) • As at least two full-length key components or key shares, in accordance with an industry-accepted method *Note: It is not required that public keys be stored in one of these forms.*				X	
3.5.4	Store cryptographic keys in the fewest possible locations.		X			
3.6	Fully document and implement all key-management processes and procedures for cryptographic keys used for encryption of cardholder data, including the following: *Note: Numerous industry standards for key management are available from various resources including NIST, which can be found at http://csrc.nist.gov.*	X				
3.6.1	Generation of strong cryptographic keys	X				
3.6.2	Secure cryptographic key distribution	X				
3.6.3	Secure cryptographic key storage	X				
3.6.4	Cryptographic key changes for keys that have reached the end of their cryptoperiod (for example, after a defined period of time has passed and/or after a certain amount of cipher-text has been produced by a given key), as defined by the associated application Provider/Vendor or key owner, and based on	X				

PCI Responsibility Matrix

		Responsibility of				
Requirement	**Requirement Text**	**N/A**	**Provider/ Vendor**	**County**	**Joint**	**Notes**
	industry best practices and guidelines (for example, NIST Special Publication 800-57).					
3.6.5	Retirement or replacement (for example, archiving, destruction, and/or revocation) of keys as deemed necessary when the integrity of the key has been weakened (for example, departure of an employee with knowledge of a clear-text key component), or keys are suspected of being compromised. *Note: If retired or replaced cryptographic keys need to be retained, these keys must be securely archived (for example, by using a key-encryption key). Archived cryptographic keys should only be used for decryption/verification purposes.*	X				
3.6.6	If manual clear-text cryptographic key-management operations are used, these operations must be managed using split knowledge and dual control. *Note: Examples of manual key-management operations include, but are not limited to: key generation, transmission, loading, storage and destruction.*	X				
3.6.7	Prevention of unauthorized substitution of cryptographic keys.	X				
3.6.8	Requirement for cryptographic key custodians to formally acknowledge that they understand and accept their key- custodian responsibilities.	X				

PNC2119994R1, Parking Access and Revenue Control Equipment and Maintenance

PCI Responsibility Matrix

		Responsibility of				
Requirement	**Requirement Text**	**N/A**	**Provider/ Vendor**	**County**	**Joint**	**Notes**
3.7	Ensure that security policies and operational procedures for protecting stored cardholder data are documented, in use, and known to all affected parties.		X			
4.1	Use strong cryptography and security protocols (for example, TLS, IPSEC, SSH, etc.) to safeguard sensitive cardholder data during transmission over open, public networks, including the following: • Only trusted keys and certificates are accepted. • The protocol in use only supports secure versions or configurations. • The encryption strength is appropriate for the encryption methodology in use. *Examples of open, public networks include but are not limited to:* *• The Internet* *• Wireless technologies, including 802.11 and Bluetooth* *• Cellular technologies, for example, Global System for Mobile communications (GSM), Code division multiple access (CDMA)* *• General Packet Radio Service (GPRS).* *• Satellite communications.*		X			
4.1.1	Ensure wireless networks transmitting cardholder data or connected to the cardholder data environment, use industry best practices to implement strong encryption for authentication and transmission.		X			

PCI Responsibility Matrix

		Responsibility of				
Requirement	**Requirement Text**	**N/A**	**Provider/ Vendor**	**County**	**Joint**	**Notes**
4.2	Never send unprotected PANs by end-user messaging technologies (for example, e- mail, instant messaging, SMS, chat, etc.).				X	
4.3	Ensure that security policies and operational procedures for encrypting transmissions of cardholder data are documented, in use, and known to all affected parties.		X			
5.1	Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers).	X				
5.1.1	Ensure that anti-virus programs are capable of detecting, removing, and protecting against all known types of malicious software.	X				
5.1.2	For systems considered to be not commonly affected by malicious software, perform periodic evaluations to identify and evaluate evolving malware threats in order to confirm whether such systems continue to not require anti-virus software.	X				
5.2	Ensure that all anti-virus mechanisms are maintained as follows: • Are kept current, • Perform periodic scans • Generate audit logs which are retained per PCI DSS Requirement 10.7.	X				
5.3	Ensure that anti-virus mechanisms are actively running and cannot be disabled or altered by users, unless specifically authorized by management on a case-by- case basis for a	X				

PCI Responsibility Matrix

		Responsibility of				
	Requirement Text	**N/A**	**Provider/ Vendor**	**County**	**Joint**	**Notes**
	limited time period. *Note: Anti-virus solutions may be temporarily disabled only if there is legitimate technical need, as authorized by management on a case-by-case basis. If anti- virus protection needs to be disabled for a specific purpose, it must be formally authorized. Additional security measures may also need to be implemented for the period of time during which anti-virus protection is not active.*					
5.4	Ensure that security policies and operational procedures for protecting systems against malware are documented, in use, and known to all affected parties.				X	
6.1	Establish a process to identify security vulnerabilities, using reputable outside sources for security vulnerability information, and assign a risk ranking (for example, as “high,” “medium,” or “low”) to newly discovered security vulnerabilities. *Note: Risk rankings should be based on industry best practices as well as consideration of potential impact. For example, criteria for ranking vulnerabilities may include consideration of the CVSS base score, and/or the classification by the vendor, and/or type of systems affected. Methods for evaluating vulnerabilities and*				X	

PCI Responsibility Matrix

		Responsibility of				
Requirement	**Requirement Text**	**N/A**	**Provider/ Vendor**	**County**	**Joint**	**Notes**
	assigning risk ratings will vary based on an organization's environment and risk-assessment strategy. Risk rankings should, at a minimum, identify all vulnerabilities considered to be a "high risk" to the environment. In addition to the risk ranking, vulnerabilities may be considered "critical" if they pose an imminent threat to the environment, impact critical systems, and/or would result in a potential compromise if not addressed. Examples of critical systems may include security systems, public-facing devices and systems, databases, and other systems that store, process, or transmit cardholder data.					
6.2	Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor-supplied security patches. Install critical security patches within one month of release. *Note: Critical security patches should be identified according to the risk ranking process defined in Requirement 6.1.*		X			
6.3	Develop internal and external software applications (including web-based administrative access to applications) securely, as follows: • In accordance with PCI DSS (for example, secure authentication and logging) • Based on industry standards and/or best practices. • Incorporating information security throughout		X			

PCI Responsibility Matrix

		Responsibility of				
Requirement	Requirement Text	N/A	Provider/ Vendor	County	Joint	Notes
	the software-development life cycle Note: this applies to all software developed internally as well as bespoke or custom software developed by a third party.					
6.3.1	Remove development, test and/or custom application accounts, user IDs, and passwords before applications become active or are released to County.		X			
6.3.2	Review custom code prior to release to production or County in order to identify any potential coding vulnerability (using either manual or automated processes) to include at least the following: • Code changes are reviewed by individuals other than the originating code author, and by individuals knowledgeable about code- review techniques and secure coding practices. • Code reviews ensure code is developed according to secure coding guidelines • Appropriate corrections are implemented prior to release. Note: This requirement for code reviews applies to all custom code (both internal and public-facing), as part of the system development life cycle. Code reviews can be conducted by knowledgeable internal personnel or third parties. Public-facing web applications are also subject to additional controls, to address ongoing		X			

PCI Responsibility Matrix

		Responsibility of				
Requirement	Requirement Text	N/A	Provider/ Vendor	County	Joint	Notes
	threats and vulnerabilities after implementation, as defined at PCI DSS Requirement 6.6.					
6.4	Follow change control processes and procedures for all changes to system components. The processes must include the following:		X			
6.4.1	Separate development/test environments from production environments, and enforce the separation with access controls.		X			
6.4.2	Separation of duties between development/test and production environments		X			
6.4.3	Production data (live PANs) are not used for testing or development		X			
6.4.4	Removal of test data and accounts before production systems become active		X			
6.4.5	Change control procedures for the implementation of security patches and software modifications must include the following:				X	
6.4.5.1	Documentation of impact.				X	
6.4.5.2	Documented change approval by authorized parties.				X	
6.4.5.3	Functionality testing to verify that the change does not adversely impact the security of the system.				X	
6.4.5.4	Back-out procedures.				X	
6.4.6	Upon completion of a significant change, all relevant PCI DSS requirements must be implemented on all new or changed systems and networks, and documentation updated as applicable.		X			

PCI Responsibility Matrix

		Responsibility of				
Requirement	**Requirement Text**	**N/A**	**Provider/ Vendor**	**County**	**Joint**	**Notes**
6.5	Address common coding vulnerabilities in software-development processes as follows: • Train developers in secure coding techniques, including how to avoid common coding vulnerabilities, and understanding how sensitive data is handled in memory. • Develop applications based on secure coding guidelines. Note: The vulnerabilities listed at 6.5.1 through 6.5.10 were current with industry best practices when this version of PCI DSS was published. However, as industry best practices for vulnerability management are updated (for example, the OWASP Guide, SANS CWE Top 25, CERT Secure Coding, etc.), the current best practices must be used for these requirements.		X			
6.5.1	Injection flaws, particularly SQL injection. Also consider OS Command Injection, LDAP and XPath injection flaws as well as other injection flaws.		X			
6.5.2	Buffer overflows				X	
6.5.3	Insecure cryptographic storage	X				
6.5.4	Insecure communications	X				
6.5.5	Improper error handling	X				
6.5.6	All "high risk" vulnerabilities identified in the vulnerability identification process (as defined in PCI DSS Requirement 6.1).				X	
6.5.7	Cross-site scripting (XSS)	X				

PCI Responsibility Matrix

		Responsibility of				
Requirement	**Requirement Text**	**N/A**	**Provider/ Vendor**	**County**	**Joint**	
6.5.8	Improper access control (such as insecure direct object references, failure to restrict URL access, directory traversal, and failure to restrict user access to functions).				X	
6.5.9	Cross-site request forgery (CSRF)				X	
6.5.10	Broken authentication and session management		X			
6.6	For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks by either of the following methods: • Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes Note: This assessment is not the same as the vulnerability scans performed for Requirement 11.2. • Installing an automated technical solution that detects and prevents web- based attacks (for example, a web- application firewall) in front of public- facing web applications, to continually check all traffic.				X	

PNC2119994R1, Parking Access and Revenue Control Equipment and Maintenance

PCI Responsibility Matrix

		Responsibility of				
Requirement	**Requirement Text**	**N/A**	**Provider/ Vendor**	**County**	**Joint**	**Notes**
6.7	Ensure that security policies and operational procedures for developing and maintaining secure systems and applications are documented, in use, and known to all affected parties.				X	
7.1	Limit access to system components and cardholder data to only those individuals whose job requires such access.				X	
7.1.1	Define access needs for each role, including: • System components and data resources that each role needs to access for their job function • Level of privilege required (for example, user, administrator, etc.) for accessing resources.				X	
7.1.2	Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities.				X	
7.1.3	Assign access based on individual personnel's job classification and function.				X	
7.1.4	Require documented approval by authorized parties specifying required privileges.				X	
7.2	Establish an access control system for systems components that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed. This access control system must include the following:	X				
7.2.1	Coverage of all system components	X				
7.2.2	Assignment of privileges to individuals based on job classification and function.	X				
7.2.3	Default "deny-all" setting.	X				

PCI Responsibility Matrix

		Responsibility of				
Requirement	**Requirement Text**	**N/A**	**Provider/ Vendor**	**County**	**Joint**	**Notes**
7.3	Ensure that security policies and operational procedures for restricting access to cardholder data are documented, in use, and known to all affected parties.	X				
8.1	Define and implement policies and procedures to ensure proper user identification management for non- consumer users and administrators on all system components as follows:	X				
8.1.1	Assign all users a unique ID before allowing them to access system components or cardholder data.	X				
8.1.2	Control addition, deletion, and modification of user IDs, credentials, and other identifier objects.				X	
8.1.3	Immediately revoke access for any terminated users.			X		
8.1.4	Remove/disable inactive user accounts within 90 days.			X		
8.1.5	Manage IDs used by Provider/Vendors to access, support, or maintain system components via remote access as follows: • Enabled only during the time period needed and disabled when not in use. • Monitored when in use.			X		
8.1.6	Limit repeated access attempts by locking out the user ID after not more than six attempts.	X				
8.1.7	Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID.	X				

PCI Responsibility Matrix

		Responsibility of				
Requirement	**Requirement Text**	**N/A**	**Provider/ Vendor**	**County**	**Joint**	**Notes**
8.1.8	If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.		X			
8.2	In addition to assigning a unique ID, ensure proper user-authentication management for non-consumer users and administrators on all system components by employing at least one of the following methods to authenticate all users: • Something you know, such as a password or passphrase • Something you have, such as a token device or smart card • Something you are, such as a biometric.	X				
8.2.1	Using strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components.	X				
8.2.2	Verify user identity before modifying any authentication credential—for example, performing password resets, provisioning new tokens, or generating new keys.			X		
8.2.3	Passwords/phrases must meet the following: • Require a minimum length of at least seven characters. • Contain both numeric and alphabetic characters. Alternatively, the passwords/phrases must have	X				

PCI Responsibility Matrix

		Responsibility of				
Requirement	Requirement Text	N/A	Provider/ Vendor	County	Joint	Notes
8.2.4	Change user passwords/passphrases at least once every 90 days.	X				
8.2.5	Do not allow an individual to submit a new password/phrase that is the same as any of the last four passwords/phrases he or she has used.	X				
8.2.6	Set passwords/phrases for first-time use and upon reset to a unique value for each user, and change immediately after the first use.	X				
8.3	Secure all individual non-console administrative access and all remote access to the CDE using multi-factor authentication. *Note: Multi-factor authentication requires that a minimum of two of the three authentication methods (see Requirement 8.2 for descriptions of authentication methods) be used for authentication. Using one factor twice (for example, using two separate passwords) is not considered multi- factor authentication*	X				
8.3.1	Incorporate multi-factor authentication for all non-console access into the CDE for personnel with administrative access.	X				
8.3.2	Incorporate multi-factor authentication for all remote network access (both user and administrator, and including third party access for support or maintenance) originating from outside the entity's network.	X				

PNC2119994R1, Parking Access and Revenue Control Equipment and Maintenance

PCI Responsibility Matrix						
		Responsibility of				
Requirement	**Requirement Text**	**N/A**	**Provider/ Vendor**	**County**	**Joint**	**Notes**
8.4	Document and communicate authentication procedures and policies to all users including: • Guidance on selecting strong authentication credentials • Guidance for how users should protect their authentication credentials • Instructions not to reuse previously used passwords • Instructions to change passwords if there is any suspicion the password could be compromised.	X				
8.5	Do not use group, shared, or generic IDs, passwords, or other authentication methods as follows: • Generic user IDs are disabled or removed. • Shared user IDs do not exist for system administration and other critical functions. • Shared and generic user IDs are not used to administer any system components.	X				
8.5.1	Additional requirement for service providers only: Service providers with remote access to County premises (for example, for support of POS systems or servers) must use a unique authentication credential (such as a password/phrase) for each customer. *Note: This requirement is not intended to apply to shared hosting providers accessing their own hosting environment, where multiple customer environments are hosted.*	X				

PCI Responsibility Matrix

		Responsibility of				
Requirement	**Requirement Text**	**N/A**	**Provider/ Vendor**	**County**	**Joint**	**Notes**
8.6	Where other authentication mechanisms are used (for example, physical or logical security tokens, smart cards, certificates, etc.), use of these mechanisms must be assigned as follows: • Authentication mechanisms must be assigned to an individual account and not shared among multiple accounts. • Physical and/or logical controls must be in place to ensure only the intended account can use that mechanism to gain access.	X				
8.7	All access to any database containing cardholder data (including access by applications, administrators, and all other users) is restricted as follows: • All user access to, user queries of, and user actions on databases are through programmatic methods. • Only database administrators have the ability to directly access or query databases. • Application IDs for database applications can only be used by the applications (and not by individual users or other non- application processes).	X				
8.8	Ensure that security policies and operational procedures for identification and authentication are documented, in use, and known to all affected parties.			X		

PCI Responsibility Matrix

		Responsibility of				
Requirement	**Requirement Text**	**N/A**	**Provider/ Vendor**	**County**	**Joint**	**Notes**
9.1	Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment.			X		
9.1.1	Use video cameras and/or access control mechanisms to monitor individual physical access to sensitive areas. Review collected data and correlate with other entries. Store for at least three months, unless otherwise restricted by law. *Note: "Sensitive areas" refers to any data center, server room or any area that houses systems that store, process, or transmit cardholder data. This excludes public-facing areas where only point-of-sale terminals are present, such as the cashier areas in a retail store.*			X		
9.1.2	Implement physical and/or logical controls to restrict access to publicly accessible network jacks. For example, network jacks located in public areas and areas accessible to visitors could be disabled and only enabled when network access is explicitly authorized. Alternatively, processes could be implemented to ensure that visitors are escorted at all times in areas with active network jacks.				X	
9.1.3	Restrict physical access to wireless access points, gateways, handheld devices, networking/communications hardware, and telecommunication lines.			X		

PCI Responsibility Matrix

		Responsibility of				
Requirement	**Requirement Text**	**N/A**	**Provider/ Vendor**	**County**	**Joint**	**Notes**
9.2	Develop procedures to easily distinguish between onsite personnel and visitors, to include: • Identifying onsite personnel and visitors (for example, assigning badges) • Changes to access requirements • Revoking or terminating onsite personnel and expired visitor identification (such as ID badges).			X		
9.3	Control physical access for onsite personnel to the sensitive areas as follows: • Access must be authorized and based on individual job function. • Access is revoked immediately upon termination, and all physical access mechanisms, such as keys, access cards, etc., are returned or disabled.			X		
9.4.x	Implement procedures to identify and authorize visitors. Procedures should include the following:			X		
9.4.1	Visitors are authorized before entering, and escorted at all times within, areas where cardholder data is processed or maintained.			X		
9.4.2	Visitors are identified and given a badge or other identification that expires and that visibly distinguishes the visitors from onsite personnel.			X		
9.4.3	Visitors are asked to surrender the badge or identification before leaving the facility or at the date of expiration.			X		

PCI Responsibility Matrix

		Responsibility of				
Requirement	**Requirement Text**	**N/A**	**Provider/ Vendor**	**County**	**Joint**	**Notes**
9.4.4	A visitor log is used to maintain a physical audit trail of visitor activity to the facility as well as computer rooms and data centers where cardholder data is stored or transmitted. Document the visitor’s name, the firm represented, and the onsite personnel authorizing physical access on the log. Retain this log for a minimum of three months, unless otherwise restricted by law.			X		
9.5	Physically secure all media.				X	
9.5.1	Store media backups in a secure location, preferably an off-site facility, such as an alternate or backup site, or a commercial storage facility. Review the location’s security at least annually.	X				
9.6	Maintain strict control over the internal or external distribution of any kind of media, including the following:				X	
9.6.1	Classify media so the sensitivity of the data can be determined.				X	
9.6.2	Send the media by secured courier or other delivery method that can be accurately tracked.	X				
9.6.3	Ensure management approves any and all media that is moved from a secured area (including when media is distributed to individuals).	X				
9.7	Maintain strict control over the storage and accessibility of media.	X				
9.7.1	Properly maintain inventory logs of all media and conduct media inventories at least annually.	X				

PCI Responsibility Matrix

		Responsibility of				
Requirement	**Requirement Text**	**N/A**	**Provider/ Vendor**	**County**	**Joint**	**Notes**
9.8	Destroy media when it is no longer needed for business or legal reasons as follows:	X				
9.8.1	Shred, incinerate, or pulp hard-copy materials so that cardholder data cannot be reconstructed. Secure storage containers used for materials that are to be destroyed.	X				
9.8.2	Render cardholder data on electronic media unrecoverable so that cardholder data cannot be reconstructed.	X				
9.9	Protect devices that capture payment card data via direct physical interaction with the card from tampering and substitution. Note: These requirements apply to card- reading devices used in card-present transactions (that is, card swipe or dip) at the point of sale. This requirement is not intended to apply to manual key-entry components such as computer keyboards and POS keypads.			X		
9.9.1	Maintain an up-to-date list of devices. The list should include the following: • Make, model of • Location of device (for example, the address of the site or facility where the device is located) • Device serial number or other method of unique identification.				X	
9.9.2	Periodically inspect device surfaces to detect tampering (for example, addition of card skimmers to devices), or substitution (for			X		

PCI Responsibility Matrix

		Responsibility of				
Requirement	**Requirement Text**	**N/A**	**Provider/ Vendor**	**County**	**Joint**	**Notes**
	example, by checking the serial number or other device characteristics to verify it has not been swapped with a fraudulent device). Note: Examples of signs that a device might have been tampered with or substituted include unexpected attachments or cables plugged into the device, missing or changed security labels, broken or differently colored casing, or changes to the serial number or other external markings.			X		
9.9.3	Provide training for personnel to be aware of attempted tampering or replacement of devices. Training should include the following: • Verify the identity of any third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices. • Do not install, replace, or return devices without verification. • Be aware of suspicious behavior around devices (for example, attempts by unknown persons to unplug or open devices). • Report suspicious behavior and indications of device tampering or substitution to appropriate personnel (for example, to a manager or security officer).			X		
9.1	Ensure that security policies and operational procedures for restricting physical access to cardholder data are documented, in use, and known to all affected parties.	X				

PCI Responsibility Matrix

		Responsibility of				
Requirement	**Requirement Text**	**N/A**	**Provider/ Vendor**	**County**	**Joint**	**Notes**
10.1	Implement audit trails to link all access to system components to each individual user.				X	
10.2	Implement automated audit trails for all system components to reconstruct the following events:				X	
10.2.1	All individual user accesses to cardholder data	X				
10.2.2	All actions taken by any individual with root or administrative privileges	X				
10.2.3	Access to all audit trails				X	
10.2.4	Invalid logical access attempts	X				
10.2.5	Use of and changes to identification and authentication mechanisms—including but not limited to creation of new accounts and elevation of privileges—and all changes, additions, or deletions to accounts with root or administrative privileges	X				
10.2.6	Initialization, stopping, or pausing of the audit logs	X				
10.2.7	Creation and deletion of system-level objects				X	
10.3	Record at least the following audit trail entries for all system components for each event:					
10.3.1	User identification		X			
10.3.2	Type of event		X			
10.3.3	Date and time		X			
10.3.4	Success or failure indication		X			
10.3.5	Origination of event	X				
10.3.6	Identity or name of affected data, system component, or resource.	X				
10.4	Using time-synchronization technology, synchronize all critical system clocks and times		X			

PCI Responsibility Matrix

		Responsibility of				
Requirement	**Requirement Text**	**N/A**	**Provider/ Vendor**	**County**	**Joint**	**Notes**
	and ensure that the following is implemented for acquiring, distributing, and storing time. *Note: One example of time synchronization technology is Network Time Protocol (NTP).*					
10.4.1	Critical systems have the correct and consistent time.		X			
10.4.2	Time data is protected.		X			
10.4.3	Time settings are received from industry-accepted time sources.		X			
10.5	Secure audit trails so they cannot be altered.		X			
10.5.1	Limit viewing of audit trails to those with a job-related need.		X			
10.5.2	Protect audit trail files from unauthorized modifications.		X			
10.5.3	Promptly back up audit trail files to a centralized log server or media that is difficult to alter.	X				
10.5.4	Write logs for external-facing technologies onto a secure, centralized, internal log server or media device.	X				
10.5.5	Use file-integrity monitoring or change- detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).	X				
10.6	Review logs and security events for all system components to identify anomalies or suspicious activity. Note: Log harvesting, parsing, and alerting tools may be used to meet this Requirement.			X		

PCI Responsibility Matrix

		Responsibility of				
Requirement	**Requirement Text**	**N/A**	**Provider/ Vendor**	**County**	**Joint**	**Notes**
10.6.1	Review the following at least daily: • All security events • Logs of all system components that store, process, or transmit CHD and/or SAD, or that could impact the security of CHD and/or SAD • Logs of all critical system components • Logs of all servers and system components that perform security functions (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, e- commerce redirection servers, etc.).			X		
10.6.2	Review logs of all other system components periodically based on the organization's policies and risk management strategy, as determined by the organization's annual risk assessment.				X	
10.6.3	Follow up exceptions and anomalies identified during the review process.				X	
10.7	Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from backup).				X	
10.8	Additional requirement for service providers only: Implement a process for the timely detection and reporting of failures of critical security control systems, including but not limited to failure of: • Firewalls • IDS/IPS				X	

PCI Responsibility Matrix

		Responsibility of				
Requirement	**Requirement Text**	**N/A**	**Provider/ Vendor**	**County**	**Joint**	**Notes**
	• FIM • Anti-virus • Physical access controls • Logical access controls • Audit logging mechanisms • Segmentation controls (if used)					
10.8.1	Additional requirement for service providers only: Respond to failures of any critical security controls in a timely manner. Processes for responding to failures in security controls must include: • Restoring security functions • Identifying and documenting the duration (date and time start to end) of the security failure • Identifying and documenting cause(s) of failure, including root cause, and documenting remediation required to address root cause • Identifying and addressing any security issues that arose during the failure • Performing a risk assessment to determine whether further actions are required as a result of the security failure • Implementing controls to prevent cause of failure from reoccurring • Resuming monitoring of security controls		X			
10.9	Ensure that security policies and operational procedures for monitoring all access to network				X	

PNC2119994R1, Parking Access and Revenue Control Equipment and Maintenance

PCI Responsibility Matrix

		Responsibility of				
Requirement	**Requirement Text**	**N/A**	**Provider/ Vendor**	**County**	**Joint**	**Notes**
	resources and cardholder data are documented, in use, and known to all affected parties.					
11.1	Implement processes to test for the presence of wireless access points (802.11), and detect and identify all authorized and unauthorized wireless access points on a quarterly basis. Note: Methods that may be used in the process include but are not limited to wireless network scans, physical/logical inspections of system components and infrastructure, network access control (NAC), or wireless IDS/IPS. Whichever methods are used, they must be sufficient to detect and identify both authorized and unauthorized devices.	X				
11.1.1	Maintain an inventory of authorized wireless access points including a documented business justification.				X	
11.1.2	Implement incident response procedures in the event unauthorized wireless access points are detected.			X		
11.2	Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades). Note: Multiple scan reports can be combined for the quarterly scan process to show that all				X	

PCI Responsibility Matrix

		Responsibility of				
Requirement	**Requirement Text**	**N/A**	**Provider/ Vendor**	**County**	**Joint**	**Notes**
	systems were scanned and all applicable vulnerabilities have been addressed. Additional documentation may be required to verify non-remediated vulnerabilities are in the process of being addressed. For initial PCI DSS compliance, it is not required that four quarters of passing scans be completed if the assessor verifies 1) the most recent scan result was a passing scan, 2) the entity has documented policies and procedures requiring quarterly scanning, and 3) vulnerabilities noted in the scan results have been corrected as shown in a re-scan(s). For subsequent years after the initial PCI DSS review, four quarters of passing scans must have occurred.					
11.2.1	Perform quarterly internal vulnerability scans and rescans as needed, until all “high- risk” vulnerabilities (as identified in Requirement 6.1) are resolved. Scans must be performed by qualified personnel.				X	
11.2.2	Perform quarterly external vulnerability scans, via an Approved Scanning Provider/Vendor (ASV) approved by the Payment Card Industry Security Standards Council (PCI SSC). Perform rescans as needed, until passing scans are achieved. Note: Quarterly external vulnerability scans must				X	

PCI Responsibility Matrix

		Responsibility of				
Requirement	**Requirement Text**	**N/A**	**Provider/ Vendor**	**County**	**Joint**	**Notes**
	be performed by an Approved Scanning Provider/Vendor (ASV), approved by the Payment Card Industry Security Standards Council (PCI SSC). Refer to the ASV Program Guide published on the PCI SSC website for scan County responsibilities, scan preparation, etc.					
11.2.3	Perform internal and external scans, and rescans as needed, after any significant change. Scans must be performed by qualified personnel.				X	
11.3	Implement a methodology for penetration testing that includes the following: • Is based on industry-accepted penetration testing approaches (for example, NIST SP800-115) • Includes coverage for the entire CDE perimeter and critical systems • Includes testing from both inside and outside the network • Includes testing to validate any segmentation and scope-reduction controls • Defines application-layer penetration tests to include, at a minimum, the vulnerabilities listed in Requirement 6.5 • Defines network-layer penetration tests to include components that support network functions as well as operating systems				X	

PCI Responsibility Matrix

		Responsibility of				
Requirement	**Requirement Text**	**N/A**	**Provider/ Vendor**	**County**	**Joint**	**Notes**
	• Includes review and consideration of threats and vulnerabilities experienced in the last 12 months • Specifies retention of penetration testing results and remediation activities results. Note: This update to Requirement 11.3 is a best practice until June 30, 2015, after which it becomes a requirement. PCI DSS v2.0 requirements for penetration testing must be followed until v3.0 is in place.					
11.3.1	Perform external penetration testing at least annually and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment).				X	
11.3.2	Perform internal penetration testing at least annually and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment).				X	
11.3.3	Exploitable vulnerabilities found during penetration testing are corrected and testing is repeated to verify the corrections.				X	
11.3.4	If segmentation is used to isolate the CDE from other networks, perform penetration tests at least annually and after any changes to				X	

PCI Responsibility Matrix

		Responsibility of				
Requirement	**Requirement Text**	**N/A**	**Provider/ Vendor**	**County**	**Joint**	**Notes**
	segmentation controls/methods to verify that the segmentation methods are operational and effective, and isolate all out- of-scope systems from systems in the CDE.					
11.3.4.1	Additional requirement for service providers only: If segmentation is used, confirm PCI DSS scope by performing penetration testing on segmentation controls at least every six months and after any changes to segmentation controls/methods.				X	
11.4	Use intrusion-detection and/or intrusion-prevention techniques to detect and/or prevent intrusions into the network. Monitor all traffic at the perimeter of the cardholder data environment as well as at critical points in the cardholder data environment, and alert personnel to suspected compromises. Keep all intrusion-detection and prevention engines, baselines, and signatures up to date.				X	
11.5	Deploy a change-detection mechanism (for example, file-integrity monitoring tools) to alert personnel to unauthorized modification (including changes, additions, and deletions) of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly.			X		
11.5.1	Implement a process to respond to any alerts generated by the change-detection solution.			X		
11.6						

PCI Responsibility Matrix

		Responsibility of				
Requirement	Requirement Text	N/A	Provider/ Vendor	County	Joint	Notes
	Ensure that security policies and operational procedures for security monitoring and testing are documented, in use, and known to all affected parties.					
12.1	Establish, publish, maintain, and disseminate a security policy.			X		
12.1.1	Review the security policy at least annually and update the policy when the environment changes.			X		
12.2	Implement a risk-assessment process that: -Is performed at least annually and upon significant changes to the environment (for example, acquisition, merger, relocation, etc.), -Identifies critical assets, threats, and vulnerabilities, and -Results in a formal, documented analysis of risk.				X	
12.3	Develop usage policies for critical technologies and define proper use of these technologies. Note: Examples of critical technologies include, but are not limited to, remote access and wireless technologies, laptops, tablets, removable electronic media, e-mail usage and Internet usage. Ensure these usage policies require the following:			X		
12.3.1	Explicit approval by authorized parties			X		
12.3.2	Authentication for use of the technology			X		
12.3.3	A list of all such devices and personnel with access			X		

PCI Responsibility Matrix

		Responsibility of				
Requirement	**Requirement Text**	**N/A**	**Provider/ Vendor**	**County**	**Joint**	**Notes**
12.3.4	A method to accurately and readily determine owner, contact information, and purpose (for example, labeling, coding, and/or inventorying of devices)				X	
12.3.5	Acceptable uses of the technology				X	
12.3.6	Acceptable network locations for the technologies				X	
12.3.7	List of company-approved products				X	
12.3.8	Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity				X	
12.3.9	Activation of remote-access technologies for vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use				X	
12.3.10	For personnel accessing cardholder data via remote-access technologies, prohibit the copying, moving, and storage of cardholder data onto local hard drives and removable electronic media, unless explicitly authorized for a defined business need. Where there is an authorized business need, the usage policies must require the data be protected in accordance with all applicable PCI DSS Requirements.	X				
12.4	Ensure that the security policy and procedures clearly define information security responsibilities for all personnel.			X		

PCI Responsibility Matrix

		Responsibility of				
Requirement	**Requirement Text**	**N/A**	**Provider/ Vendor**	**County**	**Joint**	**Notes**
12.4.1	Additional requirement for service providers only: Executive management shall establish responsibility for the protection of cardholder data and a PCI DSS compliance program to include: • Overall accountability for maintaining PCI DSS compliance • Defining a charter for a PCI DSS compliance program and communication to executive management				X	
12.5	Assign to an individual or team the following information security management responsibilities:			X		
12.5.1	Establish, document, and distribute security policies and procedures.			X		
12.5.2	Monitor and analyze security alerts and information, and distribute to appropriate personnel.			X		
12.5.3	Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations.				X	
12.5.4	Administer user accounts, including additions, deletions, and modifications.			X		
12.5.5	Monitor and control all access to data.			X		
12.6	Implement a formal security awareness program to make all personnel aware of the importance of cardholder data security.			X		

PCI Responsibility Matrix

		Responsibility of				
Requirement	**Requirement Text**	**N/A**	**Provider/ Vendor**	**County**	**Joint**	**Notes**
12.6.1	Educate personnel upon hire and at least annually. Note: Methods can vary depending on the role of the personnel and their level of access to the cardholder data.			X		
12.6.2	Require personnel to acknowledge at least annually that they have read and understood the security policy and procedures.			X		
12.7	Screen potential personnel prior to hire to minimize the risk of attacks from internal sources. (Examples of background checks include previous employment history, criminal record, credit history, and reference checks.) Note: For those potential personnel to be hired for certain positions such as store cashiers who only have access to one card number at a time when facilitating a transaction, this requirement is a recommendation only.			X		
12.8	Maintain and implement policies and procedures to manage service providers with whom cardholder data is shared, or that could affect the security of cardholder data, as follows:				X	
12.8.1	Maintain a list of service providers.				X	
12.8.2	Maintain a written agreement that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess or otherwise store, process or transmit on behalf of the County, or to the extent that they could impact the security of				X	

PCI Responsibility Matrix

		Responsibility of				
Requirement	**Requirement Text**	**N/A**	**Provider/ Vendor**	**County**	**Joint**	**Notes**
	the County's cardholder data environment. *Note: The exact wording of an acknowledgement will depend on the agreement between the two parties, the details of the service being provided, and the responsibilities assigned to each party. The acknowledgement does not have to include the exact wording provided in this requirement.*					
12.8.3	Ensure there is an established process for engaging service providers including proper due diligence prior to engagement.				X	
12.8.4	Maintain a program to monitor service providers' PCI DSS compliance status at least annually.			X		
12.8.5	Maintain information about which PCI DSS requirements are managed by each service provider, and which are managed by the entity.				X	
12.9	Additional requirement for service providers only: Service providers acknowledge in writing to County that they are responsible for the security of cardholder data the service provider possesses or otherwise stores, processes, or transmits on behalf of the County, or to the extent that they could impact the security of the County's cardholder data environment. *Note: The exact wording of an acknowledgement will depend on the agreement between the two parties, the details of the service being provided, and the responsibilities assigned to each party.*				X	

PCI Responsibility Matrix

		Responsibility of				
Requirement	**Requirement Text**	**N/A**	**Provider/ Vendor**	**County**	**Joint**	**Notes**
	The acknowledgement does not have to include the exact wording provided in this requirement.					
12.1	Implement an incident response plan. Be prepared to respond immediately to a system breach.				X	
12.10.1	Create the incident response plan to be implemented in the event of system breach. Ensure the plan addresses the following, at a minimum: • Roles, responsibilities, and communication and contact strategies in the event of a compromise including notification of the payment brands, at a minimum • Specific incident response procedures • Business recovery and continuity procedures • Data backup processes • Analysis of legal requirements for reporting compromises • Coverage and responses of all critical system components • Reference or inclusion of incident response procedures from the payment brands.				X	
12.10.2	Test the plan at least annually.			X		
12.10.3	Designate specific personnel to be available on a 24/7 basis to respond to alerts.				X	
12.10.4	Provide appropriate training to staff with security breach response responsibilities.				X	

PCI Responsibility Matrix

		Responsibility of				
Requirement	**Requirement Text**	**N/A**	**Provider/ Vendor**	**County**	**Joint**	**Notes**
12.10.5	Include alerts from security monitoring systems, including but not limited to intrusion-detection, intrusion-prevention, firewalls, and file-integrity monitoring systems.				X	
12.10.6	Develop a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments.			X		
12.11	Additional requirement for service providers only: Perform reviews at least quarterly to confirm personnel are following security policies and operational procedures. Reviews must cover the following processes: • Daily log reviews • Firewall rule-set reviews • Applying configuration standards to new systems • Responding to security alerts • Change management processes				X	
12.11.1	Additional requirement for service providers only: Maintain documentation of quarterly review process to include: • Documenting results of the reviews • Review and sign off of results by personnel assigned responsibility for the PCI DSS compliance program				X	

PCI Responsibility Matrix

		Responsibility of				
Requirement	**Requirement Text**	**N/A**	**Provider/ Vendor**	**County**	**Joint**	**Notes**
A.1	Protect each entity's (that is, merchant, service provider, or other entity) hosted environment and data, per A.1.1 through A.1.4: A hosting provider must fulfill these requirements as well as all other relevant sections of the PCI DSS. Note: Even though a hosting provider may meet these requirements, the compliance of the entity that uses the hosting provider is not guaranteed. Each entity must comply with the PCI DSS and validate compliance as applicable.				X	
A.1.1	Ensure that each entity only runs processes that have access to that entity's cardholder data environment.				X	
A.1.2	Restrict each entity's access and privileges to its own cardholder data environment only.				X	
A.1.3	Ensure logging and audit trails are enabled and unique to each entity's cardholder data environment and consistent with PCI DSS Requirement 10.				X	
A.1.4	Enable processes to provide for timely forensic investigation in the event of a compromise to any hosted merchant or service provider.			X		

AGREEMENT EXCEPTION FORM

The completed form(s) should be returned with the Vendor's submittal. If not provided with submittal, it shall be deemed an affirmation by the Vendor that it accepts the terms and conditions of the County's Agreement as disclosed in the solicitation.

The Vendor must either provide specific proposed alternative language on the form below. Additionally, a brief justification specifically addressing each provision to which an exception is taken should be provided.

There are no exceptions to the terms and conditions of the County Agreement as referenced in the solicitation; or

☆ The following exceptions are disclosed below: (use additional forms as needed; separate each Article/ Section number)

Term or Condition Article / Section	Insert version of exception or specific proposed alternative language	Provide brief justification for change
3.2.1. Software License.	Remove this section entirely.	FlashParking is providing the Country a SaaS subscription, not an installed software solution. Section 3.2.2 (Subscription rights) applies.
3.5 Updates, Upgrades and Releases	Remove the words "with advance notice"	FlashParking is constantly updating the hosting system and cannot provide advance notice to its customers.
3.9 Escrow Agreement	Remove this section entirely	FlashParking will not place its source code in escrow.
5.7 Foreign Entity Tax Withholding	Remove this section entirely	FlashParking is a US company
8.4 ADA Compliance	Remove this section entirely	While FlashParking parking equipment (kiosks) are ADA compliant, the software portal used by the County's employees is not Section 504 certified.
NEW section 6.3	Add the following section 6.3 Delivery; Risk of Loss. Contractor shall arrange, with County's full cooperation as requested by Contractor and at County's cost, the delivery of Equipment to the County facility where it is to be installed. The method of shipment and carrier shall be selected by Contractor unless County has specified in writing a method of shipment and carrier prior to shipment. If Contractor selects the carrier, upon delivery at the	FlashParking will ship the equipment to County's location approximately one week before our installation crew arrives onsite to install and commission the parking equipment. We ask that the County receive and store those boxes in a secure location during that time.

	County-designated facility, the title to and the risk of loss for the Equipment shall pass to County and, thereafter, the risk of loss for the Equipment shall be borne by County. If County elects to specify the carrier, title to and the risk of loss for the Equipment shall pass to County upon consignment to the carrier and, thereafter, the risk of loss for the Equipment shall be borne by County. It is recommended, since County bears the risk of loss or damage of the Equipment on-site, that County provide a secure, weather-controlled storage facility to store the Equipment prior to its installation.	
Exhibit A 9. Final Acceptance Test Plan	Remove No. 2 ADA Compliance	Same as 8.4 above.

Vendor Name: FlashParking, Inc.

Broward County Board of County Commissioners
PNC2119994R1

PROPOSAL BOND

This form must be completed and submitted with the Vendor's submittal. Failure to comply will deem vendor non-responsive.

BY THIS BOND, we FlashParking, Inc., as Principal, hereinafter called VENDOR, and SureTec Insurance Company, as Surety, are bound to the Board of County Commissioners of Broward County, Florida, as Obligee, hereinafter called County, in the Amount of Ten thousand and no/100 dollars----- ($10,000.00*) for the payment whereof VENDOR and surety bind themselves, their heirs, executors, administrators, successors and assigns, jointly and severally.

WHEREAS, the County is seeking to contract with a firm (registered with the Florida Department of State, Division of Corporations) for the County agencies; and

WHEREAS, the County is utilizing a request for proposals (RFP) solicitation process for this project and VENDOR in response to Solicitation No. PNC2119994R1 agrees and is bound that:

The CONDITION OF THIS BOND is that if:

VENDOR submits a timely proposal in response to the County's solicitation process; THEN THIS BOND WILL REMAIN IN FULL FORCE AND EFFECT UNTIL CONTRACT AWARD. If the VENDOR is awarded the Agreement, but fails to enter into the Agreement, (including providing a Performance and Payment Guaranty, evidence of insurance, and other requirements stated herein) then the VENDOR and surety, jointly and severally, shall be liable to the County for the full sum herein stated which shall be due and payable to the County immediately upon demand of the County, in good and lawful money of the United States of America; as liquidated damages for failure thereof of said VENDOR; OTHERWISE THE BOND SHALL REMAIN IN FULL FORCE AND EFFECT.

No right of action shall accrue on this bond to or for the use of any person or corporation other than County named herein; and

In the event suit is brought upon this bond by the County, surety shall pay reasonable attorneys' fees and costs incurred by the County in such suit.

12/ /2020 2:22 PM
p. 63

Broward County Board of
County Commissioners

Bid PNC2119994R1

Signed and sealed this 4th day of March, 2020.

WITNESSES:

Secretary

(CORPORATE SEAL)

FlashParking, Inc.
(Name of Corporation)

By CEO
(Signature and Title)

Lan Sharplin CEO
(Type Name and Title Signed Above)

IN THE PRESENCE OF:

Teresa Martin

Teresa Martin, Witness

SURETY COMPANY:
SureTec Insurance Company

By Carol Fonville
Agent and Attorney-in-Fact, Carol Fonville

Address: 9737 Great Hills Trail, Suite 32
(Street)

Austin, TX 78759
(City/State/Zip Code)

Telephone No.: 866-732-0099

12/30/2019 2:22 PM

p. 64

CERTIFICATE AS TO CORPORATE PRINCIPAL

I, Juan Rodriguez, certify that I am the Secretary of the corporation named as Principal in the foregoing Proposal Bond; that Dan Sharplin, who signed the Bond on behalf of the Principal, was then CEO of said corporation; that I know his/her signature; and his/her signature thereto is genuine; and that said Bond was duly signed, sealed and attested to on behalf of said corporation by authority of its governing body.

_______________(Seal) as
Secretary of

____
(Name of Corporation)

(SEAL)

STATE OF ~~FLORIDA~~ TEXAS)
) SS.
COUNTY OF ~~BROWARD~~ TRAVIS)

Before me, a Notary Public duly commissioned, qualified and acting personally, appeared Juan Rodriguez to me well known, who being by me first duly sworn upon oath says that he/she has been authorized to execute the foregoing Proposal Bond on behalf of VENDOR named therein in favor of COUNTY.

Subscribed and Sworn to before me this 4th day of March, 20 20.

My commission expires:

June 19, 2022

____
Notary Public, State of ~~Florida at Large~~ TEXAS

AMANDA CHINN
Notary Public, State of Texas
Comm. Expires 06-19-2022
Notary ID 131610531

Bonded by_______________

POA #: 4221009

SureTec Insurance Company

LIMITED POWER OF ATTORNEY

Know All Men by These Presents, That SURETEC INSURANCE COMPANY (the "Company"), a corporation duly organized and existing under the laws of the State of Texas, and having its principal office in Houston, Harris County, Texas, does by these presents make, constitute and appoint

Connie Grocholski, Carol Fonville

its true and lawful Attorney-in-fact, with full power and authority hereby conferred in its name, place and stead, to execute, acknowledge and deliver any and all bonds, recognizances, undertakings or other instruments or contracts of suretyship to include waivers to the conditions of contracts and consents of surety for, providing the bond penalty does not exceed

Five Million and 00/100 Dollars ($5,000,000.00)

and to bind the Company thereby as fully and to the same extent as if such bond were signed by the CEO, sealed with the corporate seal of the Company and duly attested by its Secretary, hereby ratifying and confirming all that the said Attorney-in-Fact may do in the premises. Said appointment is made under and by authority of the following resolutions of the Board of Directors of the SureTec Insurance Company:

> *Be it Resolved,* that the President, any Vice-President, any Assistant Vice-President, any Secretary or any Assistant Secretary shall be and is hereby vested with full power and authority to appoint any one or more suitable persons as Attorney(s)-in-Fact to represent and act for and on behalf of the Company subject to the following provisions:
>
> *Attorney-in-Fact* may be given full power and authority for and in the name of and of behalf of the Company, to execute, acknowledge and deliver, any and all bonds, recognizances, contracts, agreements or indemnity and other conditional or obligatory undertakings and any and all notices and documents canceling or terminating the Company's liability thereunder, and any such instruments so executed by any such Attorney-in-Fact shall be binding upon the Company as if signed by the President and sealed and effected by the Corporate Secretary.
>
> *Be it Resolved,* that the signature of any authorized officer and seal of the Company heretofore or hereafter affixed to any power of attorney or any certificate relating thereto by facsimile, and any power of attorney or certificate bearing facsimile signature or facsimile seal shall be valid and binding upon the Company with respect to any bond or undertaking to which it is attached. *(Adopted at a meeting held on 20th of April, 1999.)*

In Witness Whereof, SURETEC INSURANCE COMPANY has caused these presents to be signed by its CEO, and its corporate seal to be hereto affixed this 16th day of October , A.D. 2019 .

SURETEC INSURANCE COMPANY

SURETEC INSURANCE COMPANY TEXAS

By: ______________________
John Knox Jr., CEO

State of Texas ss:
County of Harris

On this 16th day of October , A.D. 2019 before me personally came John Knox Jr., to me known, who, being by me duly sworn, did depose and say, that he resides in Houston, Texas, that he is CEO of SURETEC INSURANCE COMPANY, the company described in and which executed the above instrument; that he knows the seal of said Company; that the seal affixed to said instrument is such corporate seal; that it was so affixed by order of the Board of Directors of said Company; and that he signed his name thereto by like order.

JACQUELYN GREENLEAF
Notary Public, State of Texas
Comm. Expires 05-18-2021
Notary ID 126903029

NOTARY PUBLIC STATE OF TEXAS

Jacquelyn Greenleaf, Notary Public
My commission expires May 18, 2021

I, M. Brent Beaty, Assistant Secretary of SURETEC INSURANCE COMPANY, do hereby certify that the above and foregoing is a true and correct copy of a Power of Attorney, executed by said Company, which is still in full force and effect; and furthermore, the resolutions of the Board of Directors, set out in the Power of Attorney are in full force and effect.

Given under my hand and the seal of said Company at Houston, Texas this 4TH day of MARCH , 2020 , A.D.

M. Brent Beaty, Assistant Secretary

Any instrument issued in excess of the penalty stated above is totally void and without any validity.
For verification of the authority of this power you may call (713) 812-0800 any business day between 8:30 am and 5:00 pm CST.

SureTec Insurance Company

THIS BOND RIDER CONTAINS IMPORTANT COVERAGE INFORMATION

Statutory Complaint Notice/Filing of Claims

To obtain information or make a complaint: You may call the Surety's toll free telephone number for information or to make a complaint or file a claim at: 1-866-732-0099. You may also write to the Surety at:

SureTec Insurance Company
9737 Great Hills Trail, Suite 320
Austin, Tx 78759

You may contact the Texas Department of Insurance to obtain information on companies, coverage, rights or complaints at 1-800-252-3439. You may write the Texas Department of Insurance at

PO Box 149104
Austin, TX 78714-9104
Fax#: 512-490-1007
Web: http://www.tdi.state.tx.us
Email: ConsumerProtection@tdi.texas.gov

PREMIUM OR CLAIM DISPUTES: Should you have a dispute concerning your premium or about a claim, you should contact the Surety first. If the dispute is not resolved, you may contact the Texas Department of Insurance.

FlashParking POWERING THE PARKING EVOLUTION

In compliance with Addendum # 8, FlashParking Inc will submit proof of required electrical licensing within three days of County's written request. Work performed for this solicitation will be performed by a licensed contractor or subcontractor as required.

Statement of Financial Stability

FlashParking has been cashflow positive since 2014 and continues to grow at 100% year over year. With that said, FlashParking made the strategic decision in 2019 to raise capital to fuel our growth even further. The $60M investment will be used to scale FlashParking's industry-leading extensible, cloud-based parking system that enables 21st-century parking and the evolution of isolated parking assets into connected mobility hubs.

We have included audited financials from 2017-2018 in a separate attachment, which must remain confidential per **Florida Statute Chapter 119.**

Per Chapter 119.07:

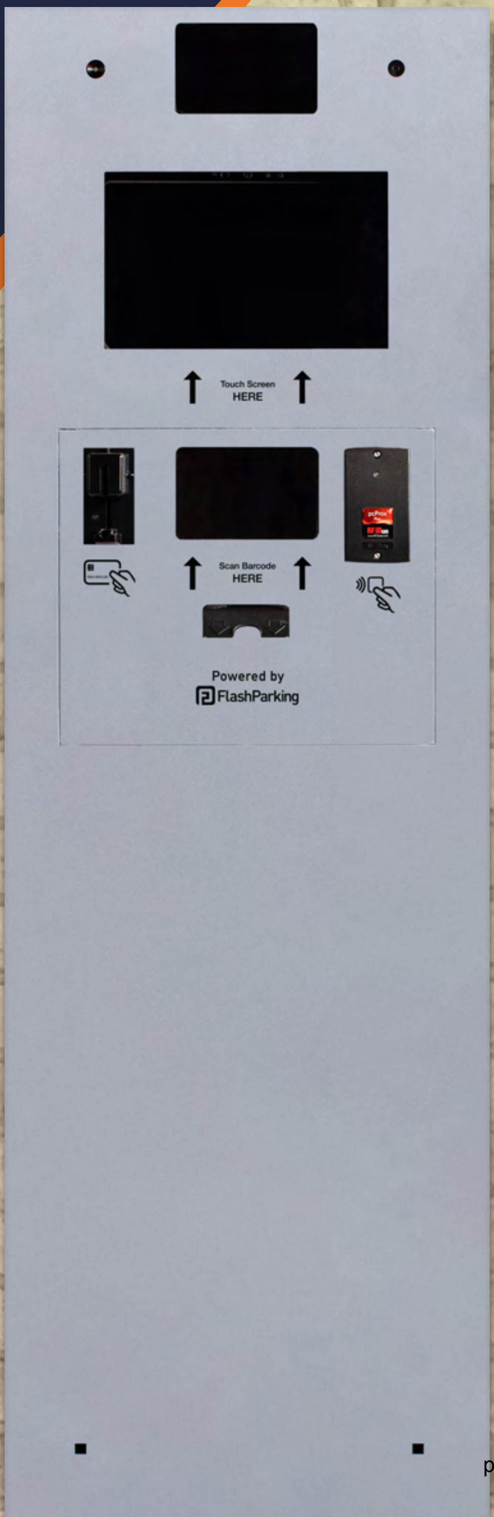
Any financial statement that an agency requires a prospective bidder to submit in order to prequalify for bidding or for responding to a proposal for a road or any other public works project is exempt from s. 119.07(1) and s. 24(a), Art. I of the State Constitution.

Additionally, FlashParking can provide financials from 2019 and any necessary licensing upon request. FlashParking's Contractor's Score, which rates us as "excellent" before raising the capital, is also available upon request.

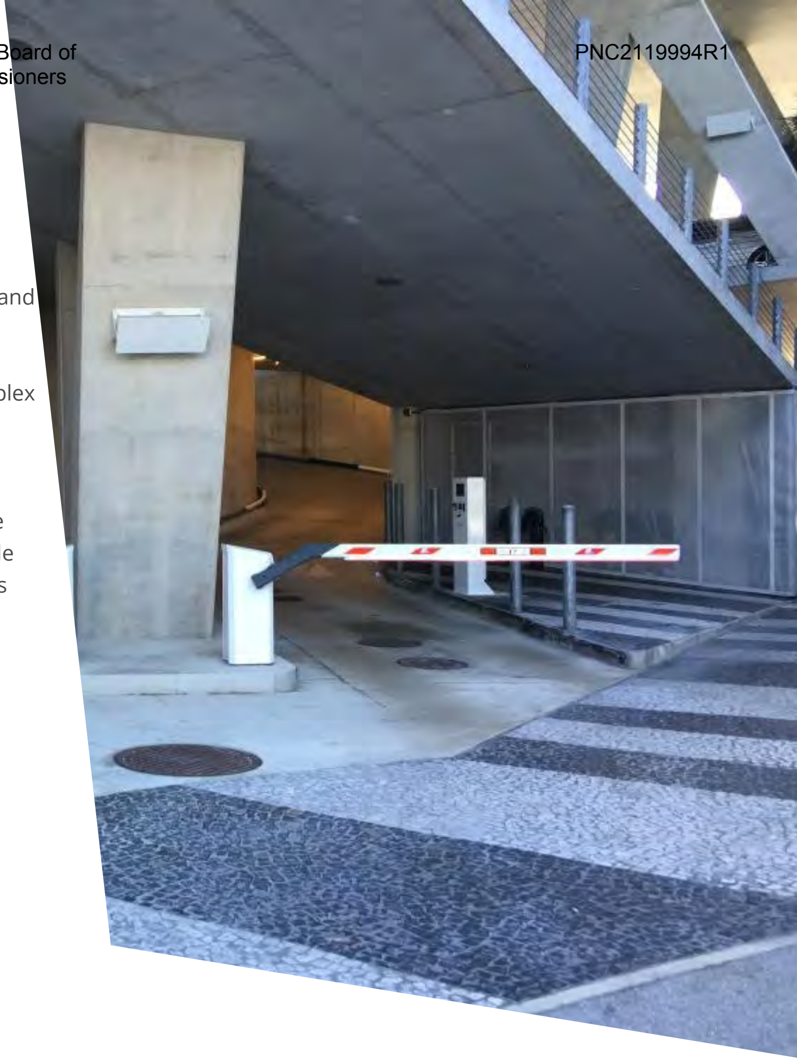
FlashPARCS

YOUR TOTAL REVENUE ACCESS CONTROL SOLUTION

FlashPARCS offers the most advanced cloud-based PARCS solution for any venue type and size. From overnight hotel parking and monthly parking in office buildings to complex mixed-use developments and event parking, FlashPARCS allows you to manage and maximize your operation from a desktop, tablet, or mobile phone.



OVERVIEW



At FlashParking, our mission is simple: to perfect the parking experience. The parking industry has been dominated by complicated, unreliable technology and processes for too long. I'm sure you agree—your guests deserve more!

From overnight hotel parking and monthly parking in office buildings to complex mixed-use developments and event parking, you can manage access and revenue control the way your customers demand with FlashPARCS.

Our touch-screen Smart Stations coupled with a cloud-based platform enable parking operators and asset owners to increase revenue and asset value while giving guests a better parking experience. Our mobile-first architecture allows you to manage your operations from the palm of your hands.

FlashPARCS is also part of FlashParking's fully integrated parking ecosystem, which delivers a unified platform for all our solutions:

- **FlashValet** (valet and event parking)
- **FlashMobile** (mobile payments)

So no matter what your parking needs are, we have you covered!

BENEFITS

1 Machine for ALL Your Needs

Identical kiosk can be configured for entry, exit, pay-on-foot, multi-space, and more.

Self-Serve Maintenance

All components are part of plug-and-play (USB-based) system to enusure maximum uptime.

FlashCare Maintenance Kit

Kit includes major replacement parts, minimizes downtime and reduces your maintenance cost.

Cash Acceptance

FlashPARCS offers two types of cash acceptance options: Bill Note Recycler and exact change only.

Monthly Parker Module

The module offers an array of access options; guests can create and manage account online.

Award-Winning Platform

Named "100 Most Brilliant Companies" by Inc. Magazine.

Worry-free PCI Compliance

Let the only Level 1 Service Provider in the industry assume 98% of your PCI responsibilities.

Seamless Integrations

Integrated with top hotel PMS, online parking reservation, legacy PARCS systems, and more.

Real-time Business Intelligence

Access to over 100+ reports accessible via phone, tablet, or browser.

All Across the U.S.

Our Smart Stations are up and running all across the U.S.

WHY YOU'LL LOVE US?

We're different! As the only born-in-the-cloud parking technology provider in the industry, FlashParking is committed to perfecting the parking experience for the customer as well as parking operators and asset owners. With FlashPARCS you can expect:

- One platform for ALL your parking needs: valet, PARCS, monthly, event, and more
- A reliable, award-winning platform
- Real-time visibility over operations
- Increase profits through better revenue control
- On-demand and scheduled reports
- Seamless integrations with Hotel PMS, eParking reservations systems, electronic validations and more
- Fast deployment
- On-screen advertising opportunities
- The ability to change rates from your mobile phone in real-time

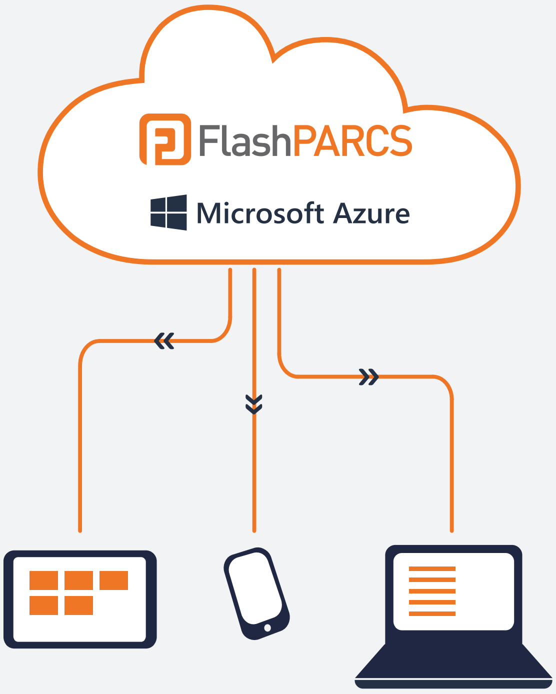
WHY YOUR GUESTS WILL LOVE US?

Guest impressions start and end at the garage entrance. FlashPARCS was built with your guests as the top priority. The minute a guest pulls up to your property, we help you deliver a "forgettable" parking experience that will leave them smiling from features like:

- Numerous options to gain entry and exit via: AVI, LPR, Prox/RFID cards, credit cards, mobile phone, or paper ticket
- Intuitive and easy-to-use user interface
- Convenient payment options like credit card, mobile payment, or cash
- Fully integrated with eParking reservation systems
- Cash acceptance options
- Member/VIP parker program
- Validation types include: electronic, text, or printed
- Service maintenance allows operators to quickly address equipment issues, thus ensuring better ingress/egress time

PLATFORM WITH **REAL-TIME OPERATIONS VISIBILITY**

- Ability to see operations in real-time via phone or browser
- Access to over 100+ business intelligence analytic reports
- Ability to fully customize reporting
- Visibility and control over revenue (no matter what tender)
- Simple tracking of credit card payments, eParking reservations, electronic validations, and more
- Automated and scheduled reporting



EQUIPMENT **BRIEFING**

Built on our innovative cloud-based architecture, FlashPARCS is designed with simplicity and usability as key priorities. Highly configurable to meet your unique facility requirements, you can expect the following:

- ✓ **Transparent equipment purchasing process with no hidden fees**
- ✓ **Low CAPEX costs minimize steep start-up fees**
- ✓ **No expensive maintenance contracts; software updates are included**
- ✓ **Easy maintenance with plug-and-play (USB-based) PARCS parts**
- ✓ **Physical kiosk is identical no matter the configuration which makes for no-fuss maintenance**
- ✓ **A maintenance kit that contains replacements for all major components so operators can quickly replace parts with minimal downtime**

HEADQUARTERS
FlashParking
3801 S. Capital of Texas Highway, Suite 250
Austin, TX 78704

SALES
sales@flashparking.com
800.213.3706

SUPPORT
support@flashparking.com
888.737.7465

FlashValet

YOUR TOTAL VALET AND EVENT PARKING SOLUTION

FlashValet offers the most advanced cloud-based valet and event parking solution for any venue type and size. From hourly rates and validations to vehicle pictures and time/attendance, FlashValet allows you to manage and maximize your operation from a desktop, tablet, or mobile phone.

OVERVIEW

At FlashParking, our mission is simple: to perfect the parking experience. The parking industry has been dominated by complicated, unreliable technology and processes for too long. I'm sure you agree–your guests deserve more!

FlashValet offers the most advanced cloud-based valet and event parking solution for any venue type and size. Whether you operate one kiosk at a local restaurant or hundreds of valet stands in venues around the world, FlashValet is priced and customized to meet the unique needs of each location.

Our iOS-based app and cloud-run software platform enable parking operators to increase revenue, better manage operations, and improve the valet experience for valued guests. The FlashValet solution seamlessly integrates with hotel PMS, online parking reservations, and electronic validations to give you total control. With our award-winning platform, you can reliably manage your valet or portfolio of valet operations from the palm of your hand.

FlashValet is also part of FlashParking's fully integrated parking ecosystem, which delivers a unified platform for all our solutions:

- **FlashPARCS** (garage and parking lots)
- **FlashMobile** (mobile payments)

So no matter what your parking needs are, we have you covered!

BENEFITS

iOS-based App

Perfect for valet at hotels, airports, restaurants, condos, hospitals, malls, and more!

Traditional Valet

Guests receive a paper ticket upon check-in and can text for their vehicle, when they are ready to leave.

Ticketless Valet

No paper tickets; guests can check-in with their mobile number.

Event Parking

FlashValet is set-up to handle stadium-level as well as small event parking venues.

Monthly Parker Module

The module offers an array of access options; guests can create and manage accounts online.

Award-Winning Platform

Named one of Inc. Magazine's "100 Most Brilliant Companies".

Worry-free PCI Compliance

Let the only Level 1 Service Provider in the industry assume 98% of your PCI responsibilities.

Valet Pay-on-Foot/Retrieval Kiosk

Give guests the ability to pay for and request their vehicle at a stand-up kiosk.

Valet Monitor Module

Enhance guest experience by broadcasting vehicle request status on a large screen monitor.

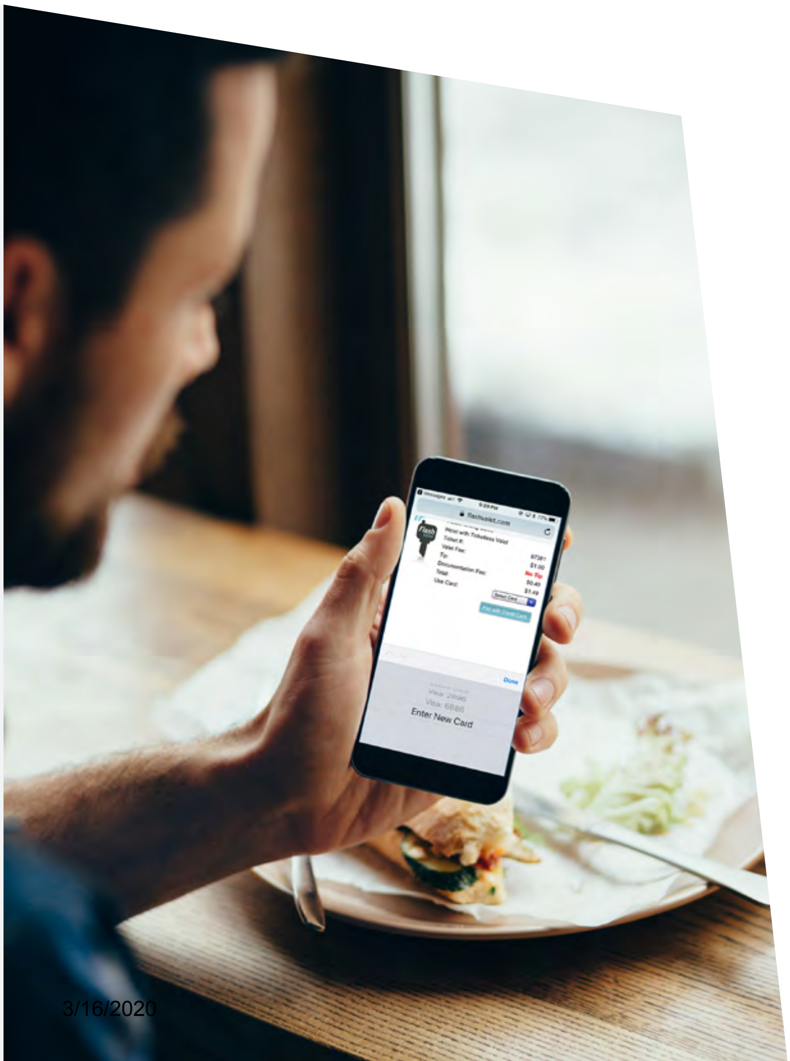
Future-Ready

Employ the latest tech with automatic software updates and interchangeable hardware.

WHY YOU'LL LOVE US?

We're different! As the only born-in-the-cloud parking technology provider in the industry, FlashParking is committed to perfecting the parking experience for customers as well as parking operators and asset owners. With FlashValet you can expect:

- An affordable solution
- A reliable, cloud-based platform
- 24/7 customer support
- Increased profits with better revenue control
- Seamless integrations with hotel PMS, eParking reservation systems, and electronic validations, offering you total control
- Minimal lost keys with key tracking software
- Photo records to prevent false damage claims
- Fast deployment (average deployment of 2 weeks)
- Surveys to get immediate feedback from your customers
- Accountability and tractability at a personnel level to promote a safer operation



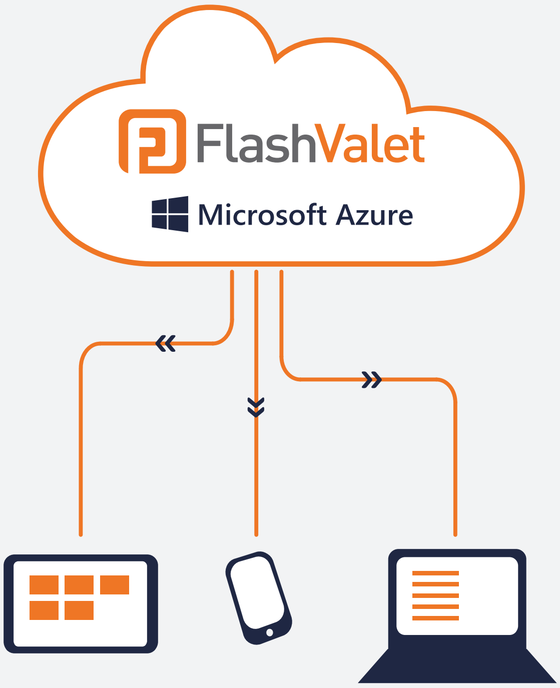
WHY YOUR GUESTS WILL LOVE US?

Guest impressions start and end at the driveway. FlashValet was built with your guests as the top priority. The minute a guest pulls up to your property, we help you deliver a truly VIP experience from beginning to end, including:

- Fast vehicle drop-off and pick-up via text request feature
- An intuitive and easy-to-use user interface
- Convenient payments including: credit card, mobile payments, and cash
- eParking parking reservation system integrations
- A ticketless valet option for guest convenience
- Remote vehicle requests via text, call, or online
- Member/VIP parker program

CORE **BENEFITS**

- Ability to see operations in real-time via phone or browser
- Access to over a 100+ business intelligence and analytics reports
- Automated and fully customizable reporting
- Simple tracking of credit card payments, eParking reservations, and electronic validations, and more



ADD-ONS

- Valet pay-on-foot/retrieval kiosk
- Valet monitor module
- eParking reservation module
- Monthly parkers and members module
- Hotel PMS and 3rd party integrations module

Issued
Hotel Demo
★752
23 Aug 12:32
Key: Hotel Demo, White Bentley
Pull
Edit
751
23 Aug 12:31
Key: Hotel Demo, Black Acura
750
Paid
$14.00
23 Aug 12:30
Key: Hotel Demo, Gold Ferrari
★749
23 Aug 12:29
Key: Hotel Demo, Red Mazda RX7, Mr. Jones
748
23 Aug 12:28
Key: Hotel Demo, Blue Honda Element
Issued
New
Active
Call
Control

EQUIPMENT **BRIEFING**

FlashValet offers affordable monthly service plans for a variety of venue types and sizes. With less than an hour of training and no necessary expensive hardware required, you can power your venue with FlashValet as soon as tomorrow.

Standard

Great for low volume operations

Pro

Perfect for high volume operations

Deluxe

Required for these operations: condo, airport, hotel, resort, casino

HEADQUARTERS
FlashParking
3801 S. Capital of Texas Highway, Suite 250
Austin, TX 78704

SALES
sales@flashparking.com
800.213.3706

SUPPORT
support@flashparking.com
888.737.7465

FlashParking

FLASHCLOUD FLASHPARKING'S CLOUD-BASED PLATFORM

SAFE. SECURE. SMARTER.

An innovative cloud-based platform powers FlashParking's entire line of solutions with maximum efficiency and key benefits.

FlashParking

VARIANCE

Transient	Overnight	Total
$123 Last Year: 122 $1 (10%) ▲	$200 Last Year: 199 $1 (8%) ▲	$323 Last Year: 315.00 $2 (12%) ▲

VEHICLE COUNT

Transient	Overnight	Total
$1,910 Last Year: 1,908 $1 (10%) ▲	$3,833 Last Year: 3,832 $1 (8%) ▲	$5,743 Last Year: 5,735.00 $2 (12%) ▲

AVERAGE PRICE

Transient	Overnight	Total
$33 Last Year: $32 $1 (15%) ▲	$26 Last Year: $31 $2 (25%) ▲	$30 Last Year: $30 $3 (30%) ▲

VEHICLE HOURLY COUNT

PERFORMANCE

Avg Vehicles/Hr	Avg Retrieval	Avg Park
$14 Last Year: 13 $1 (10%) ▲	$9 Last Year: 8 $1 (8%) ▲	$9 Last Year: 7.25 $2 (12%) ▲

OVERVIEW

From manufacturing and healthcare to service and hospitality industries, companies across the industry spectrum are undertaking “digital transformation” initiatives. Digital transformation, the fundamental shift in organizations to adopt and prioritize technology that opens new opportunities, is a key driver in gaining a competitive edge and meeting customer demands, while controlling costs and risk.

Cloud computing has become one of the most important technological innovations driving digital transformation. It has allowed businesses to run operations and scale more quickly, efficiently, and in a cost-effective manner. The Cloud has become the go-to computing platform across most industries, including transportation and parking.

Simply put, cloud computing is the delivery of computing services—servers, storage, databases, networking, software, analytics, and more—over the Internet (“the cloud”). Companies offering these computing services typically charge for cloud computing services based on usage, like being billed for water or electricity at home—but FlashParking includes cloud-based processing as a standard part of any system.

While many parking vendors are playing catch up to retrofit old solutions and cobble together cloud-based offerings, FlashParking purpose-built solutions from the ground up with a “Cloud-first” approach. We’ve essentially taken the cloud computing success seen in other industries and applied it to the parking industry to enable a better way to run parking operations and improve the bottom line.

FlashParking’s cloud-based software platform, built using Microsoft Azure Cloud Services, allows clients to capitalize on a dynamic, “future-proof” system, that will expand and support new capabilities as technology and customer demand evolves.

BENEFITS

Cost Efficiency

Onsite physical servers and the infrastructure to support them account for a significant expense to organizations. With the cloud, many of those expenses disappear, as no onsite servers are required. Computing allows cloud organizations to simply buy "resources" on virtual servers, accessed via a secure internet connection. The cloud also eliminates the need for onsite IT support to maintain physical infrastructure.

Easy Upkeep

Adopting a cloud-based approach to your operations allows you to shift the burden of system upkeep and maintenance to the vendor. You can focus on your core competencies while the technical experts (the vendor) maintains the system. System updates and upgrades are done remotely with virtually ZERO downtime, so there is no need to shut down lanes during routine system updates. This is done on your behalf, behind the scenes, without disruption to your operations.

Worry-free Compliance

As the only Level 1 Service Provider in the industry, you—the parking provider—can confidently outsource 98% of the PCI duties to us. We take on the technical burden so you can stay focused on running your operation, not on fixing and updating machines. The result is instant and on-going complete PCI compliance. It's that simple!

Scalability

Since the cloud requires no physical infrastructure, scaling resources up or down based on need is quick and easy. Scaling with FlashParking simply requires a purchase or reduction in cloud space, rather than purchasing and provisioning new physical servers.

Redundancy

Cloud computing makes data backup, disaster recovery, and business continuity easier and less expensive because data, services, and resources can be mirrored at multiple redundant sites on the cloud provider's infrastructure. A 4G/LTE back-up cellular network service for connectivity redundancy also comes standard with FlashParking solutions, so you never have to fear an internet outage. If your primary internent line goes down an automatic switch-over to the back-up cellular network occurs without skipping a beat.

Safe, Secure Transactions

We purposely built the FlashParking platform to ensure safe and secure transactions every time. As soon as a customer swipes their credit card, the information stored on the card is encrypted at the head of their credit card reader and sent directly to the payment gateway. We never store credit card information on our system and all the data (such as transaction records) is stored in the Microsoft Azure cloud, which powers 90% of Fortune 500 companies.

KEY FEATURES

- Platform built on Microsoft Azure Cloud Services
- 90% of the fortune 500 companies trust their business to Microsoft Azure Cloud
- 24/7 phone and online support
- A 4G/LTE back-up cellular network service for redundancy
- Software updates/upgrades performed remotely by FlashParking engineers
- Load balancer to ensure software updates and patches are applied with virtually ZERO downtime
- Instant and ongoing PCI compliance
- Demand-based pricing capabilities
- Mobile-friendly parking rate changes
- Mobile-based parking asset management
- 3rd-party integration capabilities via API-based architecture

HEADQUARTERS
FlashParking
3801 S. Capital of Texas Highway, Suite 250
Austin, TX 78704

SALES
sales@flashparking.com
800.213.3706

SUPPORT
support@flashparking.com
888.737.7465

FlashParking
Perfecting the Parking Experience

HEADQUARTERS
FlashParking
3801 S. Capital of Texas Highway, Suite 250
Austin, TX 78704

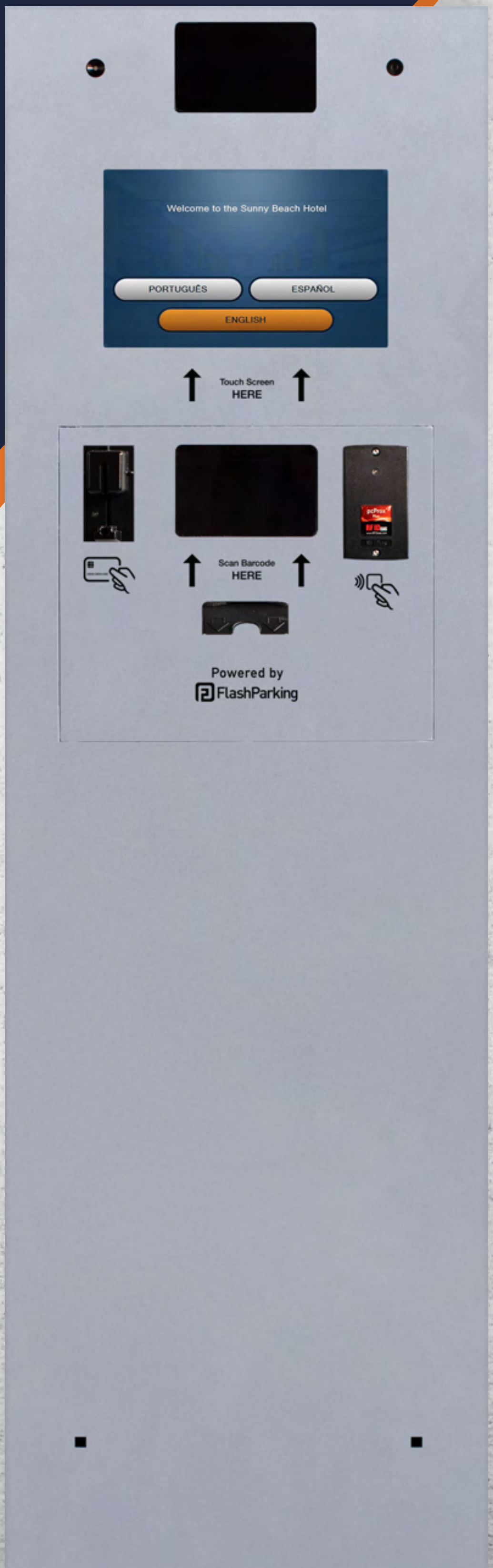
SALES
sales@flashparking.com
800.213.3706

SUPPORT
support@flashparking.com
888.737.7465

FlashParking

ENTRY/EXIT SMART STATION

SAFE. SECURE. SMARTER.
Bluetooth-enabled, cloud-based kiosk with flexible software configurations, seamless integrations, and easy DIY maintenance guarantees maximum uptime.



OVERVIEW

Smart Design

Our Entry/Exit Smart Station assembles all the essential elements needed to manage parking access and revenue control in a single elegant unit. Our physical kiosk is identical for entry, exit, or pay-on-foot.

Customizable

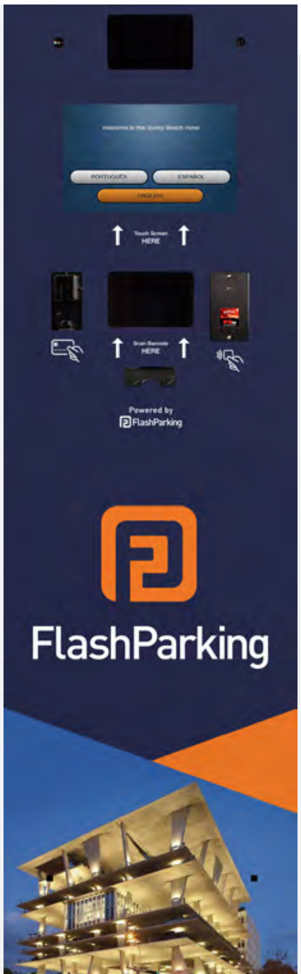
The Entry/Exit Smart Station is highly customizable to meet the unique demands of each parking facility. Whether it will be used to manage transients or monthlies, the software package is simply configured for each machine's role in the venue.

Future-proof Platform

The cloud-based software platform that powers the logic in all of our Smart Stations was purpose-built to run in the cloud, offering enhanced scalability, redundancy, and most importantly—since no on-site servers are needed—minimal maintenance and system upkeep. Cloud-based software also allows for easy system reconfiguration as technology and venue needs evolve.

Cash Acceptance Friendly

In addition to credit card payments, we offer in-lane cash acceptance options. Our cash machines can be equipped with either an exact change feature or a bill note recycler (BNR) machine that boasts a four-denomination bill recycler, which eliminates the need to empty and re-fill the machine quite as often.



SMART STATION **COMPONENTS**

1. Interactive touch-screen display
2. Credit card reader (for payments and access)
3. Ticket/receipt dispenser (pull-tear mechanism)
4. Barcode scanner (mobile and barcodes)
5. Prox/RFID card reader
6. Integrated intercom (video, mic, and speaker)

USB-based Components

All peripherals on the Smart Station are part of a plug-and-play (USB-based) system and can be swapped out in the existing machine as new technology emerges.

Easy Maintenance

Our unique FlashCare Maintenance Kit contains replacements for major components so operators can quickly replace parts in a matter of minutes with minimal downtime.

BENEFITS

To view a list of featured properties using FlashParking visit:
www.flashparking.com/featured-properties

Total Reliability

The FlashParking platform runs on the Microsoft Azure Cloud Platform, which today powers 90% of Fortune 500 companies. We provide comprehensive access to monitor and manage all your properties from a single back-end portal via mobile, tablet or desktop.

Real-time Decision Making

Manage operations like rate changes, credit card payments, eParking reservations, and electronic validations in real-time via phone or browser.

Worry-free Compliance

With FlashParking, you—the parking provider—outsource 98% of the PCI duties to us, the only Level 1 Service Provider in the industry. The result is instant and on-going complete PCI compliance. It's that simple!

Extreme Weather Rated

The Smart Stations are UL Certified to withstand all extreme weather conditions and aluminum built to withstand corrosion.

Extending Your Brand

The standard shell of the Smart Station comes in a powder-coated silver aluminum; properties looking to extend their brand to the parking facility can wrap their Smart Stations in any design.

> *"What we've seen with Flash has been really remarkable. It's been one of the only solutions we've ever installed, and not had one service or support call 6 months down the road."*
>
> ”
>
> **Ryan Hunt**
>
> President for Premier Parking

STANDARD FEATURES

The Entry/Exit Smart Station has an extensive list of feature choices to build out the perfect solution for each venue.

- Access via barcoded tickets, RFID/Prox card reader, and a barcode scanner
- Contract parking management (monthly parking)
- Support calls with a touchscreen activated Voice over IP (VoIP) two-way intercom system
- 4G/LTE back-up network service
- Bluetooth technology embedded in all Smart Stations
- Robust, real-time reporting suite with on-demand and scheduled reports and dashboards
- 24/7 phone and online support
- Ongoing PCI compliant software updates and general software patches
- Mobile app module (for managing parking operations in the palm of your hand)

1111 Lincoln Road in Miami

Toyota Music Factory in Irving, TX

OPTIONAL **FEATURES**

Display

- Multi-lingual module
- Display current rate on entry kiosk
- Digital rate display via a monitor

Payment

- Credit card (with EMV chip payment option)
- Cash acceptance module
- Web-based validation: secure access for customers, clients, and merchants to validate online or pre-printed

Management

- Online monthly parker module
- Validations (printed and electronic)
- Cash acceptance module
- Analytics and business intelligence (BI) solutions

Access

- Ticketless access via credit card or mobile number
- Monthly parkers entry/exit access via mobile phone interactive voice response (IVR) system
- Bluetooth BLE technology to allow monthly parker mobile phone access and connected car integration for monthly and transient access
- Third-party access control module (AVI, LPR, and others)
- FlashParking mobile app module (BLE)
- Long-term pass/overnight hotel module

Open API Platform with Several Integrations

- Payment platforms and gateways (USAePay and Payment Express)
- Hotel PMS including Micros Opera, Lightspeed Galaxy, Infor and more
- eParking solutions including SpotHero/Parking Panda, ParkWhiz, Ticketmaster, off-airport parking and more
- AVI readers (Tagmaster and Transcore) and LPR camera systems
- Third-party call center solution including Parker Video Intercom two-way video support

SPECS

MEASUREMENTS	
Dimensions	16"w x 12"d x 55"h
Weight	58 lbs
Color	Industrial Gray
Locks	Yes
Wrapping	Yes, customized wrapping available
ELECTRICAL	
Voltage	120V
Current Consumption	~8.0 amps max
Power Consumption	~1020 watts max
PARCS HARDWARE CAPABILITIES	
Operating Temperature	-20° to +140° F
Humidity	15-95% rH noncondensing
Agency Certifications	UL 60950-1/CSA C22.2 N. 60950-1, and UL 60950-22 Outdoor Use
Rating	UL 60950-22 under NEMA 250-2008
ADDITIONAL INFO	
Bluetooth Functionality	Yes
Multi-lingual	Yes
Communication Options	Ethernet/RJ45 with 4G/LTE back-up
FlashCare Maintenance Kit	Yes (a kit with all major peripheral components available)

HEADQUARTERS
FlashParking
3801 S. Capital of Texas Highway, Suite 250
Austin, TX 78704

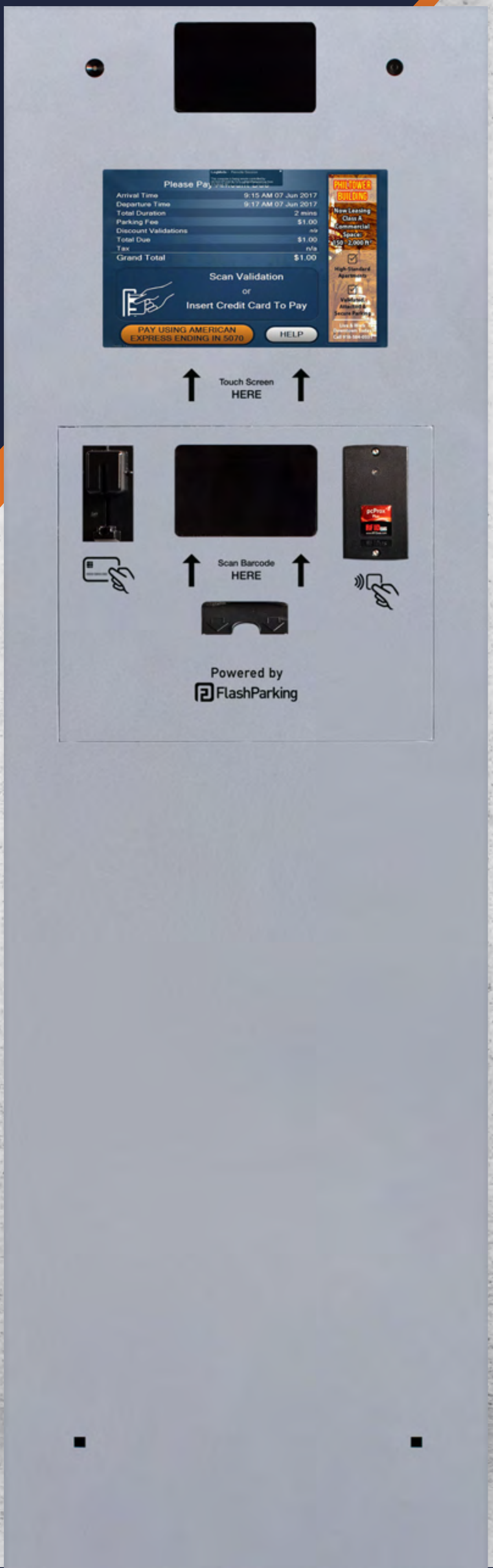
SALES
sales@flashparking.com
800.213.3706

SUPPORT
support@flashparking.com
888.737.7465

FlashParking

PAY-ON-FOOT SMART STATION

SAFE. SECURE. SMARTER.
Bluetooth-enabled, cloud-based pay-on-foot kiosk features flexible software configurations, seamless integrations, and cash acceptance options with best-in-class bill acceptance and recycler.



OVERVIEW

Smart Design

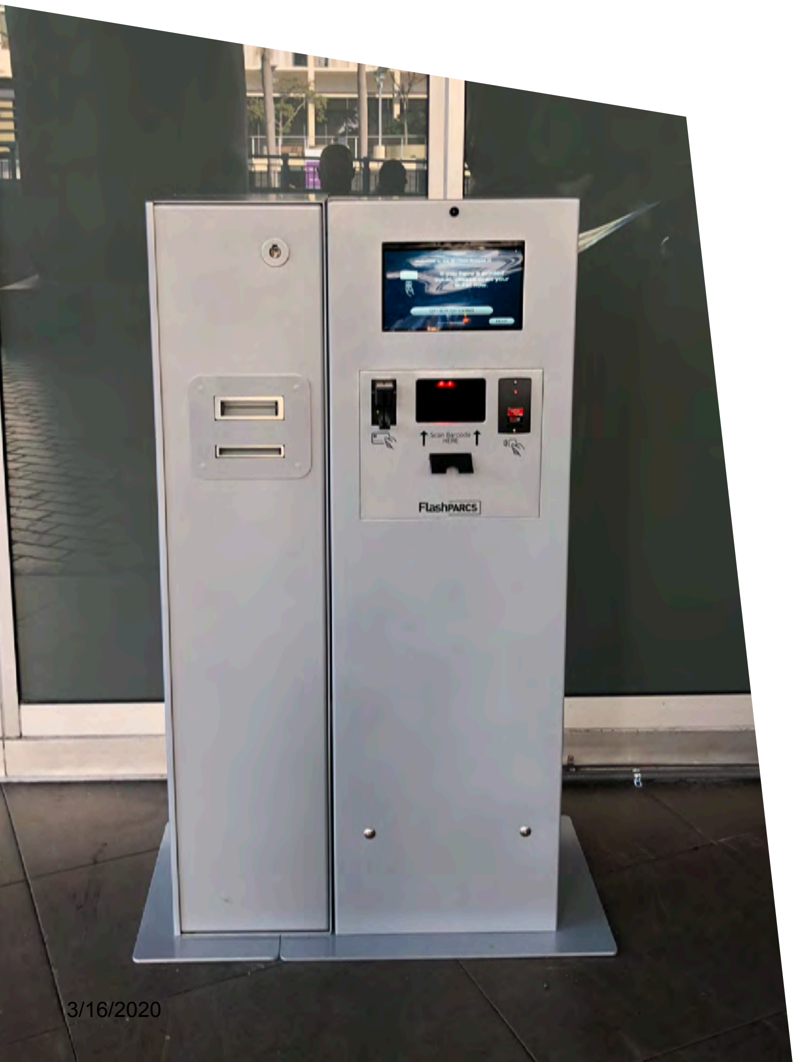
Our Pay-on-Foot (POF) Smart Station combines the essential PARCS and valet payment components in a single elegant unit, which can be paired with our unique cash acceptance machine.

Flexible Configurations

The Pay-on-Foot Smart Station can be configured for PARCS, valet, or both. The POF Smart Station can be set up anywhere often in a garage or lobby as an additional payment station. For valet operations, the Valet POF/Vehicle Retrieval Smart Station allows for guests to request their vehicle and pay.

Cash Acceptance Friendly

In addition to credit card payments, we offer cash acceptance options for both the POF and the Valet POF/Vehicle Retrieval Smart Station. Our cash machines offer two options: an exact change only machine or a bill note recycler (BNR) machine that boasts a four-denomination bill recycler, which eliminates the need to empty and re-fill the machine quite as often.



PAY-ON-FOOT **COMPONENTS**

1. Interactive touch-screen display
2. Credit card reader (for payments and access)
3. Ticket/receipt dispenser (pull-tear mechanism)
4. Barcode scanner (mobile and barcodes)
5. Integrated intercom (video, mic, and speaker)
6. Prox/RFID card reader
7. Exact Change or BNR cash machine pairing

USB-based Components

Just like the Entry/Exit Smart Station, all peripherals on the POF Smart Station are part of a plug-and-play (USB-based) system and can be swapped out in the existing machine as new technology emerges.

Easy Maintenance

Our unique FlashCare Maintenance Kit contains replacements for all major components so operators can quickly replace parts in a matter of minutes with minimal downtime.

BENEFITS

To view a list of featured properties using FlashParking visit:
www.flashparking.com/featured-properties

Total Reliability

The FlashParking platform runs on the Microsoft Azure Cloud Platform, which today powers 90% of Fortune 500 companies. We provide comprehensive access to monitor and manage all your properties from a single back-end portal via mobile, tablet or desktop.

Headache-free Bill Acceptance and Recycler

Manage operations like rate changes, credit card payments, eParking reservations, and electronic validations in real-time via phone or browser.

Worry-free Compliance

With FlashParking, you—the parking provider—outsource 98% of the PCI duties to us, the only Level 1 Service Provider in the industry. The result is instant and on-going complete PCI compliance. It's that simple!

Improved Security

All cash transactions are optimized and simplified by a single device. Reconciled funds are accounted for electronically and stored in a single locked cashbox. The BNR facilitates a closed-loop cash system, allowing facilities to simplify the cash management process and increase profitability.

Extreme Weather Rated

The Smart Stations are UL Certified to withstand all extreme weather conditions.

> *"What we've seen with Flash has been really remarkable. It's been one of the only solutions we've ever installed, and not had one service or support call 6 months down the road."*
>
> **Ryan Hunt**
> President for Premier Parking

STANDARD **FEATURES**

The Pay-on-Foot Smart Station has an extensive list of feature choices to build out the perfect solution for each venue.

- Intercom capabilities to initiate a help call with touchscreen activated Voice over IP (VoIP) two-way intercom system
- 4G/LTE back-up network service
- Bluetooth beacon technology embedded in all Smart Stations
- Robust, real-time reporting suite with on-demand and scheduled reports and dashboards
- Ongoing PCI compliant software updates and general software patches
- Mobile app module (for managing parking operations in the palm of your hand)
- Dual-side bill scanning optimizing recognition
- Self-centering transport guides automatically align bills even when fed at an angle
- Single hardware platform to reduce support and operation costs
- Accepts, stacks, and outputs cash
- Escrows bills to deliver same cash back to customers
- Pays out in bundles of up to 15 bank notes
- Lockable, removable, and durable cashbox
- Electronic memory to record cash loading recycling units
- 24/7 phone and online support

Aspen Airport in Aspen

Icon Brickell Tower in Miami

OPTIONAL **FEATURES**

Display

- Multi-lingual module
- Display current rate on entry kiosk
- Digital rate display via a monitor

Payment

- Credit card (with EMV Chip Payment option)
- Cash acceptance module
- Web-based validation: secure access for customers, clients, and merchants to validate online or pre-printed validations

Open API Platform with Several Integrations

- Payment platforms and gateways (USAePay and Payment Express)
- Third-party call center solutions including Parker Two Way Video Intercom System
- Analytics and business intelligence (BI) Solutions

SPECS

MEASUREMENTS	
Dimensions	16"w x 12"d x 55"h
Weight	58 lbs
Color	Industrial Gray
Locks	Yes
Wrapping	Yes, customized wrapping available
ELECTRICAL	
Voltage	120V
Current Consumption	~8.5 amps max
Power Consumption	~1020 watts max
PARCS HARDWARE CAPABILITIES	
Operating Temperature	-20° to +140° F
Humidity	15-95% rH noncondensing
Agency Certifications	UL 60950-1/CSA C22.2 N. 60950-1, and UL 60950-22 Outdoor Use
Rating	UL 60950-22 under NEMA 250-2008
ADDITIONAL INFO	
Bluetooth Functionality	Yes
Multi-lingual	Yes
Communication Options	Ethernet/RJ45 with 4G/LTE back-up
FlashCare Maintenance Kit	Yes (a kit with all major peripheral components available)

HEADQUARTERS
FlashParking
3801 S. Capital of Texas Highway, Suite 250
Austin, TX 78704

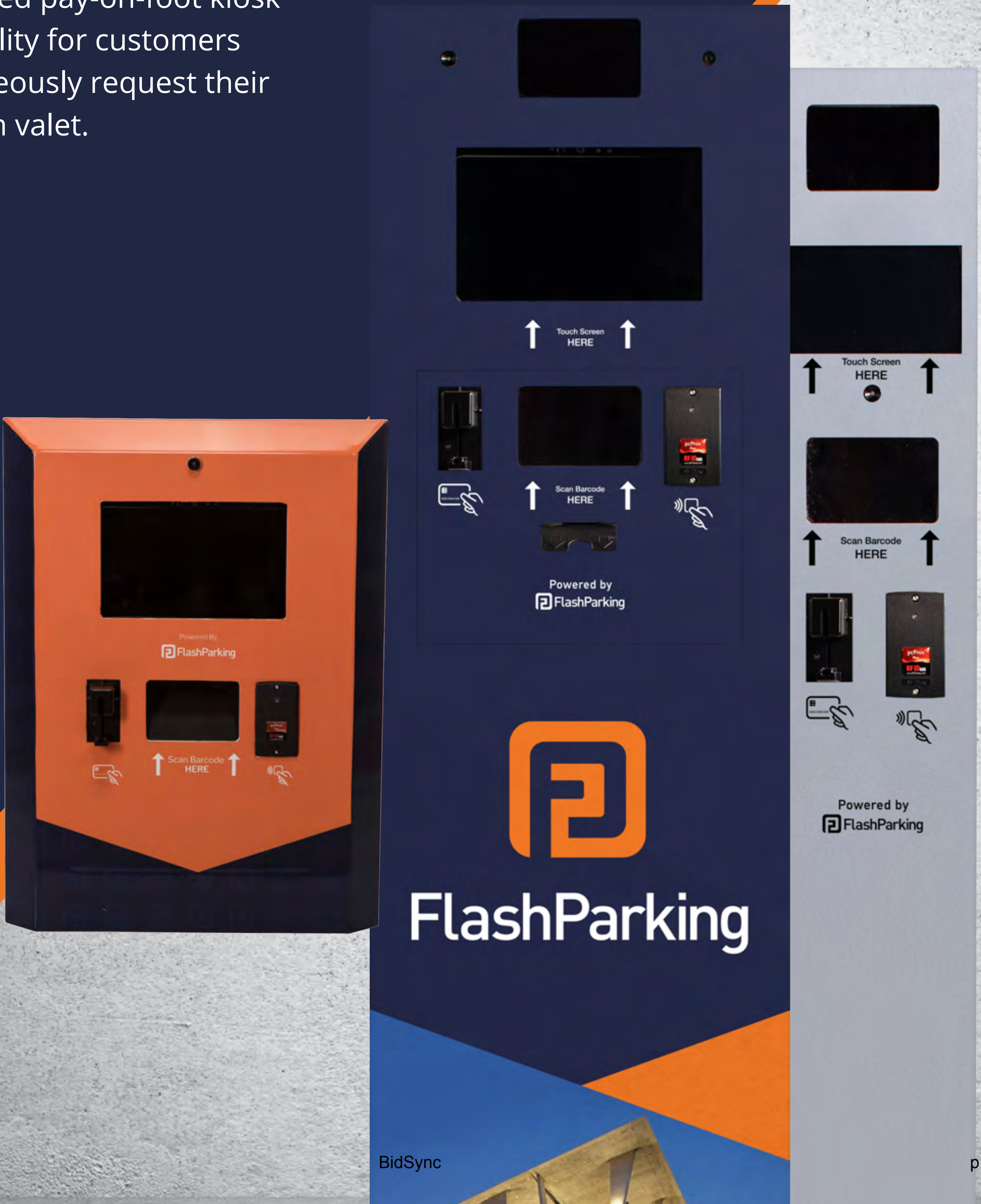
SALES
sales@flashparking.com
800.213.3706

SUPPORT
support@flashparking.com
888.737.7465

FlashPARCS

VALET PAY-ON-FOOT/RETRIEVAL SMART STATION

A cloud-based pay-on-foot kiosk with the ability for customers to simultaneously request their vehicle from valet.



OVERVIEW

Instant Revenue Lift

The valet pay-on-foot/retrieval kiosk is ideal for busy venues like hotels, airports, and retail shopping centers. By strategically placing this retrieval/payment kiosk in a lobby or near an exit, your guests are in control of when they request their vehicle and how they pay and tip.

24/7 Payment/Retrieval Option

A busy valet stand has lots of moving pieces, but with the valet pay-on-foot/retrieval kiosk you can streamline the retrieval and payment process for your guests. With this 24/7 payment/ retrieval option, guests can bypass long lines at the valet stand.

Smart Design

The valet pay-on-foot/retrieval kiosk is powered by FlashParking's award-winning cloud-based platform. All the peripherals on the kiosk are part of a plug-and-play (USB-based) system and can be swapped out in a matter of minutes with minimal downtime.

Superior Customer Experience

Keep your guests in the know when your pair a valet pay-on-foot/retrieval kiosk with our valet retrieval monitor. Guests can see in real-time where they are in the vehicle retrieval line as well as an approximate wait time.

PAY-ON-FOOT/RETRIEVAL
HARDWARE OPTIONS

Smart Station

For valet operations that would like to issue paper receipts and/or have a cash acceptance option for their customers, our full-sized Smart Station is the best machine for the job.

PARCS Mini-Smart Station

For lean valet operations, our PARCS Mini-Smart Station has all the same components as a full-sized kiosk minus a printer. Customers still have the ability to scan their parking ticket (which notifies valet to pull their car around) as well as pay using a credit card only. For receipts, customers can download a receipt through our flashreceipts.com portal.

Wall Mount Smart Station

An ideal option for a busy hotel or building lobby, the Wall Mount Smart Station can be bolted to a wall or mounted on a pedestal and has the ability to print paper receipts.

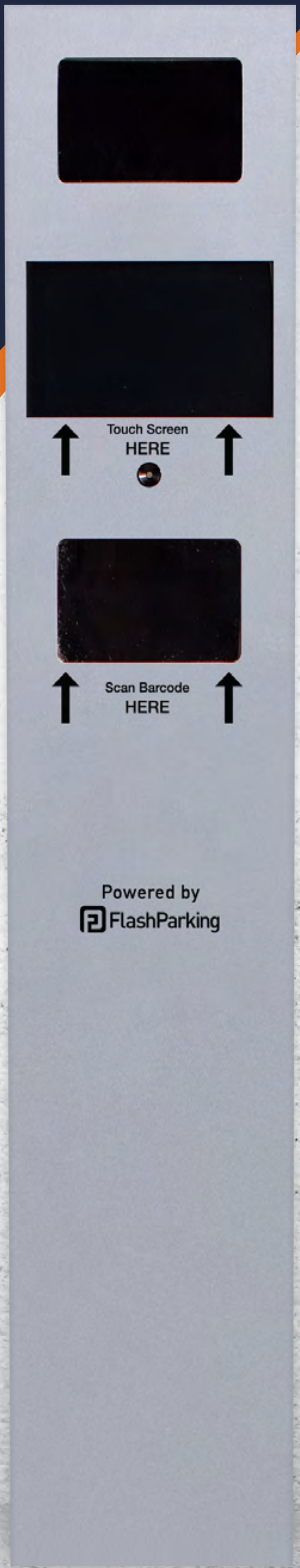
For more information about our Valet Pay-on-Foot/Retrieval Smart or Mini-Smart Station, please contact us at:

✉ **sales@flashparking.com** ☎ **800.213.3706**

FlashParking

ePARKING
MINI-SMART STATION

SAFE. SECURE. SMARTER.
A cloud-based Smart Station provides eParking reservation access via Bluetooth beacon technology and features a scanner that reads QR and barcodes.



OVERVIEW

Savvy eParking Reservation Solution

Today's parkers are increasingly sophisticated, with many looking to make their parking experience as frictionless as possible. Finding and pre-paying for parking via parking reservation solutions is becoming the method of choice for tech savvy consumers. Your parking solution should be able to meet their demands. With that understanding, we developed our eParking Reservation Mini-Smart Station to harness the power of our cloud-based parking platform, provide state-of-the-art Bluetooth access with FlashBeacon, as well as read and accept mobile or printed tickets.

Innovative Technology

FlashBeacon, our Bluetooth beacon technology, is embedded in all our products, including our eParking Reservation Mini-Smart Station. By choosing to turn on Bluetooth access, parkers can easily download the FlashParking Mobile app which interacts with the Smart Station's Bluetooth beacon to provide automatic access. This means rolling down the window to tap their prox card will become a thing of the past!

Customizable and Future-Ready

Designed to give your customers the best parking experience possible, our eParking Reservation Mini-Smart Station solution suite is highly customizable to meet the specific needs of the venue today and can be easily reconfigured in the future as those needs evolve. You will no longer need to buy new equipment as needs change, a simple re-configuration of the unit is all that is required!

Versatile Machine

The tiny yet nimble eParking Reservation Mini-Smart Station can be configured for these 2 scenarios:

eParking Reservation Only – This configuration allows you to accept eParking reservations via bluetooth access or the barcode scanner that accepts paper or mobile QR or barcodes.

Components: *Bluetooth Low Energy technology, controller, relay board, LCD display, intercom, Barcode Scanner*

eParking Reservation with Credit – This configuration allows operators to accept eParking reservations via bluetooth access or the barcode scanner that accepts paper or mobile QR or barcodes. The addition of the the credit card reader enables guests to pay for overages with a simple swipe.

Components: *Bluetooth Low Energy technology, controller, relay board, LCD display, intercom, barcode scanner, credit card reader, RFID/Prox card*

BENEFITS

To view a list of featured properties using FlashParking visit:
www.flashparking.com/featured-properties

Total Reliability

The FlashParking platform runs on Microsoft Azure cloud-platform, which today powers 90% of Fortune 500 companies. We provide comprehensive access to monitor and manage properties from a single back-end portal via mobile, tablet or desktop.

Worry-free Compliance

With FlashParking, you—the parking provider—outsource 98% of the PCI duties to us, the only Level 1 Service Provider in the industry. The result is instant and on-going complete PCI compliance. It's that simple!

Real-time Decision Making

Manage operations in real-time via phone or browser, including: rate changes, credit card payments, eParking reservations, and more.

USB-based Components

All peripherals on the Mini-Smart Station are part of a plug-and-play (USB-based) system and can be swapped out in the existing machine as new technology emerges.

Easy Maintenance

Our unique FlashCare Maintenance Kit for the Mini-Smart Station contains replacements for all major components so operators can quickly replace parts in a matter of minutes with minimal.

Assembled in the U.S.

Our Mini-Smart Stations is manufactured in Austin, TX, minimizing shipping time and increasing speed of deployment.

Extending Your Brand

The standard shell of the Mini-Smart Station comes in a powder-coated silver; properties looking to extend their brand to the parking facility can wrap their Mini-Smart Stations in a design of their choosing.

STANDARD **FEATURES**

The eParking Reservation Mini-Smart Station has an extensive list of feature choices to build out the perfect solution for each venue.

- Intercom capabilities to initiate a help call with touch-screen activated Voice over IP (VoIP) 2-way intercom system
- Available 4G/LTE back-up network service
- Bluetooth beacon technology embedded in all Mini-Smart Stations
- Robust, real-time reporting suite with on-demand and scheduled reports and dashboards
- Mobile app module (for managing parking operations in the palm of your hand)
- Ongoing PCI compliant software updates and general software patches
- 24/7 phone and online support

Centerview Towers in Irving, CA

Celebration Pointe in Gainesville, FL

OPTIONAL **FEATURES**

Display

- Multi-lingual module

Open API Platform with Several Integrations:

- Payment platforms and gateways (USAepay)
- Third-party call center solutions
- Analytics and business intelligence (BI) solutions

SPECS

MEASUREMENTS	
Dimensions	7"w x 7"d x 55"h
Weight	approx. 38 lbs
Color	Industrial Gray
Locks	Yes
Wrapping	Yes, customized wrapping available
ELECTRICAL	
Voltage	120V
Current Consumption	approx. ~8.0 amps max
Power Consumption	approx. ~1020 watts max
PARCS HARDWARE CAPABILITIES	
Operating Temperature	-20° to +140° F
Humidity	15-95% rH noncondensing
Agency Certifications	UL 60950-1/CSA C22.2 N. 60950-1, and UL 60950-22 Outdoor Use
Rating	UL 60950-22 under NEMA 250-2008
ADDITIONAL INFO	
Bluetooth Functionality	Yes
Multi-lingual	Yes

PRICING

HARDWARE	
E-Parking Mini Smart Station *(LCD Display, Barcode Scanner, Relay board, Central USB Peripheral hub, 12V power supplies, Bluetooth beacon kit)*	$3,000
E-Parking Mini Smart Station w/Credit Card *(LCD Display, Barcode Scanner, Credit Card Reader, Relay board, Central USB Peripheral hub, 12V power supplies, Bluetooth beacon kit)*	$5,000
FlashCare Kit for Mini Smart Stations *(Includes all major components of the Mini-Smart Station)*	$3,000
NETWORK EQUIPMENT	
eParking Network Kit	$400
Standard Network Kit *(Used with FlashPARCS)*	$2,500
SOFTWARE	
SaaS - Standard Package *(Unlimited numbers of lanes)*	$200/month
SaaS - With Credit Card Module *(Add-on includes firts 5,000 credit card transactions per month. Add $50 for every additional 5,000 transactions)*	$100/month
SaaS - Backup Network Module *(Add-on includes 4G/LTE backup data)*	$100/month

HEADQUARTERS
FlashParking
3801 S. Capital of Texas Highway, Suite 250
Austin, TX 78704

SALES
sales@flashparking.com
800.213.3706

SUPPORT
support@flashparking.com
888.737.7465

FlashParking

CASH MACHINE WITH BILL NOTE RECYCLER

SAFE. SECURE. SMARTER.
A cash machine equipped with best-in-class Bill Note Recycler delivers a great customer experience and simplifies the operator’s job of managing cash.

OVERVIEW

At FlashParking, we understand that a great parking experience is what keeps customers coming back. Providing multiple methods of payment for customers is key to delivering the optimal parking experience.

With FlashParking's unique cash machine configuration options, managing cash is a simple task. The cash machine was designed as an add-on component to our Smart Station. Activities associated with loading, emptying, and reconciling cash can increase labor costs. Built to provide all the cash-handling ability of a human cashier with increased security and cash management benefits, the cash machine can reduce labor costs associated with activities like loading, emptying, and reconciling cash.

FlashParking's cash machine comes in two variations: exact change bill acceptor or Bill Note Recycler (BNR).

Cash machine Options Pair With:

- ✓ Entry/Exit Smart Station – pre-pay on entry or pay on exit
- ✓ Pay-on-Foot Smart Station
- ✓ Valet Pay-on-Foot/Retrieval Smart Station – self-pay valet capability
- ✓ Multi-space Smart Station – pay by space, pay by plate parking

BENEFITS

Simple Architecture

For a streamlined experience, all functionality is operated from the touch-screen display on the paired Smart Station.

Headache-free Bill Acceptance and Recycler

The cash machine with BNR boasts 98% first time bill acceptance rates to ensure a frictionless customer experience. The BNR sports up to a 4-denomination bill recycler to minimize the emptying and re-filling of the machine and avoid downtime.

Improved Security

All cash transactions are optimized and simplified by a single device. Reconciled funds are accounted for electronically and stored in a single locked cashbox. The BNR facilitates a closed-loop cash system, allowing facilities to simplify the cash management process and increase profitability.

Key Configuration

The cash machine can be configured for key access and cashbox removal with a separate key for bill removal. This provides maximum accountability and security throughout the cash management life cycle.

Assembled in the U.S.

Our Smart Stations and cash machines are manufactured in Austin, TX, minimizing shipping time and increasing speed of deployment.

Extending Your Brand

The standard shell of the cash machine comes in a powder-coated silver; properties looking to extend their brand to the parking facility can wrap their cash machine and Smart Stations in a design of their choosing.

FEATURES

- ✓ Accepts, stacks, and outputs global currency
- ✓ Customer-friendly, high-speed and high-security acceptance
- ✓ Advanced sensor technology scans both sides of the bill for optimal recognition
- ✓ Self-centering transport guides automatically adjust and perfectly align bills—even when fed at an angle
- ✓ Simple hardware platform reduces support and operation costs
- ✓ Escrow bills to deliver the same cash back to customers
- ✓ Pays out in bundles of up to 15 bank notes
- ✓ Lockable, removable, and durable cashbox
- ✓ Electronic memory to record the cash loading of recycling units
- ✓ 24/7 phone and online support

SPECS

MEASUREMENTS	
Dimensions	11.25"w x 15.5"d x 55"h
Weight	Approx. 350 lbs
Color	Industrial Gray
Locks	Yes
Wrapping	Yes, customized wrapping available
ELECTRICAL	
Voltage	120V
Current Consumption	~8.0 amps max
Power Consumption	~41 watts max
PARCS HARDWARE CAPABILITIES	
Operating Temperature	-20° to +140° F
Humidity	15-95% rH noncondensing
Agency Certifications	UL 60950-1/CSA C22.2 N. 60950-1, and UL 60950-22 Outdoor Use
Rating	UL 60950-22 under NEMA 250-2008

FlashParking
Perfecting the Parking Experience

HEADQUARTERS
FlashParking
3801 S. Capital of Texas Highway, Suite 250
Austin, TX 78704

SALES
sales@flashparking.com
800.213.3706

SUPPORT
support@flashparking.com
888.737.7465

MAGNETIC®
ACCESS TO PROGRESS

Access

Access barrier

For access control

The Access Pro series barriers from Magnetic are optimized solutions for access control at car parks, company grounds, residential buildings, port facilities and other secured areas with lane widths up to 20 ft. Compared to the Access Pro-L, The Access Pro-H includes a taller cabinet, with more room for accessories, and a straight MicroBoom arm. Combine the Access Pro-H with the optional barrier arm skirt (with or without climb-over prevention) to effectively stop intruders from crawling under and/or climbing over the barrier.

At the heart of the Access series is the innovative MHTM™ drive that is distinguished by its energy efficiency, lack of maintenance and long service life – the Access series is designed for 10 million opening and closing cycles. The Access Pro-L and Access Pro-H are characterized by a high level of functionality and offer expansion potentials with plug-in modules and exclusive accessories. Magnetic quality lies not just in the detail, but is also easily recognizable thanks to its stylish design. The Access series has already been awarded two design prizes.

Low operating costs
With arm lengths up to 20 ft the Access Pro series is perfectly suited for a wide variety of applications. Thanks to their high energy efficiency, extremely long service lives, and simple maintenance, barriers from Magnetic are particularly cost-effective – an investment that will certainly pay off!

Innovative drive technology
The MHTM™ drive unit is maintenance-free, energy-efficient and quiet. The high torque guarantees best possible operation even under extreme weather conditions.

Legal security
Magnetic vehicular lift barriers have always been UL 325 approved. UL 325 ensures that our product guards against entrapment, fire, and electrical shock.

Easy access to components
Two simple steps: control systems and the drive unit are easily reached by removing the top cover and front plate. This increases user-friendliness and accelerates commissioning and service.

MAGNETIC AUTOCONTROL
www.magnetic-access.com/usa

ACCESS | PARKING | TOLL | TRAFFIC

Access

Access barrier

- High level of functionality for numerous applications
- High security with optional barrier arm skirts
- Very low operating costs thanks to efficient and long-lived MHTM™ drive
- Ease-of-use and optimum accessibility thanks to well thought-out design
- Acclaimed design: German Design Award 2014 and Red Dot Design Award 2012
- Designed for 10 million opening and closing cycles

Technical data	Access Pro-L	Access Pro-H
Barrier width	Max. 20 ft	Max. 20 ft
Opening/closing time	4.0 s	4.0 s
Power consumption	Max. 25 W	Max. 25 W
Drive technology	MHTM™	MHTM™
Voltage	85–264 VAC, 50/60 Hz	85–264 VAC, 50/60 Hz
Duty cycle	100 %	100 %
Housing dimensions (L x W x H)	12.4 x 14.2 x 36.0 in	12.4 x 14.2 x 36.0 in
Enclosure rating	IP 54	IP 54
Temperature range	−22 to +131 °F	−22 to +131 °F
Weight without barrier arm	88.2 lb	97 lb

Features	Access Pro-L	Access Pro-H
Standard colors	RAL 2000, 9006, 9007, 9010	RAL 2000, 9006, 9007, 9010
Barrier arm type	VarioBoom	MicroBoom
Control system	MGC Pro	MGC Pro
Integrated 2-channel detector for induction loops	Standard	Standard
Modular expansion of control system	Freely expandable	Freely expandable
Variable I/O assignment	Standard	Standard
No. of digital inputs	8	8
No. of relays/digital outputs	6/4	6/4
Selectable closing speed	Standard	Standard
Selectable opening speed	Standard	Standard

Options	Access Pro-L	Access Pro-H
Special colors	✓	✓
Standard barrier arm skirt		✓
Barrier arm skirt with climb-over prevention (height = 51 in)		✓
Barrier arm skirt with climb-over prevention (height = 70 in)		✓
Barrier arm extension set	✓	
Pendulum support*	✓	✓
Support post*	✓	✓
Barrier arm presence sensor	✓	✓
Barrier arm lock	✓	✓
Barrier arm illumination, red**	✓	✓
LED strips, red/green***	✓	✓
Warning lights	✓	✓
Hood lights	✓	✓
Key-operated switch	✓	✓
Radio module	✓	✓
Ethernet module	✓	✓
RS485 module	✓	✓
CAN module (counting)	✓	✓
Second detector module	✓	✓
GSM module	✓	✓
Photoelectric light barrier	✓	✓
Battery backup	✓	✓
Heater	✓	✓

* Barrier arms over 15 feet must use a pendulum support or support post
** Can only be used on back of barrier arm when used with climbover protection
*** Cannot be used with standard barrier arm skirt

MAGNETIC AUTOCONTROL
www.magnetic-access.com/usa

Standard barrier colors

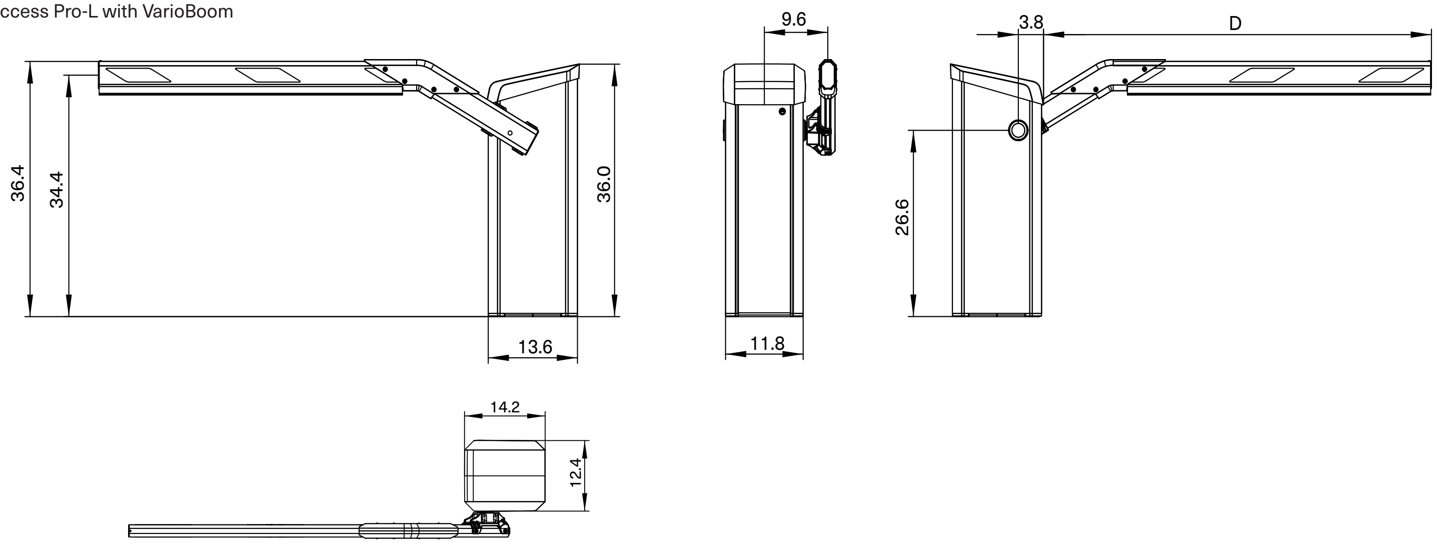
🟧	⬜	⬛	⬜
Orange (RAL 2000)	Light Grey (similar to RAL 9006)	Dark Grey (similar to RAL 9007)	White (similar to RAL 9010)

Standard door color

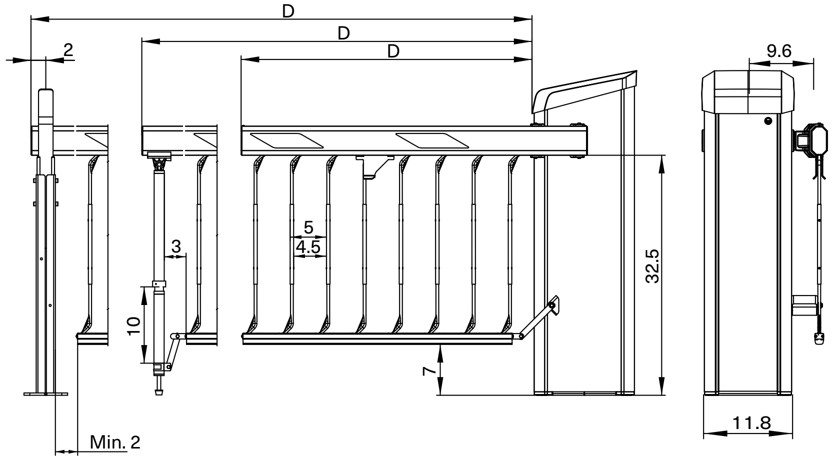
⬛
Black-Grey (Anthracite) (similar to RAL 7021)

Dimensional drawings

Access Pro-L with VarioBoom



Access Pro-H with standard barrier arm skirt



Complete dimensional drawings are available on request.

MAGNETIC®
ACCESS TO PROGRESS

Access to Progress

Magnetic stands for pioneering products – in every way. Our access control systems for vehicles or pedestrians clear the way for thousands of people every day – at car parks, toll gates, stations, airports and in buildings. Our technology is also pioneering, however: with innovative drives, intelligent control systems and well thought-out details it provides maximum safety and longevity. Are you also on the path to Magnetic?

Vehicle barriers

Access barriers
Parking barriers
Toll barriers
Traffic barriers
Special barriers

Pedestrian gates

Turnstiles

Swing gates
Tripod gates
Retractable gates
Wing gates

Terminals

Cars
Trucks

Germany
MAGNETIC AUTOCONTROL GMBH
Grienmatt 20
79650 Schopfheim
Phone +49 7622 695-5
Fax +49 7622 695-800
E-mail info@magnetic-germany.com

Australia
MAGNETIC AUTOMATION PTY LTD
38 Metrolink Circuit
Campbellfield, VIC 3061
Phone +61 3 9339 2900
E-mail info@magnetic-oz.com

Brazil
MAGNETIC AUTOCONTROL LTDA
Av. Salim Antônio Curiati, 136
04690-050 – São Paulo
Phone +55 11 5660 8500
E-mail info@magnetic-br.com

China
MAGNETIC CONTROL SYSTEMS CO., LTD
No. 3 Building, No. 51
Lane 1159, Kang Qiao (East) Road
Kang Qiao Industrial Zone, Shanghai
Phone +86 21 68182970
E-mail info@magnetic-cn.com

France
FAAC FRANCE
377 Rue Ferdinand Perrier
69808 St Priest Cedex
Phone +33 4 72 21 86 89
E-mail info@magnetic-fr.com

India
MAGNETIC AUTOCONTROL PVT LTD.
PRS Centre
Plot No. 373 to 376, 2nd Floor (West Wing)
1st Cross Street, Nehru Nagar
Old Mahabalipuram Road
Kottivakkam (Opp Rayala Technopark, Perungudi)
Chennai 600041
Phone +91 44 421 23297
E-mail info@magnetic-india.com

Middle East
FAAC MIDDLE EAST FZE
Dubai Silicon Oasis
PO Box 54886
Dubai
United Arab Emirates
Phone +971 4 3724193
E-mail info@magnetic-uae.com

N. and S. America (excl. Brazil)
FAAC INTERNATIONAL, INC
3160 Murell Road
Rockledge, FL 32955
USA
Phone +1 321 635 8585
E-mail info@magnetic-usa.com

Scandinavia
FAAC NORDIC AB
Box 125
284 22 Perstorp
Sweden
Phone +46 435 77 95 03
E-mail info@magnetic-nordic.com

Southeast Asia
MAGNETIC CONTROL SYSTEMS SDN. BHD
No. 17, Jalan Anggerik Mokara 31/54
Taman Perindustrian Kota Kemuning
40460 Shah Alam
Selangor Darul Ehsan
Malaysia
Phone +60 3 5123 0033
E-mail info@magnetic-malaysia.com

5806,0046 US_12.2016

MAGNETIC AUTOCONTROL
www.magnetic-access.com/usa

Member of FAAC group

FlashParking

FLASHBEACON

FRICTIONLESS BLUETOOTH TECHNOLOGY

Our proprietary Bluetooth beacon technology offers a modern frictionless access option for users. Users with the FlashParking mobile app can access garages and lots with the press of a button on their phone—a capability that entirely eliminates the need to roll down a window.

OVERVIEW

Modern Convenience

FlashBeacon is a proprietary patent-pending product developed by FlashParking that utilizes Bluetooth beacon technology to create a truly frictionless garage or lot access experience for monthly and transient users alike. As the only parking technology company in the industry who has a commercially viable frictionless Bluetooth access solution, FlashParking considers FlashBeacon as a core product that delivers the level of convenience that modern parkers seek in all aspects of their lives.

ENABLING SEEMLESS ENTRY AND EXIT
FlashParking
Jose Morales

How it Works

Our Bluetooth Beacon is different from the Bluetooth that connects your mobile device to a speaker system. The speaker and phone both put out a signal in the shape of a dome to find one another and connect. Our Bluetooth Beacon is embedded at the top of the parking equipment. It pulses a directional signal in the shape of a cone, 8 ft, in the direction of the parking lane. The beacon searches for the Bluetooth-enabled mobile device with the FlashParking app specifically angled at the driver's seat. Within seconds, the communication between the beacon and app are confirmed to grant access to the parking facility. Rolling down the window will become obsolete in smart facilities that team up with FlashParking.

INNOVATIVE USE CASES

Transient and Monthly Parkers works with

- Smart Station
- Mini-Smart Station

eParking Reservation works with

- Smart Station
- Mini-Smart Station

SDK Kit

- Embed FlashParking in custom apps

FEATURES

Frictionless Monthly and Transient Parking

For monthly parkers, the straightforward Bluetooth access process simply involves opening the FlashParking app, pressing a button, and immediately being permitted access in seconds. Without the need to roll down a window, scan a prox card, or wait for gates to vend, the convenience of Bluetooth access saves valuable time and effort for the parkers who use your parking facilities each day. FlashParking will roll out a frictionless transient feature in the FlashParking app later this year.

Watch Frictionless Bluetooth Access in Action
https://vimeo.com/340763243

Frictionless eParking Reservations

FlashParking has partnered with SpotHero and Arrive to offer comprehensive eParking reservation and access services. Users of these consumer-facing apps can utilize Bluetooth Beacon technology when they reserve spaces at garages with FlashParking solutions. After making a parking reservation on their phone ahead of time, these parkers will arrive at the designated garage and be permitted access once their phone connects to the Smart Station at the entry point.

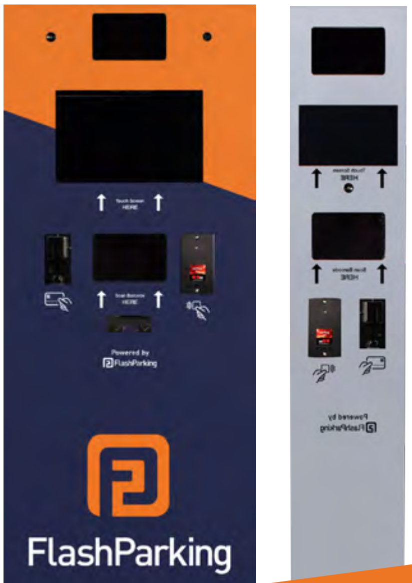
Software Development Kit

With our unique software development kit, any consumer-facing app—like SpotHero, Arrive, EVgo—or properties can also integrate FlashBeacon into their proprietary mobile app. Upon arriving at a FlashParking-equipped garage or lot after pre-reserving a space, users of a FlashBeacon-enabled program can gain access to a FlashParking-equipped garage through the respective mobile app. The frictionless nature of this transaction is a strong differentiator against traditional competitors and has the power to drive significant traffic to enabled garages and lots.

HARDWARE

FlashParking Mobile App

Our intuitive mobile app, available for iOS and Android devices, allows parkers to gain access to garages quickly and conveniently. Connecting directly to mobile payment options and other critical settings, the FlashParking app is a readily available means of communicating and interacting with parkers.



Smart Station/Mini-Smart Station

Both the FlashParking Full & Mini Smart Stations come equipped with Bluetooth beacon technology, which means that customers can opt to take advantage of the technology at any time.

MONTHLY PARKERS USE FLASHBEACON AT

Please Separate Parking Cards before scanning
VISITOR PARKING
TMC | TEXAS MEDICAL CENTER

Texas Medical Center

Thousands of monthly parkers at Texas Medical Center (TMC) use FlashBeacon technology each day to gain access to garages and lots. Utilizing this technology not only makes their parking experience more convenient, but also contributes to reducing congestion on critical internal roads by reducing the time it takes to get in and out of garages.

The City of Las Vegas

Monthly parkers in downtown Las Vegas also utilize our innovative Bluetooth beacon technology to enter and exit city garages. Largely employees of the municipality, these users interact with our technology to simplify their commutes and streamline the parking process.

FlashParking

HEADQUARTERS

FlashParking
3801 S. Capital of Texas Highway, Suite 250
Austin, TX 78704

SALES

sales@flashparking.com
800.213.3706

SUPPORT

support@flashparking.com
888.737.7465

FlashParking

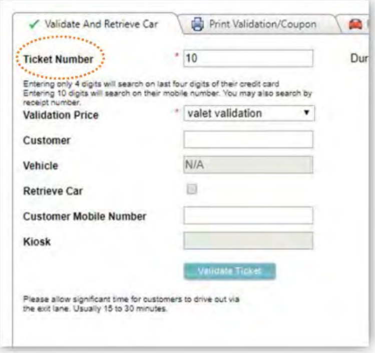
FlashParking's Flexible and Easy-to-Use Validation Platform is the Smart Way to Validate

Overview

Our web-based validation system powered by the FlashParking platform provides operators and asset owners an intelligent way to validate parking from any connected device with three different validation types: electronic, printed, and text-based.

Three Types of Validations

1. **Electronic Validations** are unique in that customers do not have to take any action for the validation to be processed; the validator simply accesses their FlashParking portal to perform the validation. The validator manually enters the customer's ticket number, sets the validation price, and then confirms the validation. The new, validated rate will then be automatically applied to the customer's ticket.



Ticket Number * 10

Entering only 4 digits will search on last four digits of their credit card
Entering 10 digits will search on their mobile number. You may also search by receipt number.

Validation Price * valet validation

Customer

Vehicle N/A

Retrieve Car □

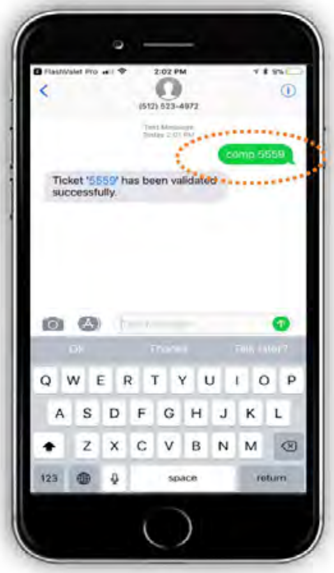
Customer Mobile Number

Kiosk

Please allow significant time for customers to drive out via the exit lane. Usually 15 to 30 minutes.

2. **Printed Validations** are a straightforward way for parking operators to serve visitors of the variety of different businesses it's garage or lot serves. With no need for special paper, individual and bulk barcode validations can be printed out Avery labels. Parkers can apply the validation to the back of their ticket that can be scanned at an exit or pay-on-foot kiosk after the original ticket. The validated amount will immediately be deducted from the user's balance.

3. **Validating by Text** is a convenient option for users as it eliminates the need for customers to keep track of printed validations and doesn't require validators to log into the portal each time. Validators' phone numbers first need to be added to the Admin Portal in order to gain validation capabilities. Pre-approved validators can send a customer's ticket number to a specific phone number associated with the location. The validator will then receive confirmation that the customer ticket has been validated.



comp 5559

Ticket '5559' has been validated successfully.

Validators and Managing User Rights

FlashParking's validation system allows you to offer different validations for different validators. The operator uses a unique user name/password to access the revenue control system to create validations and manage user rights for each validator.

Flexible to Meet Your Unique Venue Needs

Our exceptionally flexible validation system can provide multiple scenarios for validations. It can calculate the remaining balance if the parker exceeds the validated time and request payment, therefore allowing you to capture additional revenue.

Hardware

Self-Validator Mini-Smart Station
Perfect for busy retail storefronts or office buildings, our Self-Validating Mini-Smart Station enables parks to validate their parking without asking for assistance. To learn more, **CLICK HERE.**

Validation Wall Mount Station
Ideal for venues with tight spaces, the Wall Mount Smart Station configured a self-validator can be bolted to a wall or mounted to a pedestal. To learn more, **CLICK HERE.**

To learn more about the various capabilities of FlashParking's software, please visit:
https://www.flashparking.com/flashparcs/

What is PCI Compliance and what does it mean for Parking operators?

In 2006, the major payment cards (Visa, MasterCard, American Express, Discover and JCB International) developed the Payment Card Industry Data Security Standards (PCI DSS), a set of security standards designed to ensure that all companies that accept, process, store or transmit credit card information maintain a secure environment. When properly implemented and maintained, these security standards combat the risk of hackers and fraudulent charges.

While the PCI Council developed the framework for cardholder security, it's up to all merchants, both small and large, to build and maintain a secure network and systems. If a cardholder's information becomes compromised, it can result in more than a merchant or operator's tarnished reputation. It can lead to fraud losses, diminished sales, fines and penalties, legal costs, and more.

Best Practices of PCI DSS Compliance

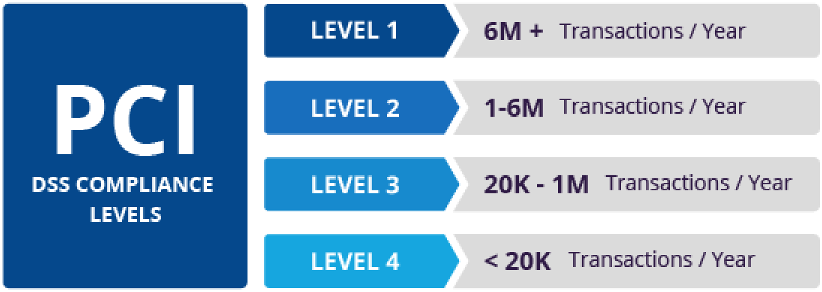
The best way to protect the safety of cardholder data is to make sure that the data is continually secure, from the moment a credit card reader captures data to when it flows into the payment system.

To achieve PCI DSS compliance a merchant or operator must take on the monstrous task of completing 12 requirements broken into 6 groups of various technical and operational tasks (see next page).

This is significantly different than using a PA DSS certified system or application. This level of certification simply implies that the system or application can support your own PCI-compliance program. There is simply no equivalence in PCI DSS and PA DSS certification.

How FlashParking Simplifies and Streamlines PCI DSS Compliance and Maintenance

At FlashParking, we are committed to delivering PCI DSS compliant technology that takes the burden of away from our customers. Our system is PCI DSS certified as a Level 1 Service Provider, which means we ensure that a payment processing system can handle millions of transactions daily in a reliable and safe environment. It is the highest level of PCI compliance available.



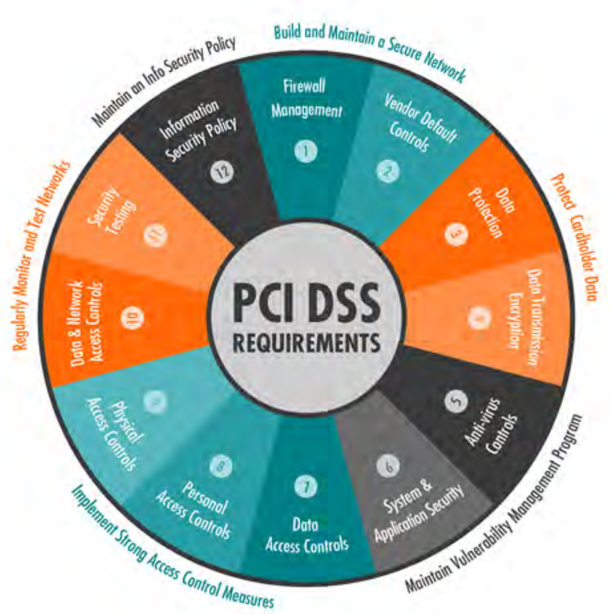
PCI DSS COMPLIANCE LEVELS

LEVEL 1	6M + Transactions / Year
LEVEL 2	1-6M Transactions / Year
LEVEL 3	20K - 1M Transactions / Year
LEVEL 4	< 20K Transactions / Year

We do so by building and maintaining secure networks and systems. As soon as customer swipes his/her credit card, the information stored on a credit card is encrypted at the head of the credit card reader and sent over to the payment gateway . We never store credit card information on our system, but all other data, such as transaction records, is stored in the Microsoft cloud.

We are experts at providing PCI DSS compliance for all equipment, hardware and software. An operator still has minimal responsibilities for maintaining compliance - you must develop a security policy and train employees to check the credit card reader once a week to make sure that a skimmer hasn't been installed on the device. Designed to look just like a credit card reader, a skimmer captures data before it goes into the real credit card reader. Once an employee verifies that the credit card reader is free of a skimmer, it's business as usual in a secure environment.

Complications of obtaining PCI DSS Compliance


Build and Maintain a Secure Network
Protect Cardholder Data
Maintain Vulnerability Management Program
Implement Strong Access Control Measures
Regularly Monitor and Test Networks
Maintain an Info Security Policy
Firewall Management
1
Vendor Default Controls
2
Data Protection
3
Data Transmission Encryption
4
Anti-virus Controls
5
System & Application Security
6
Data Access Controls
7
Personal Access Controls
8
Physical Access Controls
9
Data & Network Access Controls
10
Security Testing
11
Information Security Policy
12
PCI DSS
REQUIREMENTS

You can achieve PCI compliance in various ways, in the parking industry you normally have two:

1. A PA DSS certified application or system. This means that this system is capable of achieving PCI compliance if you follow the hundreds of guidelines and on-going maintenance that is required by PCI. This type of system will be hosted on-site and it is the parking provider's responsibility to ensure the system is maintained properly to achieve PA DSS compliance. Simply put, the burden lies on the parking operator to maintain PCI compliance.
2. A PCI DSS, Level 1 Service Provider such as FlashParking. In this case the Service Provider takes on the majority of the burden of maintaining compliance. This reduces your PCI scope significantly.

Meeting these requirements demands executing over 250 specific tasks, as well as documenting your process to do those tasks as well as documenting that they have been completed. Finally, you have to be audited. This is an annual certification, meaning every 365 days this process begins again.

There are 12 requirements for meeting the PCI DSS, broken into 6 groups:

Build and Maintain a Secure Network

Requirement 1: Install and maintain a firewall configuration to protect cardholder data
Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

Protect Cardholder Data

Requirement 3: Protect stored cardholder data
Requirement 4: Encrypt transmission of cardholder data across open, public networks

Maintain a Vulnerability Management Program

Requirement 5: Use and regularly update anti-virus software
Requirement 6: Develop and maintain secure systems and applications

Implement Strong Access Control Measures

Requirement 7: Restrict access to cardholder data by business need-to-know
Requirement 8: Assign a unique ID to each person with computer access
Requirement 9: Restrict physical access to cardholder data

Regularly Monitor and Test Networks

Requirement 10: Track and monitor all access to network resources and cardholder data
Requirement 11: Regularly test security systems and processes

Maintain an Information Security Policy

Requirement 12: Maintain a policy that addresses information security

Encryption and Data Flow Diagram

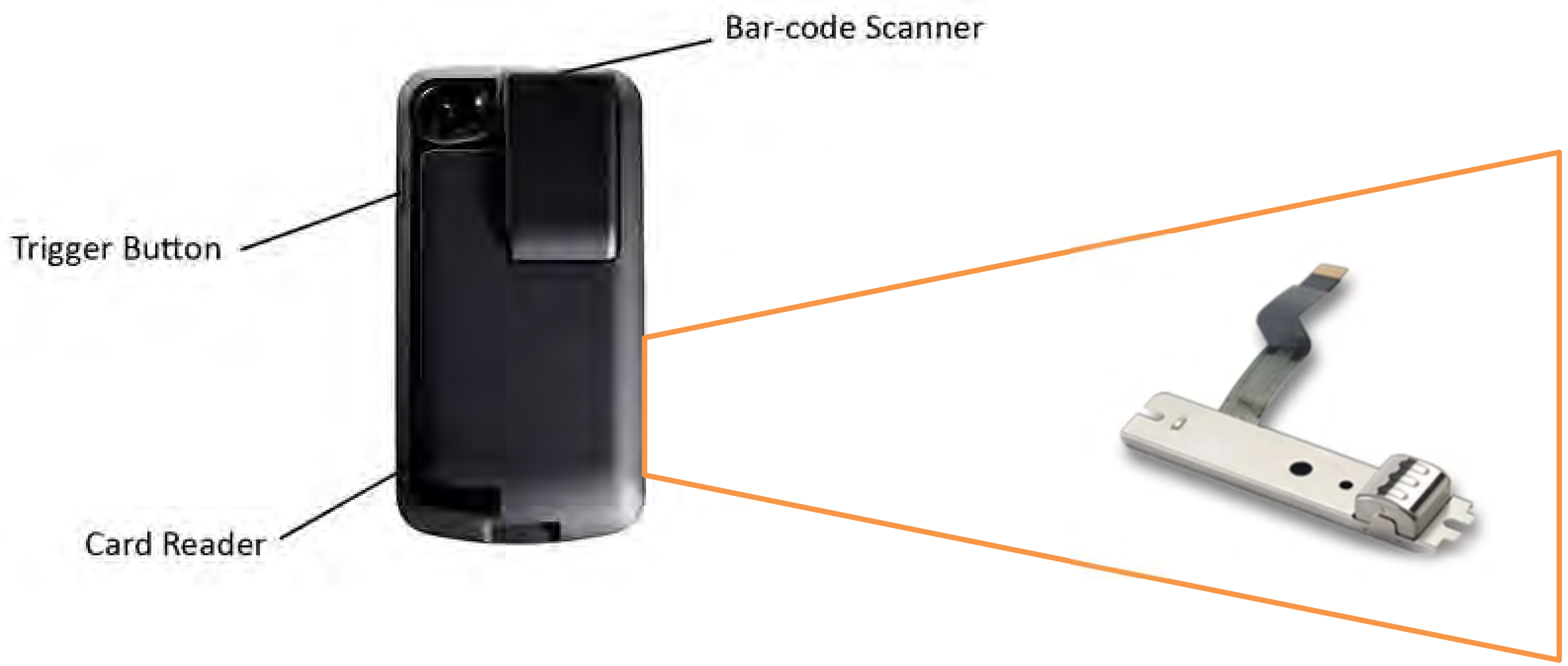
FlashParking

Windcave

USAepay

Confidential

Magnetic Head (Point to Point) Encryption – Linea Pro

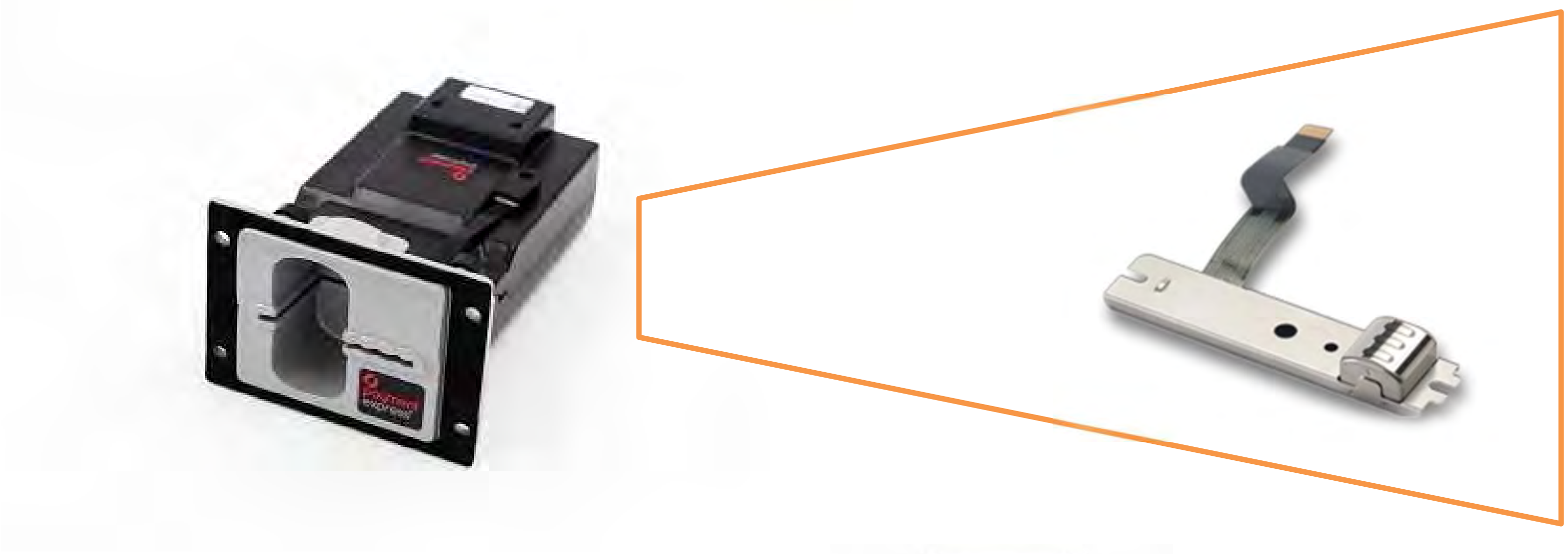


All credit card sensitive data will be encrypted at the point of swipe in the magnetic head using DUKPT (3DES-112, AES-128, AES-2560 encryption algorithms). Only our gateway partner USAePay has the keys to decrypt the sensitive data.

Magnetic Head (Point to Point) Encryption – Spectrum Air

All credit card sensitive data will be encrypted at the point of swipe in the magnetic head using DUKPT (3DES-112, AES-128, AES-2560 encryption algorithms). Only our gateway partner USAePay has the keys to decrypt the sensitive data.

Magnetic Head (Point to Point) Encryption – SCR200E

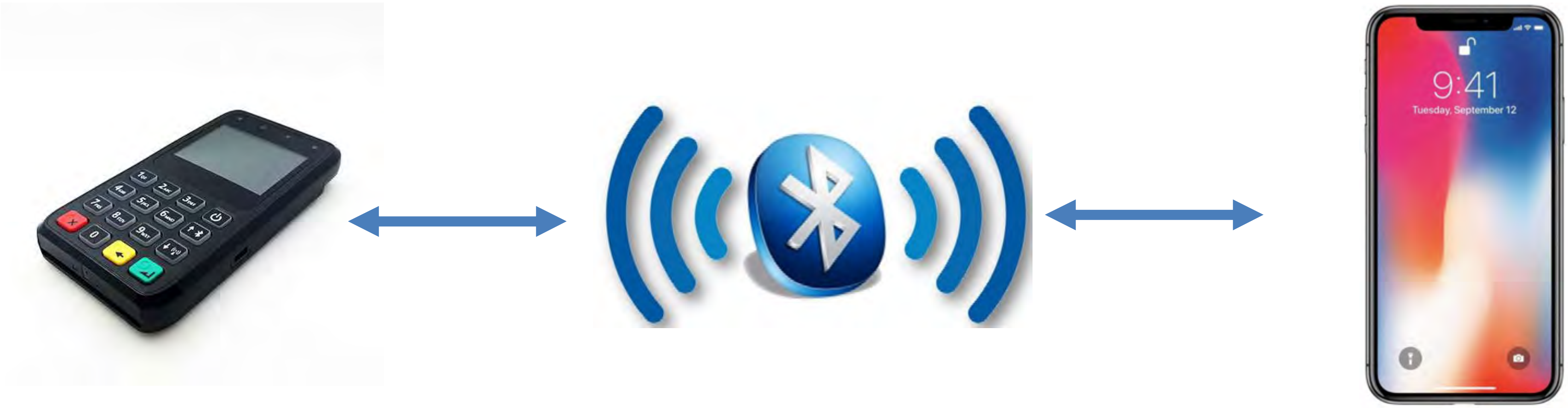


All credit card sensitive data will be encrypted at the point of swipe in the magnetic head using DUKPT (3DES-112, AES-128, AES-2560 encryption algorithms). Only our gateway partner Payment Express/WindCave has the keys to decrypt the sensitive data. This solution is also a PCI DSS - P2PE validated. Optional items: BFR contactless antenna for NFC payments and the SKP200E for pin entry.

Magnetic Head (Point to Point) Encryption – MP200

All credit card sensitive data will be encrypted at the point of swipe in the magnetic head or CHIP insert using DUKPT (3DES-112, AES-128, AES-2560 encryption algorithms). Only our gateway partner USAePay has the keys to decrypt the sensitive data.

MP200 – Bluetooth paired with Apple iOS device



The MP200 connects to an Apple iOS device via paired Bluetooth connection.

The MP200 uses Bluetooth encryption as follows: Encryption Mode 2 and Security Mode 4 - this means encryption is required for all traffic between the MP200 and the Apple iOS device.

Summary of Bluetooth encryption: (for more details please visit: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-121r1.pdf)

The encryption key provided to the encryption algorithm is produced using an internal key generator (KG). The KG produces stream cipher keys based on the 128-bit link key, which is a secret that is held in the Bluetooth devices; a 128-bit random number (EN_RAND); and the 96-bit ACO value. The ACO is produced during the authentication procedure, as shown in Figure 3-4. The Bluetooth encryption procedure is based on a stream cipher, E0. A key stream output is exclusive-ORed with the payload bits and sent to the receiving device. This key stream is produced using a cryptographic algorithm based on linear feedback shift registers (LFSRs).12 The encryption function takes the following as inputs: the master device address (BD_ADDR), the 128-bit random number (EN_RAND), a slot number based on the piconet clock, and an encryption key, which when combined initialize the LFSRs before the transmission of each packet, if encryption is enabled. The slot number used in the stream cipher changes with each packet; the ciphering engine is also reinitialized with each packet while the other variables remain static.

Secure Key Management/Injection Flow

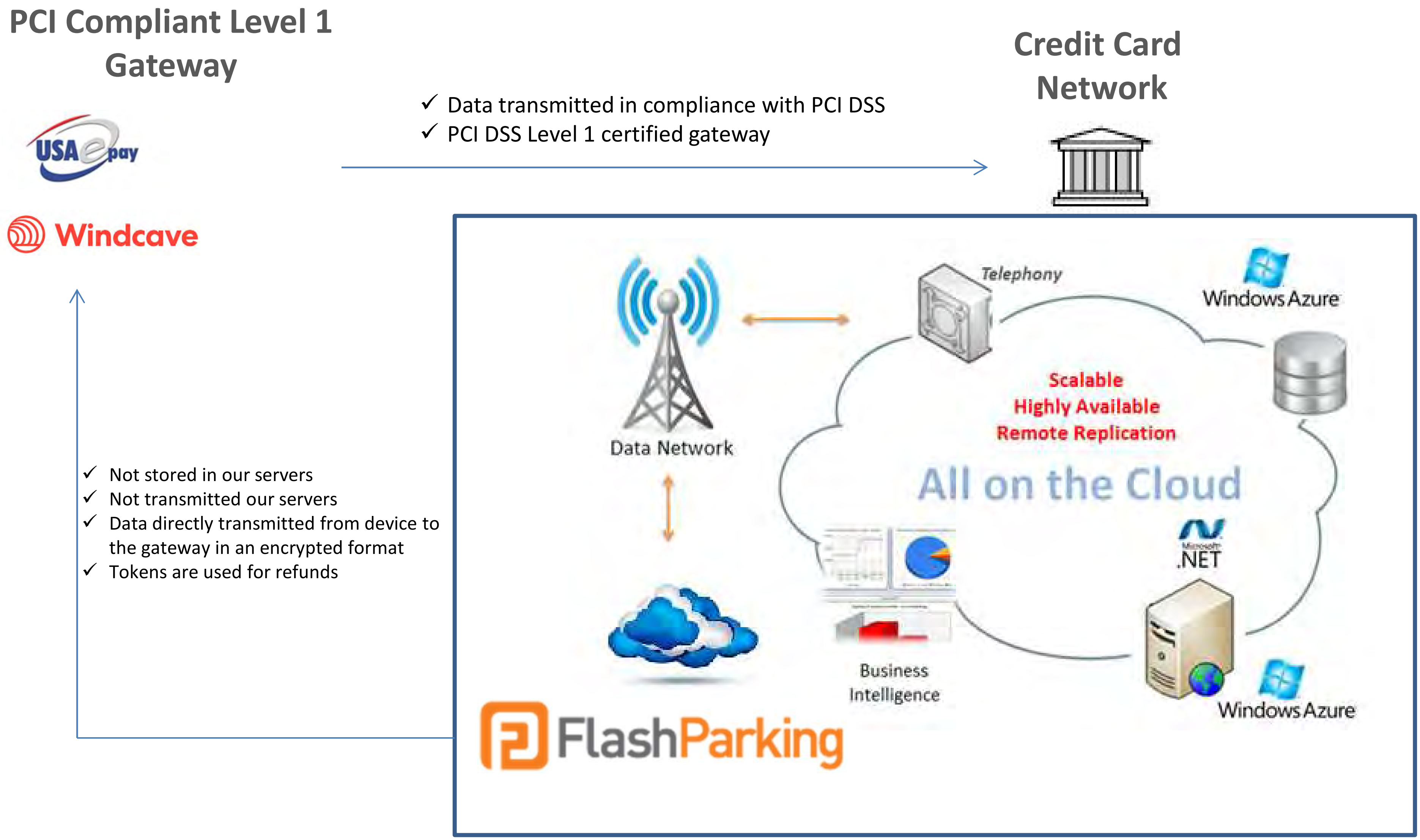
1-) Purchase credit card reader units from various vendors

2-) For Linea-pro's units are shipped directly to Spencer Technologies for the key injections process on each unit. For Spectrum Air those are injected with the keys at IDTech. For MP200, POSPORTAL is a certified KEY Injection facility and ships direct. For the SCR200 those are injected directly by Payment Express/WindCave.

3-) The units are then shipped to assembly line or final destination at customer sites

*POSPORTAL, IDTech and Spencer Technologies exchange encryption keys directly with USAePAY. For Payment Express, it's a P2PE validated solution, so they control all of the encryption keys.

FlashParking Platform



PCI Compliant Level 1 Gateway

- ✓ Data transmitted in compliance with PCI DSS
- ✓ PCI DSS Level 1 certified gateway

Credit Card Network

- ✓ Not stored in our servers
- ✓ Not transmitted our servers
- ✓ Data directly transmitted from device to the gateway in an encrypted format
- ✓ Tokens are used for refunds

device sends "card data" directly to the gateway without storing or transmitting via our servers / backend platform.

Card Swiped with Linea-Pro/Tab sleeve

2

PCI Compliant Level 1 Gateway

- ✓ Data transmitted in compliance with PCI DSS
- ✓ PCI DSS Level 1 certified gateway

3

Credit Card Network

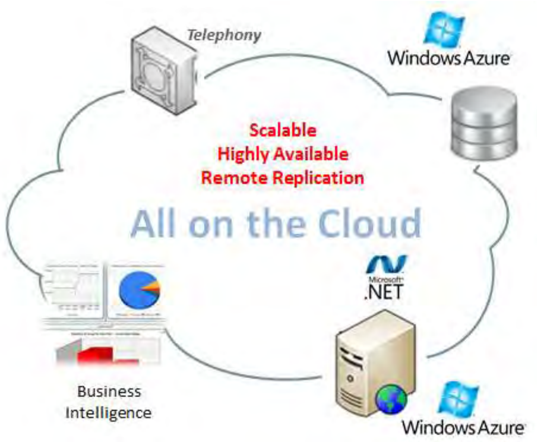
- ✓ Card Holder Data Encrypted
- ✓ SSL Encryption (TLS1.2)
- ✓ Standard Security procedures
- ✓ DUKPT (3DES-112, AES-128, AES-256 encryption algorithms)

FlashParking Platform

- ✓ No Card Data
- ✓ No Sensitive Data
- ✓ No Card Data transmitted
- ✓ Tokens are used for refunds

1

- ✓ Card swiped
- ✓ Not stored in our servers
- ✓ Not transmitted by our servers
- ✓ Data directly transmitted from device to the gateway in an encrypted format



Card Swiped with SCR200E

2

PCI Compliant Level 1 Gateway

Windcave

- ✓ Data transmitted in compliance with PCI DSS
- ✓ PCI DSS Level 1 certified gateway

3

Credit Card Network

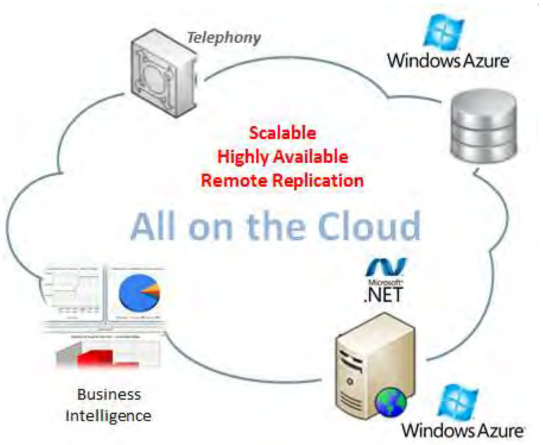
- ✓ Card Holder Data Encrypted
- ✓ SSL Encryption (TLS1.2)
- ✓ Standard Security procedures
- ✓ DUKPT (3DES-112, AES-128, AES-256 encryption algorithms)

FlashParking Platform

- ✓ No Card Data
- ✓ No Sensitive Data
- ✓ No Card Data transmitted
- ✓ Tokens are used for refunds

1

- ✓ Card swiped
- ✓ Not stored in our servers
- ✓ Not transmitted by our servers
- ✓ Data directly transmitted from device to the gateway in an encrypted format



Confidential

Card Swiped with Spectrum Air

2

PCI Compliant Level 1 Gateway

- ✓ Data transmitted in compliance with PCI DSS
- ✓ PCI DSS Level 1 certified gateway

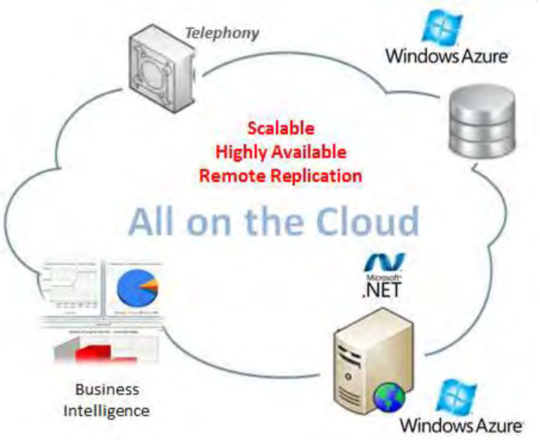
3

Credit Card Network

- ✓ Card Holder Data Encrypted
- ✓ SSL Encryption (TLS1.2)
- ✓ Standard Security procedures
- ✓ DUKPT (3DES-112, AES-128, AES-256 encryption algorithms)

FlashParking Platform

- ✓ No Card Data
- ✓ No Sensitive Data
- ✓ No Card Data transmitted
- ✓ Tokens are used for refunds



1

- ✓ Card swiped
- ✓ Not stored in our servers
- ✓ Not transmitted by our servers
- ✓ Data directly transmitted from device to the gateway in an encrypted format

Confidential

Card Swiped or Chip Inserted with MP200

2

PCI Compliant Level 1 Gateway

USAepay

- ✓ Data transmitted in compliance with PCI DSS
- ✓ PCI DSS Level 1 certified gateway

3

Credit Card Network

- ✓ Card Holder Data Encrypted
- ✓ SSL Encryption (TLS1.2)
- ✓ Standard Security procedures
- ✓ DUKPT (3DES-112, AES-128, AES-256 encryption algorithms)

1

- ✓ Card swiped or Chip Inserted
- ✓ Not stored in our servers
- ✓ Not transmitted by our servers
- ✓ Data directly transmitted from device to the gateway in an encrypted format

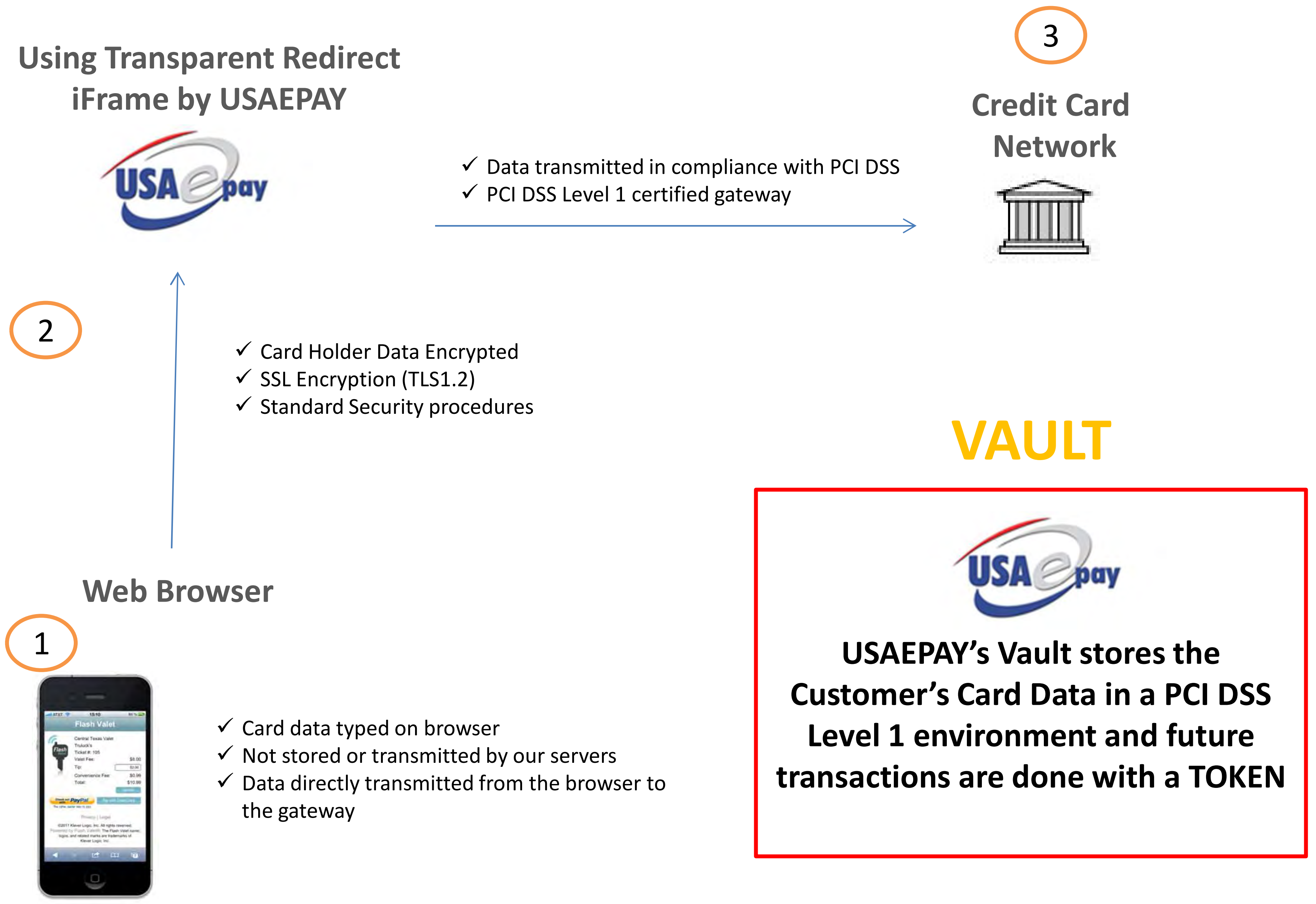
FlashParking Platform

- ✓ No Card Data
- ✓ No Sensitive Data
- ✓ No Card Data transmitted
- ✓ Tokens are used for refunds

Telephony
Windows Azure
Scalable
Highly Available
Remote Replication
All on the Cloud
Microsoft .NET
Business Intelligence
Windows Azure

Confidential

Online or App based Payments



3

Credit Card Network

Using Transparent Redirect iFrame by USAEPAY

- ✓ Data transmitted in compliance with PCI DSS
- ✓ PCI DSS Level 1 certified gateway

2

- ✓ Card Holder Data Encrypted
- ✓ SSL Encryption (TLS1.2)
- ✓ Standard Security procedures

VAULT

USAEPAY's Vault stores the Customer's Card Data in a PCI DSS Level 1 environment and future transactions are done with a TOKEN

Web Browser

1

- ✓ Card data typed on browser
- ✓ Not stored or transmitted by our servers
- ✓ Data directly transmitted from the browser to the gateway

Security
Standards Council

Payment Card Industry (PCI)
Data Security Standard

Attestation of Compliance for Onsite Assessments – Service Providers

Version 3.2.1

June 2018

Security Standards Council

Section 1: Assessment Information

Instructions for Submission

This Attestation of Compliance must be completed as a declaration of the results of the service provider's assessment with the *Payment Card Industry Data Security Standard Requirements and Security Assessment Procedures (PCI DSS).* Complete all sections: The service provider is responsible for ensuring that each section is completed by the relevant parties, as applicable. Contact the requesting payment brand for reporting and submission procedures.

Part 1. Service Provider and Qualified Security Assessor Information

Part 1a. Service Provider Organization Information

Company Name:	FlashParking, Inc.		DBA (doing business as):		
Contact Name:	Juan Rodriquez		Title:	CEO	
Telephone:	512.402.8960		E-mail:	juan.rodriguez@flashparking.com	
Business Address:	3801 South Capital of Texas Highway, Ste. 250		City:	Austin	
State/Province:	Texas	Country:	US	Zip:	78704
URL:	www.flashparking.com				

Part 1b. Qualified Security Assessor Company Information (if applicable)

Company Name:	UHY LLP				
Lead QSA Contact Name:	Richard Peters		Title:	Principal	
Telephone:	713.325.7870		E-mail:	rpeters@uhy-us.com	
Business Address:	10613 W Sam Houston Pkwy North, Ste. 175		City:	Houston	
State/Province:	Texas	Country:	US	Zip:	77064
URL:	www.uhy-us.com				

PCI Security Standards Council

Part 2. Executive Summary

Part 2a. Scope Verification

Services that were INCLUDED in the scope of the PCI DSS Assessment (check all that apply):

Name of service(s) assessed:	FlashValet, FlashMobile, FlashPARCS, and associated Website /Frames used for mobile payments and online payments

Type of service(s) assessed:

Hosting Provider:

□ Applications / software
□ Hardware
□ Infrastructure / Network
□ Physical space (co-location)
□ Storage
□ Web
□ Security services
□ 3-D Secure Hosting Provider
□ Shared Hosting Provider
□ Other Hosting (specify):

Managed Services (specify):

□ Systems security services
□ IT support
□ Physical security
□ Terminal Management System
☒ Other services (specify):
Software-as-a-Service (SaaS

Payment Processing:

□ POS / card present
□ Internet / e-commerce
□ MOTO / Call Center
□ ATM
□ Other processing (specify):

□ Account Management	□ Fraud and Chargeback	□ Payment Gateway/Switch
□ Back-Office Services	□ Issuer Processing	□ Prepaid Services
□ Billing Management	□ Loyalty Programs	□ Records Management
□ Clearing and Settlement	□ Merchant Services	□ Tax/Government Payments
□ Network Provider		
□ Others (specify):		

***Note:** These categories are provided for assistance only, and are not intended to limit or predetermine an entity's service description. If you feel these categories don't apply to your service, complete "Others." If you're unsure whether a category could apply to your service, consult with the applicable payment brand.*

Part 2a. Scope Verification *(continued)*

Services that are provided by the service provider but were *NOT INCLUDED* in the scope of the PCI DSS Assessment (check all that apply):

Name of service(s) not assessed:	None

Type of service(s) not assessed:

Hosting Provider:

- □ Applications / software
- □ Hardware
- □ Infrastructure / Network
- □ Physical space (co-location)
- □ Storage
- □ Web
- □ Security services
- □ 3-D Secure Hosting Provider
- □ Shared Hosting Provider
- □ Other Hosting (specify):

Managed Services (specify):

- □ Systems security services
- □ IT support
- □ Physical security
- □ Terminal Management System
- □ Other services (specify):

Payment Processing:

- □ POS / card present
- □ Internet / e-commerce
- □ MOTO / Call Center
- □ ATM
- □ Other processing (specify):

□ Account Management	□ Fraud and Chargeback	□ Payment Gateway/Switch
□ Back-Office Services	□ Issuer Processing	□ Prepaid Services
□ Billing Management	□ Loyalty Programs	□ Records Management
□ Clearing and Settlement	□ Merchant Services	□ Tax/Government Payments
□ Network Provider		

□ Others (specify):

Provide a brief explanation why any checked services were not included in the assessment:	

Part 2b. Description of Payment Card Business	
Describe how and in what capacity your business stores, processes, and/or transmits cardholder data.	None, FlashParking does not store, process, or transmit CHD. By utilizing remote key injection and encryption at the instant a credit card is swiped or dipped into a FlashParking system, there is no possibility to decrypt or intercept any CHD.
Describe how and in what capacity your business is otherwise involved in or has the ability to impact the security of cardholder data.	The assessment focused on the FlashValet, FlashPARCS and FlashMobile SaaS offering: FlashValet, FlashPARCS and FlashMobile are utilized by parking operators to manage parking operations which include the acceptance of credit cards. Credit cards are swiped at the parking operator device where the credit card number is encrypted immediately at the SLED and transmitted directly to USAePay (a PCI Compliant payment gateway). USAePay provides tokenized values back which can be used instead of the PAN for further transactions (such as refunds). On some units, a Payment Express EMV reader is utilized in a similar process. These devices are encrypted immediately when the card is dipped and FlashParking has no access to the decryption keys. FlashParking has no access to decryption keys whatsoever for any device. CHD is not stored on the local device, the SaaS applications, or any FlashParking servers. In addition to the SaaS offering, FlashValet, FlashPARCS and FlashMobile allow consumers to pay for parking services using their personal mobile devices. A consumer will utilize the service and a text message is sent which directs the consumer to the USAePay pay page (a PCI Compliant payment gateway) via an iFrame redirect. Consumers then enter credit card information, which is posted directly into USAePay infrastructure. Consumers have an option to store their credit card for future use. If a consumer selects this option, USAePay will issue a token back, which is stored by FlashParking. Furthermore, a consumer can visit a website and purchase monthly parking permits; this also uses an iFrame directly to USAePay. Again, CHD is not stored on the local device, the SaaS applications, or any FlashParking servers.

Part 2c. Locations

List types of facilities (for example, retail outlets, corporate offices, data centers, call centers, etc.) and a summary of locations included in the PCI DSS review.

Type of facility:	Number of facilities of this type	Location(s) of facility (city, country):
Example: Retail outlets	*3*	*Boston, MA, USA*
FlashParking Corporate HQ	1	Austin, Texas
Microsoft Azure	1	Azure Cloud

Part 2d. Payment Applications

Does the organization use one or more Payment Applications? □ Yes ☑ No

Provide the following information regarding the Payment Applications your organization uses:

Payment Application Name	Version Number	Application Vendor	Is application PA-DSS Listed?	PA-DSS Listing Expiry date (if applicable)
None			□ Yes □ No	
			□ Yes □ No	
			□ Yes □ No	
			□ Yes □ No	
			□ Yes □ No	
			□ Yes □ No	

Part 2e. Description of Environment

Provide a ***high-level*** description of the environment covered by this assessment. *For example:* • *Connections into and out of the cardholder data environment (CDE).* • *Critical system components within the CDE, such as POS devices, databases, web servers, etc., and any other necessary payment components, as applicable.*	The scope of this assessment focused on the hardware, software, and applications provided in the SaaS offering, the flow of data, and the associated processes. The parking operator and consumer devices and networks were excluded from the scope of the review. Neither FlashParking employees nor its customers have access to CHD once it has been swiped or dipped. USAePay and Payment Express, as PCI compliant service providers, provide a majority of the components related to CHD security.
Does your business use network segmentation to affect the scope of your PCI DSS environment? *(Refer to "Network Segmentation" section of PCI DSS for guidance on network segmentation)*	□ Yes ☒ No

Part 2f. Third-Party Service Providers

Does your company have a relationship with a Qualified Integrator & Reseller (QIR) for the purpose of the services being validated?	□ Yes ☒ No

If Yes:

Name of QIR Company:	Not applicable
QIR Individual Name:	
Description of services provided by QIR:	

Does your company have a relationship with one or more third-party service providers (for example, Qualified Integrator Resellers (QIR), gateways, payment processors, payment service providers (PSP), web-hosting companies, airline booking agents, loyalty program agents, etc.) for the purpose of the services being validated?	☒ Yes □ No

If Yes:

Name of service provider:	**Description of services provided:**
USAePay	Payment Gateway
Microsoft Azure	Platform as a Service (PaaS)
Payment Express	Payment Gateway

Note: Requirement 12.8 applies to all entities in this list.

Part 2g. Summary of Requirements Tested

For each PCI DSS Requirement, select one of the following:

- **Full** – The requirement and all sub-requirements of that requirement were assessed, and no sub-requirements were marked as "Not Tested" or "Not Applicable" in the ROC.
- **Partial** – One or more sub-requirements of that requirement were marked as "Not Tested" or "Not Applicable" in the ROC.
- **None** – All sub-requirements of that requirement were marked as "Not Tested" and/or "Not Applicable" in the ROC.

For all requirements identified as either "Partial" or "None," provide details in the "Justification for Approach" column, including:

- Details of specific sub-requirements that were marked as either "Not Tested" and/or "Not Applicable" in the ROC
- Reason why sub-requirement(s) were not tested or not applicable

***Note:** One table to be completed for each service covered by this AOC. Additional copies of this section are available on the PCI SSC website.*

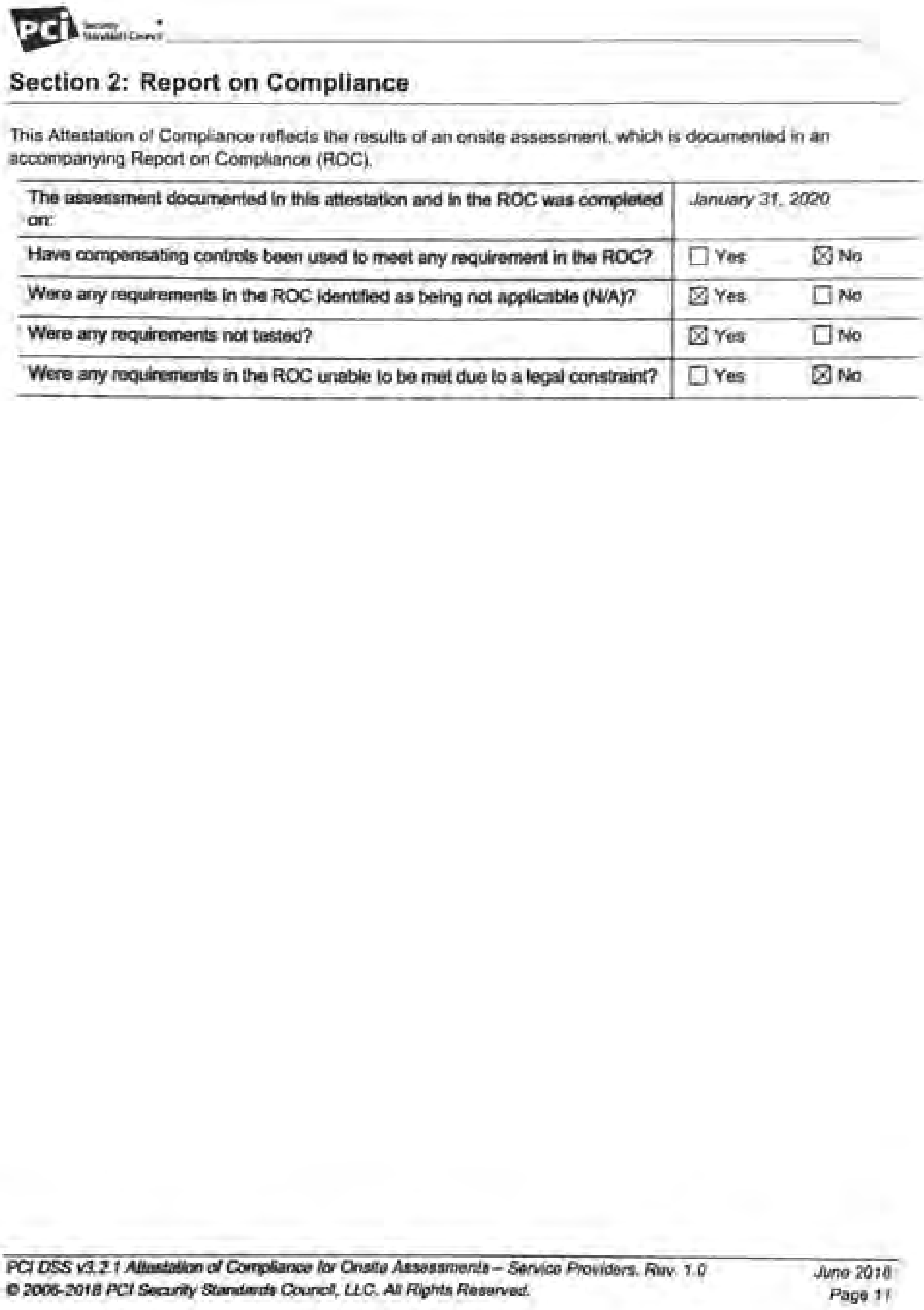
Name of Service Assessed:	FlashValet, FlashMobile, FlashPARCS, and associated Website iFrames

PCI DSS Requirement	**Details of Requirements Assessed**			
	Full	**Partial**	**None**	**Justification for Approach** (Required for all "Partial" and "None" responses. Identify which sub-requirements were not tested and the reason.)
Requirement 1:	□	□	☒	Assessor confirmed through interview, document inspection, and hardware/software assessment that all payment processing is performed directly to USAePay or Payment Express (PCI compliant service providers) from SaaS deployment. The transaction is encrypted at the SLED or dip and transmitted directly to USAePay or Payment Express. No CHD is stored, transmitted, or processed within the SaaS solution or FlashParking local network. Processing utilizes USAePay or Payment Express protocols and payment functions, which have been found PCI compliant. FlashParking employees have no access decryption keys and as such have no access to CHD. Once confirmed, no further testing was performed in these areas.
Requirement 2:	□	□	☒	Assessor confirmed through interview, document inspection, and hardware/software assessment that all payment processing is performed directly to USAePay or Payment Express (PCI compliant service providers) from SaaS deployment. The transaction is encrypted at the SLED or dip and transmitted directly to USAePay or Payment Express. No CHD is stored, transmitted, or processed within the SaaS solution or FlashParking local network. Processing utilizes USAePay or Payment Express protocols and payment functions, which have

				been found PCI compliant. FlashParking employees have no access decryption keys and as such have no access to CHD. Once confirmed, no further testing was performed in these areas.
Requirement 3:	□	☒	□	Testing was performed in this area, but several areas of key management were determined to be not applicable. It was determined that FlashParking has no access to decryption keys or CHD in any capacity. Once determined, no further testing was performed around key management.
Requirement 4:	□	□	☒	Assessor performed testing and analysis and determined that wireless is not in scope for PCI. There is no access to CHD or decryption keys in any capacity including wired and wireless networks.
Requirement 5:	□	□	☒	Assessor confirmed through interview, document inspection, and hardware/software assessment that all payment processing is performed directly to USAePay or Payment Express (PCI compliant service providers) from SaaS deployment. The transaction is encrypted at the SLED or dip and transmitted directly to USAePay or Payment Express. No CHD is stored, transmitted, or processed within the SaaS solution or FlashParking local network. Processing utilizes USAePay or Payment Express protocols and payment functions, which have been found PCI compliant. FlashParking employees have no access decryption keys and as such have no access to CHD. Once confirmed, no further testing was performed in these areas.
Requirement 6:	□	☒	□	Some controls were considered not applicable because the assessor confirmed the areas were not in scope for testing based upon interview, document inspection, and hardware/software assessment performed .
Requirement 7:	□	□	☒	Assessor confirmed through interview, document inspection, and hardware/software assessment that all payment processing is performed directly to USAePay or Payment Express (PCI compliant service providers) from SaaS deployment. The transaction is encrypted at the SLED or dip and transmitted directly to USAePay or Payment Express. No CHD is stored, transmitted, or processed within the SaaS solution or FlashParking local network. Processing utilizes USAePay or Payment Express protocols and payment functions, which have been found PCI compliant. FlashParking employees have no access decryption keys and as such have no access to CHD. Once confirmed, no further testing was performed in these areas.

Requirement 8:	□	□	☒	Assessor confirmed through interview, document inspection, and hardware/software assessment that all payment processing is performed directly to USAePay or Payment Express (PCI compliant service providers) from SaaS deployment. The transaction is encrypted at the SLED or dip and transmitted directly to USAePay or Payment Express. No CHD is stored, transmitted, or processed within the SaaS solution or FlashParking local network. Processing utilizes USAePay or Payment Express protocols and payment functions, which have been found PCI compliant. FlashParking employees have no access decryption keys and as such have no access to CHD. Once confirmed, no further testing was performed in these areas.
Requirement 9:	□	□	☒	Assessor confirmed through interview, document inspection, and hardware/software assessment that all payment processing is performed directly to USAePay or Payment Express (PCI compliant service providers) from SaaS deployment. The transaction is encrypted at the SLED or dip and transmitted directly to USAePay or Payment Express. No CHD is stored, transmitted, or processed within the SaaS solution or FlashParking local network. Processing utilizes USAePay or Payment Express protocols and payment functions, which have been found PCI compliant. FlashParking employees have no access decryption keys and as such have no access to CHD. Once confirmed, no further testing was performed in these areas.
Requirement 10:	□	□	☒	Assessor confirmed through interview, document inspection, and hardware/software assessment that all payment processing is performed directly to USAePay or Payment Express (PCI compliant service providers) from SaaS deployment. The transaction is encrypted at the SLED or dip and transmitted directly to USAePay or Payment Express. No CHD is stored, transmitted, or processed within the SaaS solution or FlashParking local network. Processing utilizes USAePay or Payment Express protocols and payment functions, which have been found PCI compliant. FlashParking employees have no access decryption keys and as such have no access to CHD. Once confirmed, no further testing was performed in these areas..
Requirement 11:	□	☒	□	Some controls were considered not applicable because the assessor confirmed the areas were not in scope for testing based upon interview, document inspection, and hardware/software assessment performed.
Requirement 12:	□	☒	□	Some controls were considered not applicable because the assessor confirmed the areas were not in scope for testing

				based upon interview, document inspection, and hardware/software assessment performed .
Appendix A1:	□	□	☒	Not applicable, not a shared hosting provider
Appendix A2:	□	□	☒	Not applicable



Section 2: Report on Compliance

This Attestation of Compliance reflects the results of an onsite assessment, which is documented in an accompanying Report on Compliance (ROC).

The assessment documented in this attestation and in the ROC was completed on:	*January 31, 2020*	
Have compensating controls been used to meet any requirement in the ROC?	□ Yes	☒ No
Were any requirements in the ROC identified as being not applicable (N/A)?	☒ Yes	□ No
Were any requirements not tested?	☒ Yes	□ No
Were any requirements in the ROC unable to be met due to a legal constraint?	□ Yes	☒ No

Section 3: Validation and Attestation Details

Part 3. PCI DSS Validation

This AOC is based on results noted in the ROC dated *January 31, 2020*.

Based on the results documented in the ROC noted above, the signatories identified in Parts 3b-3d, as applicable, assert(s) the following compliance status for the entity identified in Part 2 of this document (***check one***):

☒ **Compliant:** All sections of the PCI DSS ROC are complete, all questions answered affirmatively resulting in an overall **COMPLIANT** rating, thereby FlashParking, Inc. has demonstrated full compliance with the PCI DSS.

□ **Non-Compliant:** Not all sections of the PCI DSS ROC are complete, or not all questions are answered affirmatively, resulting in an overall **NON-COMPLIANT** rating, thereby *(Service Provider Company Name)* has not demonstrated full compliance with the PCI DSS.

Target Date for Compliance:

An entity submitting this form with a status of Non-Compliant may be required to complete the Action Plan in Part 4 of this document. *Check with the payment brand(s) before completing Part 4.*

□ **Compliant but with Legal exception:** One or more requirements are marked "Not in Place" due to a legal restriction that prevents the requirement from being met. This option requires additional review from acquirer or payment brand.

If checked, complete the following:

Affected Requirement	Details of how legal constraint prevents requirement being met

Part 3a. Acknowledgement of Status

Signatory(s) confirms:
(Check all that apply)

☒ The ROC was completed according to the *PCI DSS Requirements and Security Assessment Procedures*, Version 3.2.1, and was completed according to the instructions therein.

☒ All information within the above-referenced ROC and in this attestation fairly represents the results of my assessment in all material respects.

☒ I have confirmed with my payment application vendor that my payment system does not store sensitive authentication data after authorization.

☒ I have read the PCI DSS and I recognize that I must maintain PCI DSS compliance, as applicable to my environment, at all times.

☒ If my environment changes, I recognize I must reassess my environment and implement any additional PCI DSS requirements that apply.

Part 3a. Acknowledgement of Status *(continued)*	
☒	No evidence of full track data[1], CAV2, CVC2, CID, or CVV2 data[2], or PIN data[3] storage after transaction authorization was found on ANY system reviewed during this assessment.
☐	ASV scans are being completed by the PCI SSC Approved Scanning Vendor *Not applicable*

Part 3b. Service Provider Attestation	
Signature of Service Provider Executive Officer ↑	*Date:* [redacted]
Service Provider Executive Officer Name: Juan Rodriguez	*Title:* CEO

Part 3c. Qualified Security Assessor (QSA) Acknowledgement (if applicable)	
If a QSA was involved or assisted with this assessment, describe the role performed:	QSA performed full Level 1 service provider assessment as well as application penetration testing for FlashValet, FlashPARCS, and FlashMobile and associated websites.

Signature of Duly Authorized Officer of QSA Company ↑	*Date:* [redacted]
Duly Authorized Officer Name: Richard Peters, QSA	*QSA Company:* UHY LLP

Part 3d. Internal Security Assessor (ISA) Involvement (if applicable)	
If an ISA(s) was involved or assisted with this assessment, identify the ISA personnel and describe the role performed:	N/A

[1] Data encoded in the magnetic stripe or equivalent data on a chip used for authorization during a card-present transaction. Entities may not retain full track data after transaction authorization. The only elements of track data that may be retained are primary account number (PAN), expiration date, and cardholder name.

[2] The three- or four-digit value printed by the signature panel or on the face of a payment card used to verify card-not-present transactions.

[3] Personal identification number entered by cardholder during a card-present transaction, and/or encrypted PIN block present within the transaction message.

Part 4. Action Plan for Non-Compliant Requirements

Select the appropriate response for "Compliant to PCI DSS Requirements" for each requirement. If you answer "No" to any of the requirements, you may be required to provide the date your Company expects to be compliant with the requirement and a brief description of the actions being taken to meet the requirement.

Check with the applicable payment brand(s) before completing Part 4.

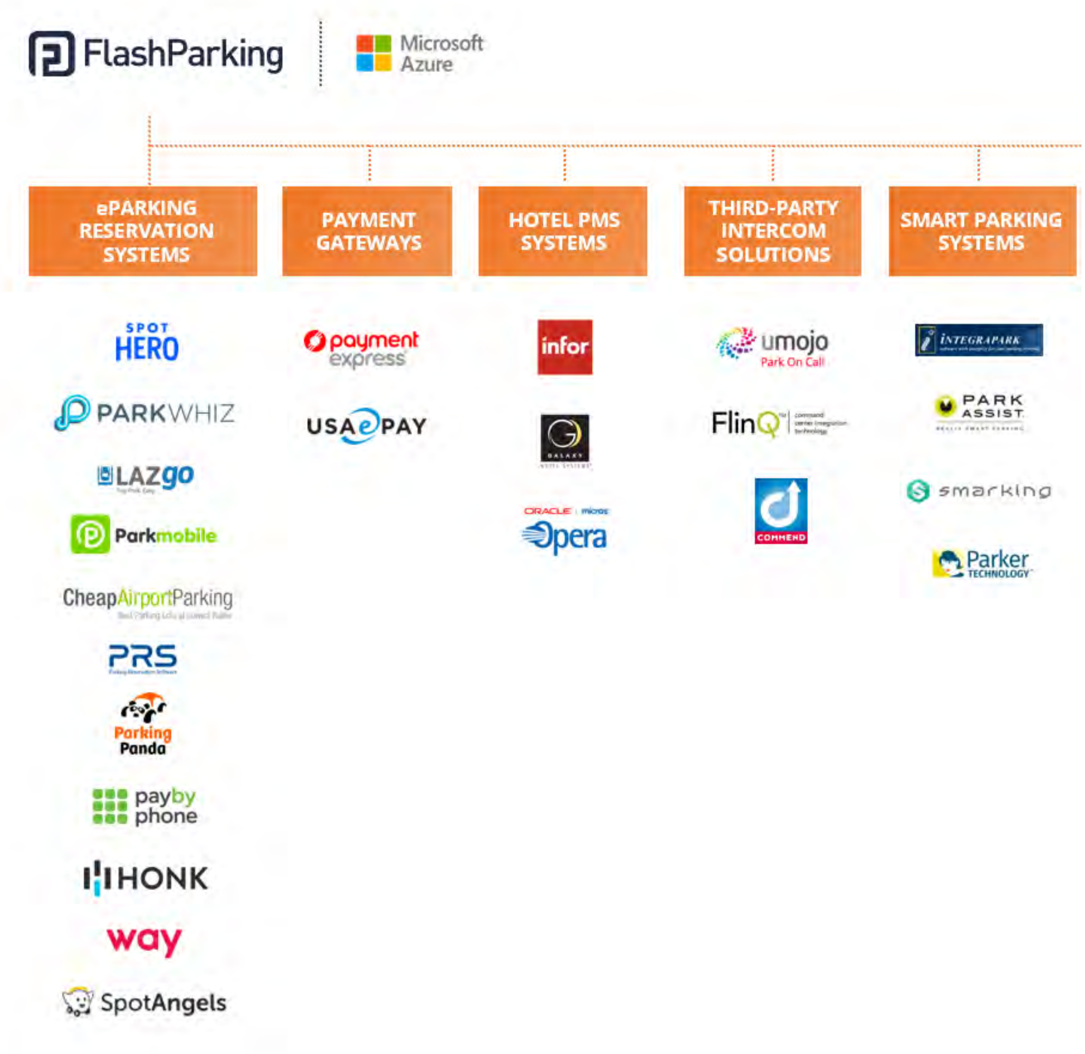
PCI DSS Requirement	Description of Requirement	Compliant to PCI DSS Requirements (Select One)		Remediation Date and Actions (If "NO" selected for any Requirement)
		YES	NO	
1	Install and maintain a firewall configuration to protect cardholder data	☒	□	
2	Do not use vendor-supplied defaults for system passwords and other security parameters	☒	□	
3	Protect stored cardholder data	☒	□	
4	Encrypt transmission of cardholder data across open, public networks	☒	□	
5	Protect all systems against malware and regularly update anti-virus software or programs	☒	□	
6	Develop and maintain secure systems and applications	☒	□	
7	Restrict access to cardholder data by business need to know	☒	□	
8	Identify and authenticate access to system components	☒	□	
9	Restrict physical access to cardholder data	☒	□	
10	Track and monitor all access to network resources and cardholder data	☒	□	
11	Regularly test security systems and processes	☒	□	
12	Maintain a policy that addresses information security for all personnel	☒	□	
Appendix A1	Additional PCI DSS Requirements for Shared Hosting Providers	□	□	N/A
Appendix A2	Additional PCI DSS Requirements for Entities using SSL/early TLS for Card-Present POS POI Terminal Connections	□	□	N/A

DISCOVER JCB mastercard VISA

MULTI-SITE API TECHNOLOGY

FlashParking's technology allows for multi-site APIs:

- ✓ Standard open API framework allows for ease of integrations
- ✓ Multi-lingual | Multi-currency | Multi-control for ease of international deployments
- ✓ Customized solutions unique to venue and/or parking operator



How to Pull a Report

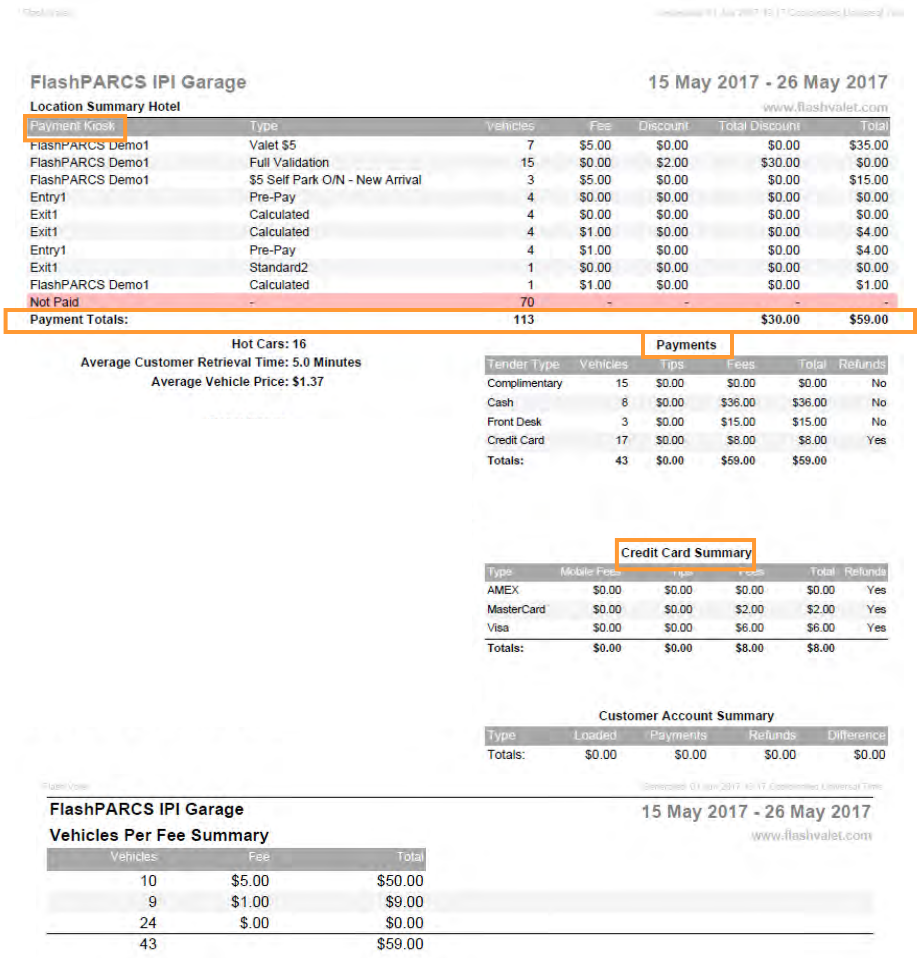
1. Log into portal.flashvalet.com
2. Select Reports tab on top left
3. Scroll down to select the desired report
4. Select the desired time/date range to run the report
5. Select Submit

Recommended Reports

Location Summary Hotel	FlashPARCS Vend Exceptions	Electronic Payments
Location Trans Detail	Location Issued Ticket Detail (xls)	eValidation by Date and Validator
Contact Center Detail	Occupancy Per Hour (PARCS)	Kiosk Summary

Location Summary Hotel

This report provides an executive-level summary of tickets processed per price per kiosk. It also provides a payment summary broken down by tender type and includes a sub-report that provides the number of vehicles processed per fee.



FlashPARCS IPI Garage
15 May 2017 - 26 May 2017
Location Summary Hotel
www.flashvalet.com

Payment Kiosk	Type	Vehicles	Fee	Discount	Total Discount	Total
FlashPARCS Demo1	Valet $5	7	$5.00	$0.00	$0.00	$35.00
FlashPARCS Demo1	Full Validation	15	$0.00	$2.00	$30.00	$0.00
FlashPARCS Demo1	$5 Self Park O/N - New Arrival	3	$5.00	$0.00	$0.00	$15.00
Entry1	Pre-Pay	4	$0.00	$0.00	$0.00	$0.00
Exit1	Calculated	4	$0.00	$0.00	$0.00	$0.00
Exit1	Calculated	4	$1.00	$0.00	$0.00	$4.00
Entry1	Pre-Pay	4	$1.00	$0.00	$0.00	$4.00
Exit1	Standard2	1	$0.00	$0.00	$0.00	$0.00
FlashPARCS Demo1	Calculated	1	$1.00	$0.00	$0.00	$1.00
Not Paid	-	70	-	-	-	-
Payment Totals:		**113**			**$30.00**	**$59.00**

Hot Cars: 16
Average Customer Retrieval Time: 5.0 Minutes
Average Vehicle Price: $1.37

Payments

Tender Type	Vehicles	Tips	Fees	Total	Refunds
Complimentary	15	$0.00	$0.00	$0.00	No
Cash	8	$0.00	$36.00	$36.00	No
Front Desk	3	$0.00	$15.00	$15.00	No
Credit Card	17	$0.00	$8.00	$8.00	Yes
Totals:	**43**	**$0.00**	**$59.00**	**$59.00**	

Credit Card Summary

Type	Mobile Fees	Tips	Fees	Total	Refunds
AMEX	$0.00	$0.00	$0.00	$0.00	Yes
MasterCard	$0.00	$0.00	$2.00	$2.00	Yes
Visa	$0.00	$0.00	$6.00	$6.00	Yes
Totals:	**$0.00**	**$0.00**	**$8.00**	**$8.00**	

Customer Account Summary

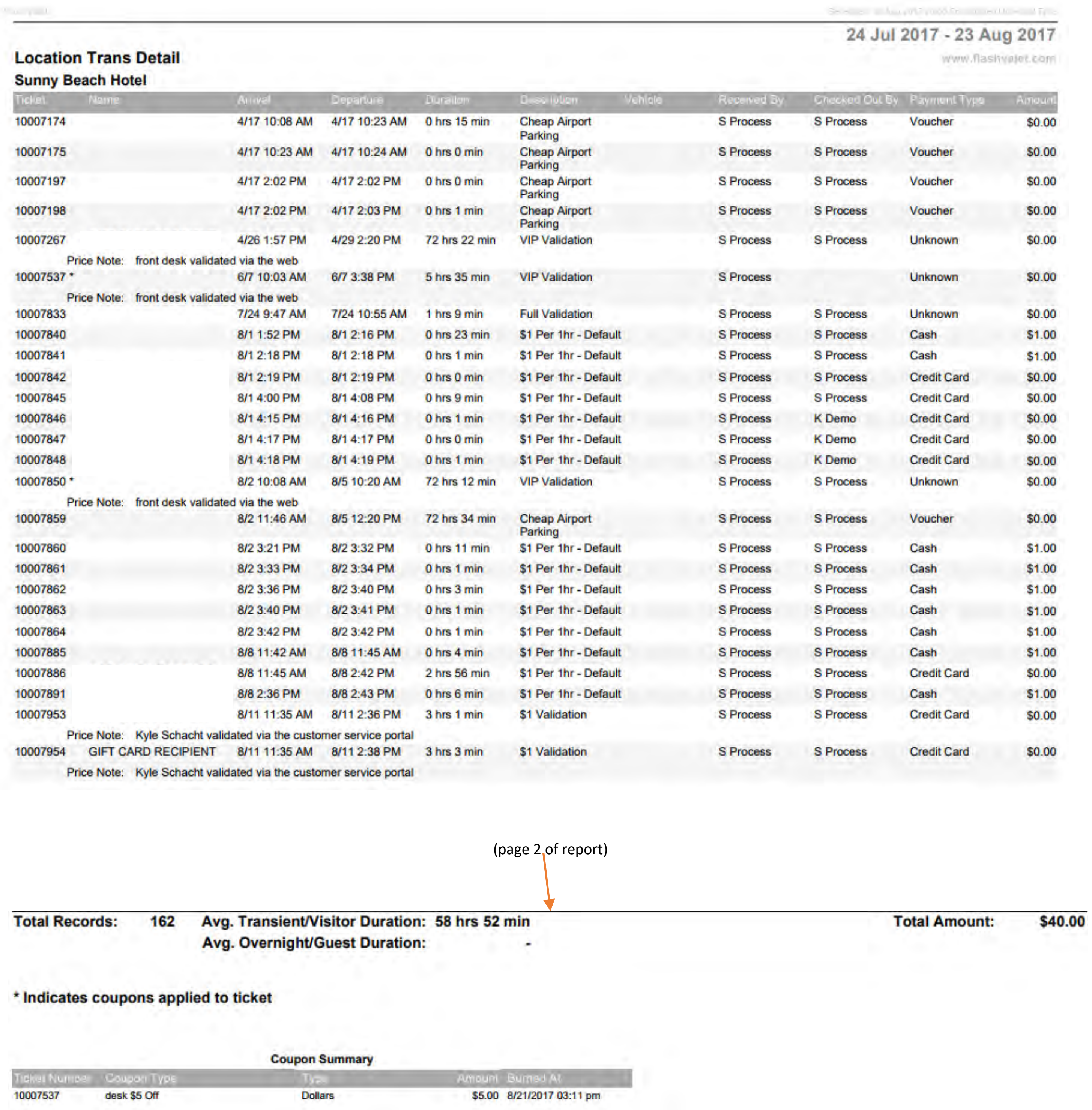
Type	Loaded	Payments	Refunds	Difference
Totals:	$0.00	$0.00	$0.00	$0.00

FlashPARCS IPI Garage
15 May 2017 - 26 May 2017
Vehicles Per Fee Summary
www.flashvalet.com

Vehicles	Fee	Total
10	$5.00	$50.00
9	$1.00	$9.00
24	$.00	$0.00
43		$59.00

Location Trans Detail

This report is ideal for viewing each transaction in detail—including ticket number, arrival, departure, duration, and payment information. At the end of the report is the total amount transacted as well as an average duration and coupon summary.



24 Jul 2017 - 23 Aug 2017
www.flashvalet.com

Location Trans Detail

Sunny Beach Hotel

Ticket	Name	Arrival	Departure	Duration	Description	Vehicle	Received By	Checked Out By	Payment Type	Amount
10007174		4/17 10:08 AM	4/17 10:23 AM	0 hrs 15 min	Cheap Airport Parking		S Process	S Process	Voucher	$0.00
10007175		4/17 10:23 AM	4/17 10:24 AM	0 hrs 0 min	Cheap Airport Parking		S Process	S Process	Voucher	$0.00
10007197		4/17 2:02 PM	4/17 2:02 PM	0 hrs 0 min	Cheap Airport Parking		S Process	S Process	Voucher	$0.00
10007198		4/17 2:02 PM	4/17 2:03 PM	0 hrs 1 min	Cheap Airport Parking		S Process	S Process	Voucher	$0.00
10007267		4/26 1:57 PM	4/29 2:20 PM	72 hrs 22 min	VIP Validation		S Process	S Process	Unknown	$0.00
Price Note:	front desk validated via the web									
10007537 *		6/7 10:03 AM	6/7 3:38 PM	5 hrs 35 min	VIP Validation		S Process		Unknown	$0.00
Price Note:	front desk validated via the web									
10007833		7/24 9:47 AM	7/24 10:55 AM	1 hrs 9 min	Full Validation		S Process	S Process	Unknown	$0.00
10007840		8/1 1:52 PM	8/1 2:16 PM	0 hrs 23 min	$1 Per 1hr - Default		S Process	S Process	Cash	$1.00
10007841		8/1 2:18 PM	8/1 2:18 PM	0 hrs 1 min	$1 Per 1hr - Default		S Process	S Process	Cash	$1.00
10007842		8/1 2:19 PM	8/1 2:19 PM	0 hrs 0 min	$1 Per 1hr - Default		S Process	S Process	Credit Card	$0.00
10007845		8/1 4:00 PM	8/1 4:08 PM	0 hrs 9 min	$1 Per 1hr - Default		S Process	S Process	Credit Card	$0.00
10007846		8/1 4:15 PM	8/1 4:16 PM	0 hrs 1 min	$1 Per 1hr - Default		S Process	K Demo	Credit Card	$0.00
10007847		8/1 4:17 PM	8/1 4:17 PM	0 hrs 0 min	$1 Per 1hr - Default		S Process	K Demo	Credit Card	$0.00
10007848		8/1 4:18 PM	8/1 4:19 PM	0 hrs 1 min	$1 Per 1hr - Default		S Process	K Demo	Credit Card	$0.00
10007850 *		8/2 10:08 AM	8/5 10:20 AM	72 hrs 12 min	VIP Validation		S Process	S Process	Unknown	$0.00
Price Note:	front desk validated via the web									
10007859		8/2 11:46 AM	8/5 12:20 PM	72 hrs 34 min	Cheap Airport Parking		S Process	S Process	Voucher	$0.00
10007860		8/2 3:21 PM	8/2 3:32 PM	0 hrs 11 min	$1 Per 1hr - Default		S Process	S Process	Cash	$1.00
10007861		8/2 3:33 PM	8/2 3:34 PM	0 hrs 1 min	$1 Per 1hr - Default		S Process	S Process	Cash	$1.00
10007862		8/2 3:36 PM	8/2 3:40 PM	0 hrs 3 min	$1 Per 1hr - Default		S Process	S Process	Cash	$1.00
10007863		8/2 3:40 PM	8/2 3:41 PM	0 hrs 1 min	$1 Per 1hr - Default		S Process	S Process	Cash	$1.00
10007864		8/2 3:42 PM	8/2 3:42 PM	0 hrs 1 min	$1 Per 1hr - Default		S Process	S Process	Cash	$1.00
10007885		8/8 11:42 AM	8/8 11:45 AM	0 hrs 4 min	$1 Per 1hr - Default		S Process	S Process	Cash	$1.00
10007886		8/8 11:45 AM	8/8 2:42 PM	2 hrs 56 min	$1 Per 1hr - Default		S Process	S Process	Credit Card	$0.00
10007891		8/8 2:36 PM	8/8 2:43 PM	0 hrs 6 min	$1 Per 1hr - Default		S Process	S Process	Cash	$1.00
10007953		8/11 11:35 AM	8/11 2:36 PM	3 hrs 1 min	$1 Validation		S Process	S Process	Credit Card	$0.00
Price Note:	Kyle Schacht validated via the customer service portal									
10007954	GIFT CARD RECIPIENT	8/11 11:35 AM	8/11 2:38 PM	3 hrs 3 min	$1 Validation		S Process	S Process	Credit Card	$0.00
Price Note:	Kyle Schacht validated via the customer service portal									

(page 2 of report)

Total Records: 162 Avg. Transient/Visitor Duration: 58 hrs 52 min
Avg. Overnight/Guest Duration: -
Total Amount: $40.00

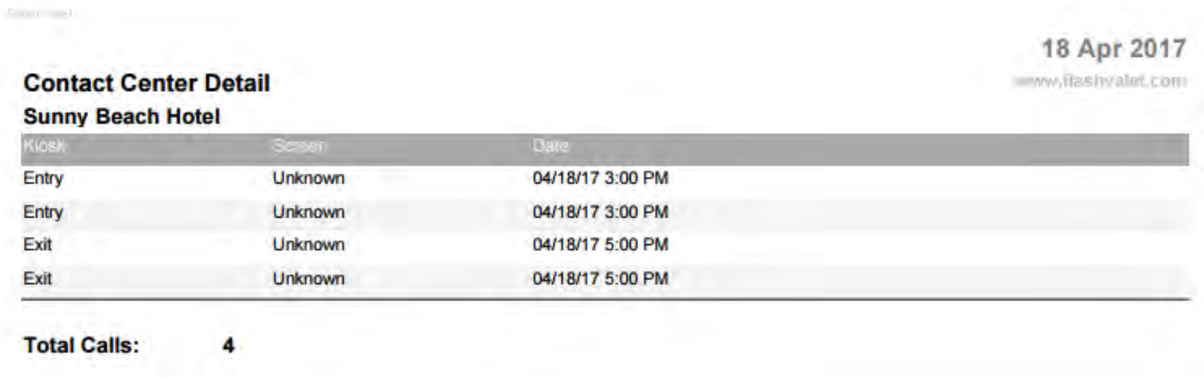
*** Indicates coupons applied to ticket**

Coupon Summary

Ticket Number	Coupon Type	Type	Amount	Burned At
10007537	desk $5 Off	Dollars	$5.00	8/21/2017 03:11 pm

Contact Center Detail

This report provides details on all support calls from any kiosk.



18 Apr 2017
www.flashvalet.com

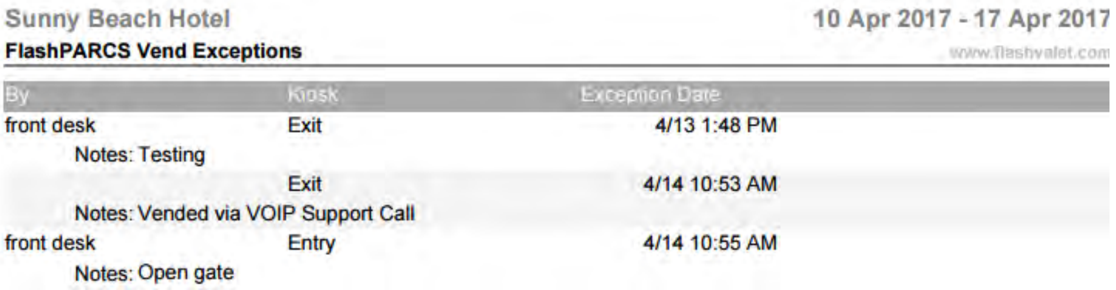
Contact Center Detail
Sunny Beach Hotel

Kiosk	Screen	Date
Entry	Unknown	04/18/17 3:00 PM
Entry	Unknown	04/18/17 3:00 PM
Exit	Unknown	04/18/17 5:00 PM
Exit	Unknown	04/18/17 5:00 PM

Total Calls: 4

FlashPARCS Vend Exceptions

This report details each time the “vend” option in the mobile app was used, as well as when the gate has been vended via a support call. Notes are required when vending through the app and will also appear on this report.

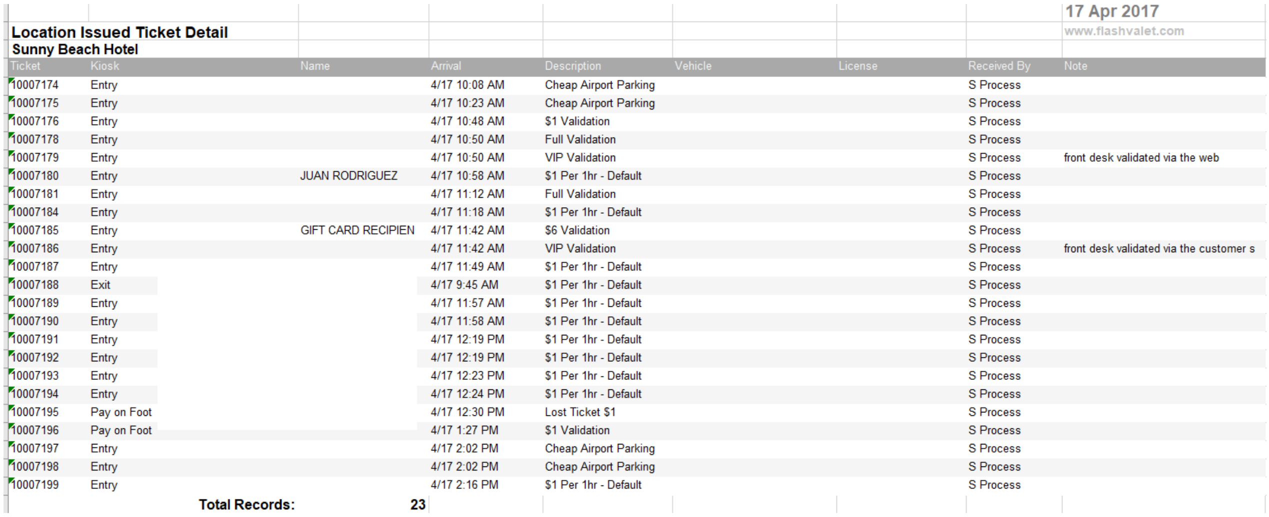


Sunny Beach Hotel
FlashPARCS Vend Exceptions
10 Apr 2017 - 17 Apr 2017
www.flashvalet.com

By	Kiosk	Exception Date
front desk	Exit	4/13 1:48 PM
Notes: Testing		
	Exit	4/14 10:53 AM
Notes: Vended via VOIP Support Call		
front desk	Entry	4/14 10:55 AM
Notes: Open gate		

Location Issued Ticket Detail (xls)

This report provides a detailed list of all transient tickets that were issued for a selected time period per kiosk.



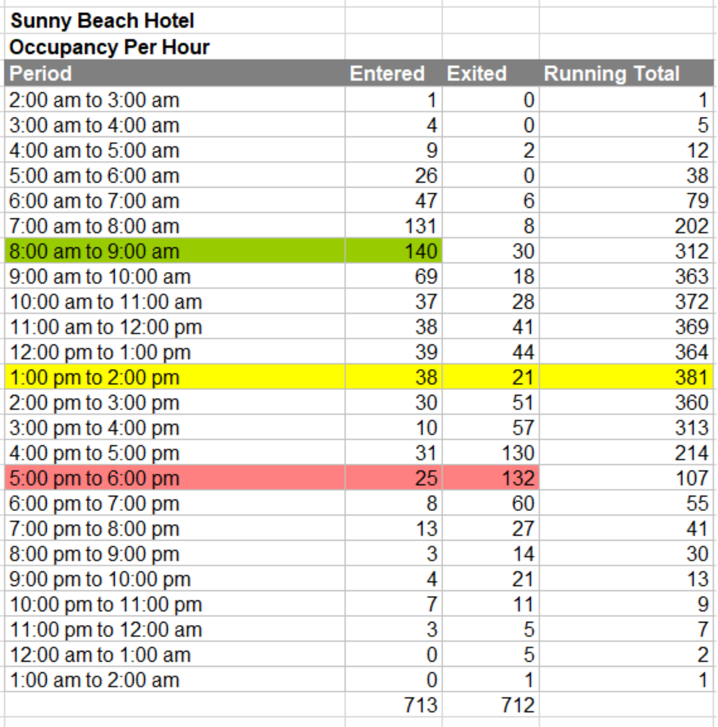
17 Apr 2017
www.flashvalet.com

Location Issued Ticket Detail
Sunny Beach Hotel

Ticket	Kiosk	Name	Arrival	Description	Vehicle	License	Received By	Note
10007174	Entry		4/17 10:08 AM	Cheap Airport Parking			S Process	
10007175	Entry		4/17 10:23 AM	Cheap Airport Parking			S Process	
10007176	Entry		4/17 10:48 AM	$1 Validation			S Process	
10007178	Entry		4/17 10:50 AM	Full Validation			S Process	
10007179	Entry		4/17 10:50 AM	VIP Validation			S Process	front desk validated via the web
10007180	Entry	JUAN RODRIGUEZ	4/17 10:58 AM	$1 Per 1hr - Default			S Process	
10007181	Entry		4/17 11:12 AM	Full Validation			S Process	
10007184	Entry		4/17 11:18 AM	$1 Per 1hr - Default			S Process	
10007185	Entry	GIFT CARD RECIPIEN	4/17 11:42 AM	$6 Validation			S Process	
10007186	Entry		4/17 11:42 AM	VIP Validation			S Process	front desk validated via the customer s
10007187	Entry		4/17 11:49 AM	$1 Per 1hr - Default			S Process	
10007188	Exit		4/17 9:45 AM	$1 Per 1hr - Default			S Process	
10007189	Entry		4/17 11:57 AM	$1 Per 1hr - Default			S Process	
10007190	Entry		4/17 11:58 AM	$1 Per 1hr - Default			S Process	
10007191	Entry		4/17 12:19 PM	$1 Per 1hr - Default			S Process	
10007192	Entry		4/17 12:19 PM	$1 Per 1hr - Default			S Process	
10007193	Entry		4/17 12:23 PM	$1 Per 1hr - Default			S Process	
10007194	Entry		4/17 12:24 PM	$1 Per 1hr - Default			S Process	
10007195	Pay on Foot		4/17 12:30 PM	Lost Ticket $1			S Process	
10007196	Pay on Foot		4/17 1:27 PM	$1 Validation			S Process	
10007197	Entry		4/17 2:02 PM	Cheap Airport Parking			S Process	
10007198	Entry		4/17 2:02 PM	Cheap Airport Parking			S Process	
10007199	Entry		4/17 2:16 PM	$1 Per 1hr - Default			S Process	
	Total Records:	**23**						

Occupancy Per Hour (PARCS)

The Occupancy Per Hour (PARCS) report details the number of vehicles that entered and exited per hour, along with a running total at each hour. This report is only available in .xls format.

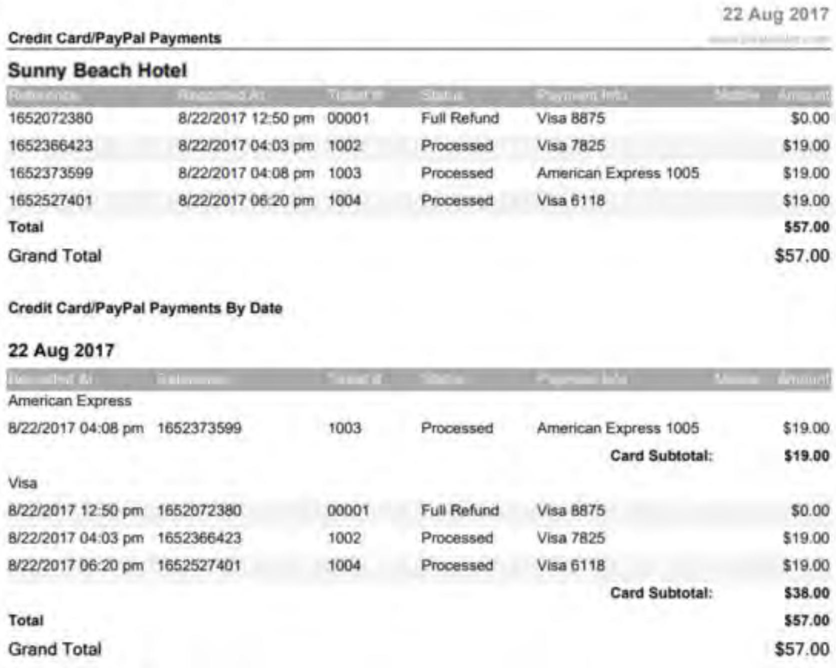


Sunny Beach Hotel
Occupancy Per Hour

Period	Entered	Exited	Running Total
2:00 am to 3:00 am	1	0	1
3:00 am to 4:00 am	4	0	5
4:00 am to 5:00 am	9	2	12
5:00 am to 6:00 am	26	0	38
6:00 am to 7:00 am	47	6	79
7:00 am to 8:00 am	131	8	202
8:00 am to 9:00 am	140	30	312
9:00 am to 10:00 am	69	18	363
10:00 am to 11:00 am	37	28	372
11:00 am to 12:00 pm	38	41	369
12:00 pm to 1:00 pm	39	44	364
1:00 pm to 2:00 pm	38	21	381
2:00 pm to 3:00 pm	30	51	360
3:00 pm to 4:00 pm	10	57	313
4:00 pm to 5:00 pm	31	130	214
5:00 pm to 6:00 pm	25	132	107
6:00 pm to 7:00 pm	8	60	55
7:00 pm to 8:00 pm	13	27	41
8:00 pm to 9:00 pm	3	14	30
9:00 pm to 10:00 pm	4	21	13
10:00 pm to 11:00 pm	7	11	9
11:00 pm to 12:00 am	3	5	7
12:00 am to 1:00 am	0	5	2
1:00 am to 2:00 am	0	1	1
	713	712	

Electronic Payments

This report provides details for each credit card transaction and breaks down subtotals per credit card type.



22 Aug 2017

Credit Card/PayPal Payments

Sunny Beach Hotel

Reference	Recorded At	Ticket #	Status	Payment Info	Mobile	Amount
1652072380	8/22/2017 12:50 pm	00001	Full Refund	Visa 8875		$0.00
1652366423	8/22/2017 04:03 pm	1002	Processed	Visa 7825		$19.00
1652373599	8/22/2017 04:08 pm	1003	Processed	American Express 1005		$19.00
1652527401	8/22/2017 06:20 pm	1004	Processed	Visa 6118		$19.00
Total						**$57.00**
Grand Total						$57.00

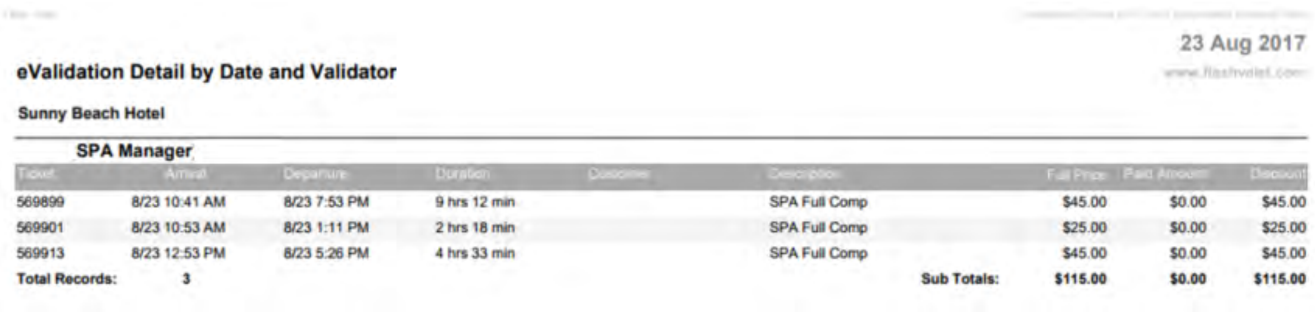
Credit Card/PayPal Payments By Date

22 Aug 2017

Recorded At	Reference	Ticket #	Status	Payment Info	Mobile	Amount
American Express						
8/22/2017 04:08 pm	1652373599	1003	Processed	American Express 1005		$19.00
					Card Subtotal:	**$19.00**
Visa						
8/22/2017 12:50 pm	1652072380	00001	Full Refund	Visa 8875		$0.00
8/22/2017 04:03 pm	1652366423	1002	Processed	Visa 7825		$19.00
8/22/2017 06:20 pm	1652527401	1004	Processed	Visa 6118		$19.00
					Card Subtotal:	**$38.00**
Total						**$57.00**
Grand Total						$57.00

eValidation by Date and Validator

This report details all electronic and printed validations that are used, including the discount amount (for billing back). This report subtotals validation usage per validator.



23 Aug 2017

eValidation Detail by Date and Validator

www.flashvalet.com

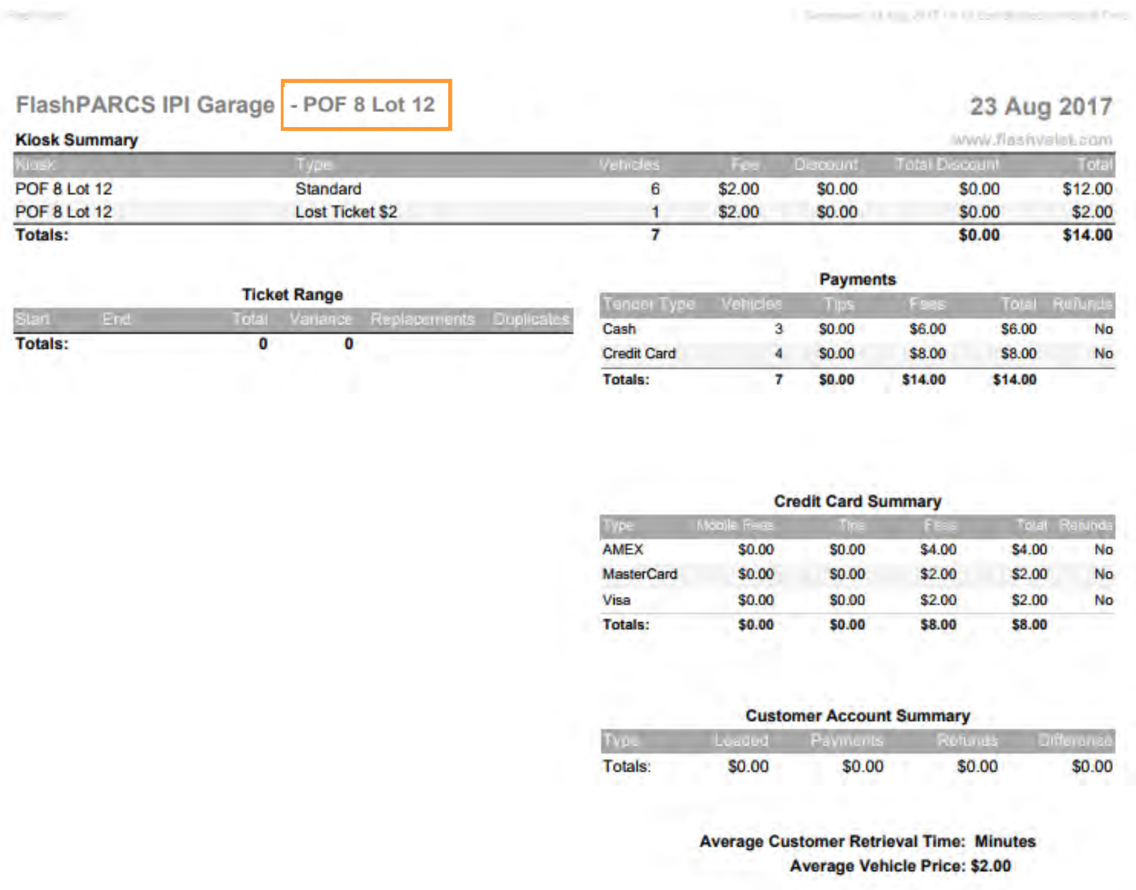
Sunny Beach Hotel

SPA Manager

Ticket	Arrival	Departure	Duration	Customer	Description	Full Price	Paid Amount	Discount
569899	8/23 10:41 AM	8/23 7:53 PM	9 hrs 12 min		SPA Full Comp	$45.00	$0.00	$45.00
569901	8/23 10:53 AM	8/23 1:11 PM	2 hrs 18 min		SPA Full Comp	$25.00	$0.00	$25.00
569913	8/23 12:53 PM	8/23 5:26 PM	4 hrs 33 min		SPA Full Comp	$45.00	$0.00	$45.00
Total Records:	**3**				**Sub Totals:**	**$115.00**	**$0.00**	**$115.00**

Kiosk Summary

This report mimics the Location Summary Hotel, but is separated out by individual kiosk.



FlashPARCS IPI Garage - POF 8 Lot 12

23 Aug 2017

Kiosk Summary

www.flashvalet.com

Kiosk	Type	Vehicles	Fee	Discount	Total Discount	Total
POF 8 Lot 12	Standard	6	$2.00	$0.00	$0.00	$12.00
POF 8 Lot 12	Lost Ticket $2	1	$2.00	$0.00	$0.00	$2.00
Totals:		**7**			**$0.00**	**$14.00**

Ticket Range

Start	End	Total	Variance	Replacements	Duplicates
Totals:		**0**	**0**		

Payments

Tender Type	Vehicles	Tips	Fees	Total	Refunds
Cash	3	$0.00	$6.00	$6.00	No
Credit Card	4	$0.00	$8.00	$8.00	No
Totals:	**7**	**$0.00**	**$14.00**	**$14.00**	

Credit Card Summary

Type	Mobile Fees	Tips	Fees	Total	Refunds
AMEX	$0.00	$0.00	$4.00	$4.00	No
MasterCard	$0.00	$0.00	$2.00	$2.00	No
Visa	$0.00	$0.00	$2.00	$2.00	No
Totals:	**$0.00**	**$0.00**	**$8.00**	**$8.00**	

Customer Account Summary

Type	Loaded	Payments	Refunds	Difference
Totals:	$0.00	$0.00	$0.00	$0.00

Average Customer Retrieval Time: Minutes
Average Vehicle Price: $2.00

FlashParking

SAMPLE PROJECT COMMUNICATION AND IMPLEMENTATION PLAN

3801 S. CAPITAL OF TEXAS HIGHWAY, SUITE 250
AUSTIN, TX 78704

PROJECT COMMUNICATION AND IMPLEMENTATION PLAN

CONTENTS

PROJECT COMMUNICATION DOCUMENTS

The following documents and schedules will be managed by the FlashParking Installation Team to safeguard effective communication. Our goal will be to maintain open communication to promote a smooth and pleasant transition for our client and their patrons.

PROJECT COMMUNICATION TABLE

Document	Recipients	Responsible Party	Update frequency
Installation status report	Client	Flash Project Team	Daily
Risk management document	Client	Flash Project Team	Daily
Issue management document	Client	Flash Project Team	Daily
Updated project schedule	Client	Flash Project Team	Weekly

TEAM STRUCTURE

The following project team has collectively managed, installed and commissioned over 10,000 installations in industries such as PARCS, Petroleum and Energy. Each bring a unique and influential perspective to establish an installation and implementation plan designed to consider every phase of the project.

TEAM INTRODUCTIONS

- ***Jim DuFon, Vice President of Strategic Projects***
  - Jim is an experienced Sales Executive in the Parking Industry. Over the past 9 years at Parkeon and then FlashParking, he has overseen the sale and installation of over 1000 kiosks in cities such as Miami, Washington D.C., Virginia Beach and Las Vegas.

- ***Wes Vinecombe, Vice President of Operations***
  - Wes has managed and supported large, complex installations and operations nationally in both the petroleum and energy industries for almost 20 years. Enterprise installations consisting of thousands of sites including: Michaels (1,100 sites), LA Fitness (500 sites), Big Lots (1,200 sites), 24 Hour Fitness (300 sites) and Tuesday Morning (500 sites) requiring the careful coordination and execution of a proven leader. Additionally, he was responsible for fulfilling over 70,000 support requests a year, creating a skilled network across the country. He has brought to FlashParking his wide-spread knowledge and experience to help create an efficient and demonstrated Installation plan. Wes will be leading the team from an Executive Level, monitoring the onsite progress and providing an open line of communication to the Executive Team.

- ***Liz Young, Director of Customer Experience***
  - Liz began her career in PARCS in 1996 and has scaled the ranks from training customers to ultimately managing over 3,000 lanes of equipment. Her extensive involvement working closely with Operators, Manufacturers, Vendors and Customers provides an exclusive insight on the installation process. Her astute understanding of how a downed facility affects the operation and experience for the end user makes her a customer proponent that will push internally to assure a successful project. Liz will work closely with both the Operational Project Team as well as the Installation Project Team. This close interaction will ensure that not only installation milestones are met but that the Customer Experience is smooth, and that the operation will continue to flow.

- ***Casey Ackman, Implementation Manager***
  - For the last 15 years Casey has honed his skills on implementing new projects. Having implemented over 8,000 sites including: Michaels (1,100 sites), LA Fitness (500 sites), Big Lots (1,200 sites), 24 Hour Fitness (300 sites) and Tuesday Morning (500 sites), Casey is able to identify risk factors before they are present to prevent disruption to the project timeline. His professionalism and approach to the implementation of a project ensures a well-developed and accurate implementation plan. He will also be present for all Project Management meetings and communication onsite.

- ***Matt Braddock, Install Manager***
  - Matt has managed and installed over 150 lanes of equipment for FlashParking, in addition to Pay on Foot Devices, LPR and AVI solutions. Matt is responsible to consult, select and manage sub-contractors across the country to meet his timelines and milestones. His attention to detail and ability to lead his

crew to successful completion provide the level of expertise and trust needed to be our man on the ground. Using his degree in Physics, Matt can find out of the box solutions for complex challenges that arise, while onsite. Matt will be on the ground day to day throughout the installation and will be the first point of contact.

- ***John Durham, Support Manager***
  - John has managed support teams of up to 30 agents and has a keen understanding for the impact of quick resolution and clear communication. With his extensive experience and support, our installation team knows that they are in good hands and will receive speedy responses to ensure a timely installation. John will participate in Project calls to safeguard the installation process and keep the Support Team in the know of every phase, to be able to assist when needed.

- ***Allison Noblitt, Training Manager***
  - Allison began with FlashParking in 2012, after having been a managing editor for a local Tech magazine. Her proficiency for attention to detail and granular understanding of how things come together made her a natural for training on the Flash systems. Since, Allison has earned the esteem of her customers who recognize the extent of her knowledge. She will be a recurring presence onsite for ongoing training. Knowing how to best utilize the system is key to success, therefore training will be emphasized and repeated as necessary for everyone's success.

TEAM ASSIGNMENTS

Client

Project Team

Team	Team goals	Team lead	Project Resource
Exec Operations Team	To oversee the project team and communicate progress internally to Flash exec team and escalate any presented risk factors for immediate attention	Wes Vinecombe	3 times a month and as needed
Implementation Team	To lead the team by monitoring and managing risk factors and expectations. Available for all PM meetings and any any on-site meetings.	Casey Ackman	3 days a week and as needed for PM Meetings
Installation Team – On-site Project Lead	Will oversee the installations crews onsite	Matt Braddock	Daily
Installation Crews	To install the equipment safely and efficiently.	4 crews of 2 or 3 members each	Daily
Customer Experience Team	To understand and consider the needs of the operations The City and its patrons throughout the installation process	Liz Young	2 times a month and as needed
Support Team	To comprehend the goals and intentions for operational use of the FlashParking system in order to properly configure and successfully test	John Durham	Phone support as needed
Training Team	To work closely with the Implementation team and the operator to create a customized training program specific to the needs of the operations	Allison Noblitt	1 week on-site, ongoing phone and email support as needed.

PROJECT STATUS

TRACKING STATUS AND COMPLETION

A daily update will be provided by the Project Team to maintain an open communicaon a nd track expectaons.

Date	Were milestones met?	Were any risks idenfied?	Were any changes requested?	Daily summary of Installaon

RISK AND ISSUE MANAGEMENT

TRACKING RISKS AND ISSUES

The following risks will be identified and communicated as early as possible to mitigate the impact on timeline and overall project success. These risk factors will be updated daily until resolved.

Date recorded	Risk description	Impact	Mitigation plan

TESTING PLAN

The FlashParking goal is to get your facility up and running as quickly, but as efficiently as possible. To accomplish this, we have structured different levels of testing and counter checks. This thorough and vigorous setup ensures that when your equipment is installed and turned on you are ready to start collecting revenue. These checklists and guides below will assist us in creating an easy installation and turn key operation.

Acceptance Testing Configuration Guide

Project Name:

Facility Name:

Functional Test (annotate measurements, date/time where needed, check all others)

Today's date (for each device					
Record device name (i.e. location/lane/type)					
Record MAC address of each device					
Record ip Address of each device					
Gate Mfr					
Gate Model					
Gate Arm Type					
Gate Arm Length					
Gate Arm Clearance (if Articulating)					
Entry/Exit Kiosk					
Test Arming loop with Mega-ohm meter, record					
Test Safety loop with Mega-ohm meter, record					
New or Existing Arming Loop					
New or Existing Safety Loop					
Confirm Arming loop is directly in front of the kiosk					
Measure distance between arming and closing (safety) loop, record					
Measure distance between kiosk and gate boom, record					
Arm the arming loop to activate the entry/exit screen					
Enter by pulling a ticket/exit with ticket					
Enter/exit with credit card number					

Enter/exit with phone number					
Enter/exit with prox card					
Enter/exit with AVI (if applicable)					
Enter/exit with cash (if applicable)					
Cross/test entry safety loop to activate ticket					
Test help button					
Make sure they can remotely vend the gate					
Confirm the FlashPARCs application is running in SecureLockdown					
Transaction test performed at each Exit and POF kiosk					
Confirm grace period					
Confirm rates					
Pay with credit card and print receipt					
Pay with cash if applicable and print receipt					
Cross/test safety loop to close out ticket					
Refund credit card transactions through app					
Acumera					
Disconnect primary internet, confirm cell modem connect					
Record Cell Modem ip address					
Record cell modem imei number					
Record cell modem signal strength (how many bars)					
Magnetic gate programming					
Function> program mode> automatic mode 5					
setup> delays> Hold Open 10 secs					
setup>vend count> reset behavior> TO/reset on close					
Inputs/Outputs> #3 (typical)> open low priority					
loop detector 1a-b>					
mode a> Safety					
mode b> Presence OEM					

Frequency Settings> Freq. Shift>					
Loop A High					
Loop B High					
Set frequencies for adjacent lane(s) to Loop A Low + Loop B Low					
Factory Settings>1754>User settings as factory settings					
NO5- Presence loop feedback					
NO4- Safety loop feedback					
C4-6 terminate both commons from A/D inputs on relay board					
IN3 Vend gate input from NO1 on relay board					
24V- from common on relay board					
Cleanup					
Police each work area	✓				
All Kiosks have paper installed	✓				
Lock Gates and Kiosks	✓				
Digital picture of device - identify device by name in pic	✓				
Tour Site with Customer	✓				
Demonstrate each device for customer	✓				
Have customer pull a ticket and "enter"	✓				
Have the customer "exit"	✓				
Have the customer log a help call	✓				
Annotate any recommendations on customer sign off form					
Customer signs sign off form					

Pre-Shipment Configuration	QA Release?	Y/N
Project Name:	Release Date:	
Facility Name:	QA Agent:	

Kiosk pre-config setup steps	ENTRY1	ENTRY2	EXIT1	EXIT2
Name and label kiosk with location and lane description				
Plug in kiosk to power source. Turn on power strip				
Check all USB connections and power fully pushed in.				
Turn on amplifier. Turn volume almost all the way up. Back it off a ¼ turn. Turn bass all the way down. Turn treble all the way up.				
Once tablet boots up:				
Plug in CAT5				
Set correct time zone				
Accept the legal stuff				
Skip the Wi-Fi step				
Select Customize Settings				
Turn all features off. Note, there are 3 pages of features. First page has 5 to turn off so you'll have to scroll down.				
Personalize your PC- select "skip this step"				
Create an account for this PC. Name it "KTest" or anything you want. This account will get deleted. Leave everything else blank.				
Tablet will now start loading Windows. Takes a couple of minutes.				
You should now have a desktop.				
Push and hold Windows symbol in bottom right corner. Select "Shut down or sign out"				
Sign in as kleverlogic				
Go to Control Panel-> User Accounts-> Manage another account-> "Ktest"-> Delete the account-> Delete files-> Delete Account				
Go to Control Panel-> Sound-> Recording (tap mic to test response"-> Sounds-> select Asterisk-> Test-> you should hear loud noise through speaker. If not, troubleshoot audio hardware.				
Push and hold Windows symbol in bottom right corner.				
Log Me In: Select Settings-> System-> About-> Rename PC-> Type in kiosk name. Should be location and lane description (15 character maximum limit)-> Select restart				

Double tap Log Me In browser shortcut on desktop				
Type in kiosk name. Should be location and lane description				
Select Download option. Takes a while depending on internet connection				
Select Run				
Select Finish				
Select “next” through all options				
Enter Log Me In password.				
Display Configuration				
Close out of all Log Me In screens				
You’ll get a couple of pop-ups. One of them will ask if you want Log Me In to run in the background, select yes.				
Press and hold on the operating system background for 3 seconds, and then release to display the pop-up or context menu for the desktop.				
Select the option for “Display Settings”				
Select the option for “Advanced Display Settings”				
Select a resolution of “1024 x 768”				
Click “Apply” or close the window if the resolution setting is already correct.				
Press and hold on the background again to display the context menu.				
Select “Graphic Options”, then “Panel Fit”, then “Scale Full Screen”.				

Kiosk pre-config setup steps

Date and Time:				
Task Scheduler > Task Scheduler Library > Delete OneDrive Standalone Update Task				
Device Manager:				
Verify Date, Time, and Timezone are correct.				
Devices and Printers:USB Controllers > Right-click > Properties > Power Management settings for all USB Hub devices and uncheck settings to allow to suspend.				
Network Devices > Wireless Adapter > Right-click > Disable				
Set Hengstler printer to Default.				
Display				

Right-click > Printer Properties > Print Quality > Dark, High				
Print Test Page				
System				
Change Display Settings > Advanced Display Settings > Verify Resolution is 1024 x 768				
User Accounts				
Right click Desktop background > Graphic Options > Panel Fit > Scale to Fit				
Group Policy Editor				
Verify Computer Name is 15 or less characters. To change the name, click here.				
Go to Administrative Templates > Windows Components > Windows Defender				
Manage Other Accounts > Delete all users except Kleverlogic				
MOIR Demo				
Double-click Turn off Windows Defender, set to Enabled.				
MOIR Config Utility				
General Setting				
General Settings > HID Mode				
General Settings > Read on Withdraw				
Enter manual command				
Select Send to Reader.				
Change Advanced Settings				
Security				
Verify Read On Withdrawal Only and ID TECH USB HID are selected.				
Select Send to Reader.				
Verify Preamble says "Card Seated"				
See Cash Acceptance for installation instructions for each type of cash machine.				
Uncheck Card Seated On, Check Media Detected On, Check NGA Protocol for encrypt output, Check No Data On				
Copy latest / required FlashPARCS software suite.				
Delete sqlite file if exists				
Launch FlashPARCS software, login, and assign to appopriate kiosk.				
Set Encrypt Struct to Original, Check Display Exp Date				
Shut Down Kiosk (Commmand line: shutdown -s)				
Deactivate Monitoring - Portal > Location > FlashPARCs > Select Kiosk > Deactivate				

License key - 749c781b-6acf-4775-b2d0-3cf4464b9061				
Set password				
Verify settings				
Enable				
Verify it works.				
Disable				

Pre-Shipment Configuration	Facility Passed?
Project Name:	Test Date:
Facility Name:	Install Manager:

Test Description	ENTRY1	ENTRY2
Audio Tests		
Press and hold on the Start button for 3 seconds, and then release to display a context menu.		
Select “Control Panel”.		
Select “Hardware and Sound” or “Sound” icon, depending on the available view.		
Select the displayed speaker device, and click “Properties”.		
Select the “Advanced”, then “Test”.		
Adjust the amplifier volume to ensure the playback sound is loud enough to account for motor noise and other environmental noise.		
Select “OK” or “Cancel” to return to the sound menu.		
Select “Recording”		
Tap the top of the microphone to ensure is it registering sound.		
move to roughly 2 feet away from the SmartStation and begin speaking (i.e. test 1, 2), ensuring that the volume level reaches at least half way up the audio indicator If volume levels are not high enough, select “Properties” then “Levels” and adjust the “Microphone Boost” slider until the volume levels are acceptable.		
Printer Test		
Have commissioner verify that paper is loaded correctly in printer.		
Navigate to “Control Panel”, then “Devices and Printers”.		

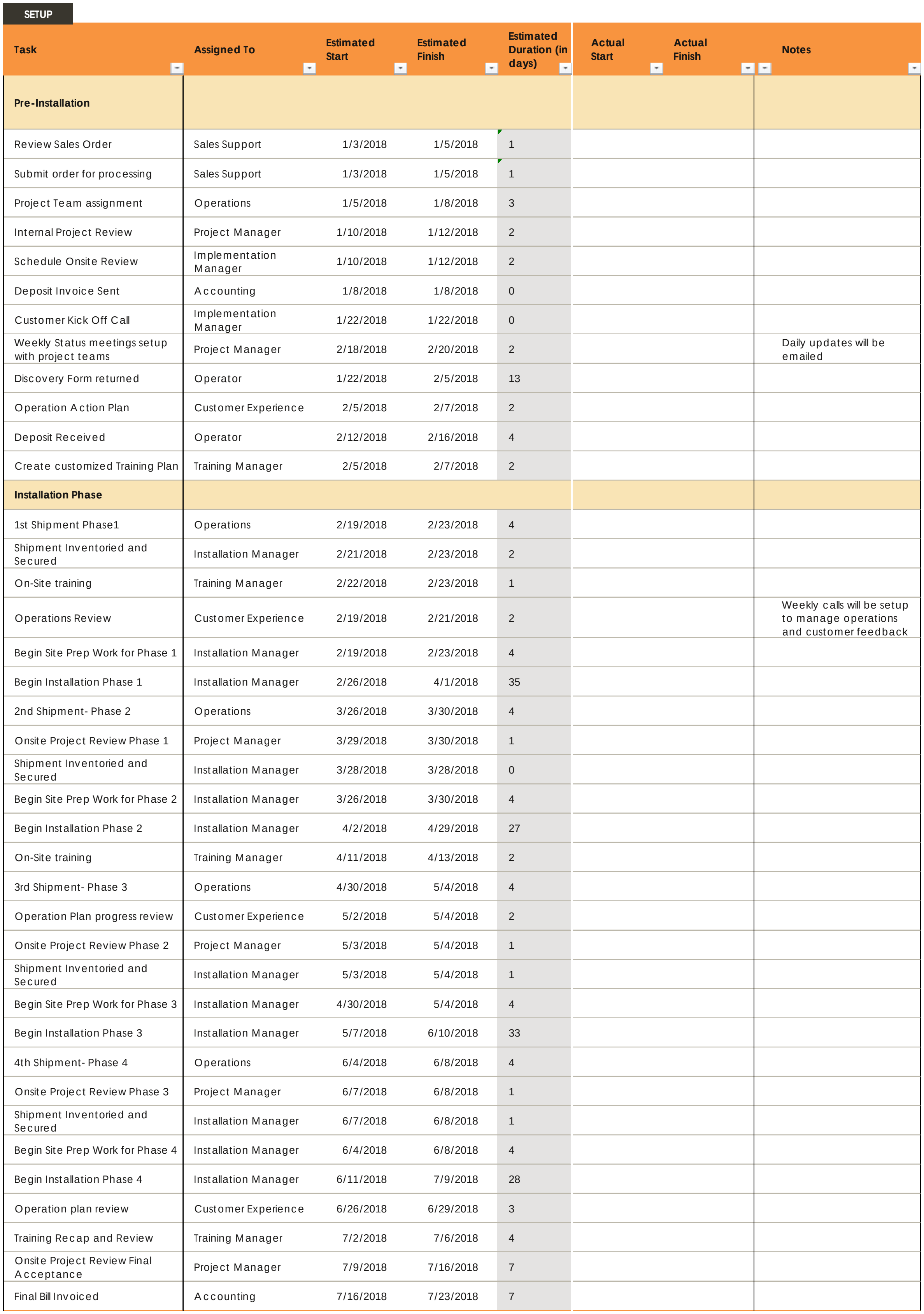
Right-click on the Hengstler C-56 printer and select “Set As Default Printer”		
Right-click again on the printer and select “Printer Properties”		
Select the “Printer Settings” tab.		
Set “Impression Quality” to “Dark”, and Print Quality to “High”.		
Select the “General” tab.		
Click “Print Test Page”		
Have commissioner verify that test page is printed.		
Secure Lockdown		
Launch Secure Lockdown		
Copy Product Key from Dropbox/KL IT/FlashPARCS/Secure Lockdown/Activation Key		
Paste into required form.		
Set FlashPARCS application to run in Secure Lockdown		
Launch Secure Lockdown again.		
Use Keyboard Shortcut Alt+Shift+S		
Set Password to		
Enabled Secure Lockdown and reboot		
Support Calls		
Enter valid test number (i.e. Commissioner’s Cell Number, or Support Agent’s direct dial phone number) into portal. – I suspect this should always go to a support agent as any background noise issue will also be a problem for anyone on site trying to hear, possibly resulting in the microphone being set too high.		

Onsite Commissioner should select the Call Support button, and verify it dials to 2nd onsite person or Support Agent, and both microphone and speaker volume are acceptable for site's environmental noise. – see note in number 1 above		
Transaction Processing		
Test ticket process by shorting entry and exit loops.		
Test Credit Card process by shorting entry and exit loops (ensure backend merchant functionality by allowing grace period to expire and CC to be charged).		
LogMeIn		
Registration and Groups		
Create Site Specific Group in LogMeIn		
Name = State-Site Description (i.e. TX-Office Machines)		
Click "Save"		
Navigate to "Configuration" then "Host Preferences"		
Click "Edit" on the line for "Disabled_Printing_Packages"		
Click "Save"		
Navigate to "Alerts" then "Manage Alert Packages"		
Click "Edit" on the line for "Default Alert Packages"		
Select the appropriate Group / Computers from the list by checking the boxes.		
Click "Save and Close"		
Verify Date / Time Settings		
This must be performed for each SmartStation.		
Connect to the SmartStation through LogMeIn		
Navigate to "Control Panel" then "Date and Time".		
Verify that Date, Time, and Timezone are correct.		
Updating FlashPARCS Software		
Navigate to "Computers" then click "File Manager" for the appropriate SmartStation.		
Navigate to Drop Box files for newest FlashPARCS software		
If you do not have a Drop Box drive listed - DO WHAT		
Copy all files from Drop Box to C:\Program Files\FlashPARCS		

In C:\Program Files\FlashPARCS, delete the file named “FlashParcs.sqlite”		
Kiosk (entry & exit) relay board terminations		
A/D 1- Presence loop feedback		
A/D2- Safety loop feedback		
NO1- Vend gate 24v		
Comm- Vend gate common		

PROJECT CHECKLIST

Sample Project Tracker



Task	Assigned To	Estimated Start	Estimated Finish	Estimated Duration (in days)	Actual Start	Actual Finish	Notes
Pre-Installation							
Review Sales Order	Sales Support	1/3/2018	1/5/2018	1			
Submit order for processing	Sales Support	1/3/2018	1/5/2018	1			
Project Team assignment	Operations	1/5/2018	1/8/2018	3			
Internal Project Review	Project Manager	1/10/2018	1/12/2018	2			
Schedule Onsite Review	Implementation Manager	1/10/2018	1/12/2018	2			
Deposit Invoice Sent	Accounting	1/8/2018	1/8/2018	0			
Customer Kick Off Call	Implementation Manager	1/22/2018	1/22/2018	0			
Weekly Status meetings setup with project teams	Project Manager	2/18/2018	2/20/2018	2			Daily updates will be emailed
Discovery Form returned	Operator	1/22/2018	2/5/2018	13			
Operation Action Plan	Customer Experience	2/5/2018	2/7/2018	2			
Deposit Received	Operator	2/12/2018	2/16/2018	4			
Create customized Training Plan	Training Manager	2/5/2018	2/7/2018	2			
Installation Phase							
1st Shipment Phase1	Operations	2/19/2018	2/23/2018	4			
Shipment Inventoried and Secured	Installation Manager	2/21/2018	2/23/2018	2			
On-Site training	Training Manager	2/22/2018	2/23/2018	1			
Operations Review	Customer Experience	2/19/2018	2/21/2018	2			Weekly calls will be setup to manage operations and customer feedback
Begin Site Prep Work for Phase 1	Installation Manager	2/19/2018	2/23/2018	4			
Begin Installation Phase 1	Installation Manager	2/26/2018	4/1/2018	35			
2nd Shipment- Phase 2	Operations	3/26/2018	3/30/2018	4			
Onsite Project Review Phase 1	Project Manager	3/29/2018	3/30/2018	1			
Shipment Inventoried and Secured	Installation Manager	3/28/2018	3/28/2018	0			
Begin Site Prep Work for Phase 2	Installation Manager	3/26/2018	3/30/2018	4			
Begin Installation Phase 2	Installation Manager	4/2/2018	4/29/2018	27			
On-Site training	Training Manager	4/11/2018	4/13/2018	2			
3rd Shipment- Phase 3	Operations	4/30/2018	5/4/2018	4			
Operation Plan progress review	Customer Experience	5/2/2018	5/4/2018	2			
Onsite Project Review Phase 2	Project Manager	5/3/2018	5/4/2018	1			
Shipment Inventoried and Secured	Installation Manager	5/3/2018	5/4/2018	1			
Begin Site Prep Work for Phase 3	Installation Manager	4/30/2018	5/4/2018	4			
Begin Installation Phase 3	Installation Manager	5/7/2018	6/10/2018	33			
4th Shipment- Phase 4	Operations	6/4/2018	6/8/2018	4			
Onsite Project Review Phase 3	Project Manager	6/7/2018	6/8/2018	1			
Shipment Inventoried and Secured	Installation Manager	6/7/2018	6/8/2018	1			
Begin Site Prep Work for Phase 4	Installation Manager	6/4/2018	6/8/2018	4			
Begin Installation Phase 4	Installation Manager	6/11/2018	7/9/2018	28			
Operation plan review	Customer Experience	6/26/2018	6/29/2018	3			
Training Recap and Review	Training Manager	7/2/2018	7/6/2018	4			
Onsite Project Review Final Acceptance	Project Manager	7/9/2018	7/16/2018	7			
Final Bill Invoiced	Accounting	7/16/2018	7/23/2018	7			

PROJECT SCHEDULE

Client	Sample			**Project**	Sample
Contact	**Fax**			**Date**	
Address		_		**Start**	1/15/2018
City, St. Zip		_		**Completion**	7/9/2018
ID	**Task**	**Duration**	**Start Date**	**Finish Date**	**Notes**
	Pre-Installation				
1	Review Sales Items	2	1/15/2018	1/17/2018	
2	Submit order for processing	3	1/17/2018	1/20/2018	
3	Project Team assignment	2	1/22/2018	1/24/2018	
4	Internal Project Review	2	1/22/2018	1/24/2018	
5	Schedule Onsite Review	5	1/22/2018	1/27/2018	
6	Identify Staging Warehouse	2	1/22/2018	1/24/2018	
7	Deposit Invoice Sent	1	1/29/2018	1/30/2018	
8	Customer Kickoff Call	1	2/5/2018	2/6/2018	
9	Weekly status meetings setup w/ project teams	5	2/12/2018	2/17/2018	
10	Operation Action Plan	1	2/12/2018	2/13/2018	
11	Deposit Received	5	2/12/2018	2/17/2018	
12	Create Customized Training Plan	5	2/14/2018	2/19/2018	
	PHASE 1				
13	System Configuration and Testing (see Test Plan)	2	2/20/2018	2/22/2018	
14	QA Approves shipping	4	2/23/2018	2/27/2018	
15	1st Shipment	1	2/27/2018	2/28/2018	
16	Shipment Inventoried and Secured	1	2/26/2018	2/27/2018	
17	OnSite Training	1	2/26/2018	2/27/2018	
18	Operations Review	1	2/27/2018	2/28/2018	
	Installation Prep Work				
19	Unbox and inspect all equipment in staging area	3	2/27/2018	3/2/2018	
20	Power on and establish connectivity in staging area	2	2/28/2018	3/2/2018	
21	Establish shipping schedule for equipment to sites	28	2/28/2018	3/28/2018	
	Onsite Installation				
22	*Facility- To be Determined by Project Team*	28	2/28/2018	3/28/2018	
A	Run ethernet CAT6 cable from the network demarcation point to the FlashPARCS SmartStation Kiosk				
B	Mounting FlashPARCS network kit with back-up LTE in each lot or garage (will be pre-configured				

	prior to shipping) - incl failover testing				
C	Remove existing equipment				
D	Cut new loops				
E	Install new loop				
F	Seal new loops				
G	Calibrate and connect loops to the gate				
H	Electrical runs to equipment				
I	Bolt down SmartStation kiosk				
J	Bolt down gate				
K	Run cable between kiosk and gate				
L	Re-placing or installing new bollards				
M	Clean-up - removal of removed equipment				
N	Painting island and or bollards				
O	Site Acceptance Testing (See Test Plan Document)				
P	Finalized Documentation for facility completion				
23	*Facility- To be Determined by Project Team*	28	2/28/2018	3/28/2018	
A	Run ethernet CAT6 cable from the network demarcation point to the FlashPARCS SmartStation Kiosk				
B	Mounting FlashPARCS network kit with back-up LTE in each lot or garage (will be pre-configured prior to shipping) - incl failover testing				
C	Remove existing equipment				
D	Cut new loops				
E	Install new loop				
F	Seal new loops				
G	Calibrate and connect loops to the gate				
H	Electrical runs to equipment				
I	Bolt down SmartStation kiosk				
J	Bolt down gate				
K	Run cable between kiosk and gate				
L	Re-placing or installing new bollards				

SUMMARY OF WHAT TO EXPECT DURING AN INSTALLATION

The FlashParking team has spent endless cycles on simplifying and optimizing the installation process. Considering downtime, flow and customer experience, the Flash team will have you back up and collecting revenue faster than anyone else. All software configuration will be done well in advance by the onboarding team. The project team will work closely with the operations team to carefully understand the complexity of the operation. When the installation team arrives on the ground it will be ready to proceed. The FlashPARCS system is 100% cloud based, therefore there is no need to install servers on racks or to install and configure software. From a communication standpoint, we do not use RS485 or an equivalent, instead we utilize traditional ethernet CAT6 cables, which makes the installation much easier. Below we describe the installation process, so you know what to expect.

In 6 to 8 hours, the following work is done to complete a lane install:

- ✓ Running one ethernet CAT6 cable from the network demarcation point to the FlashPARCS SmartStation Kiosk
- ✓ Mounting FlashPARCS network kit with back-up LTE in each lot or garage (will be pre-configured prior to shipping)
- ✓ Removing old entry (ticket/chip spitter) or exit (exit verifier) machine
- ✓ Removing old gate
- ✓ Cutting, installing & calibrating new arming loop (loops to be installed are preformed DB loops; highest performance in the market, they also typically save 30 minutes during install)
- ✓ Cutting, installing & calibrating new safety loop (loops to be installed are preformed DB loops; highest performance in the market, they also typically save 30 minutes during install)
- ✓ Connecting both loops to the gate
- ✓ Extending or re-routing existing electrical power lines to new SmartStation Kiosk and gate
- ✓ Bolting down SmartStation kiosk (they immediately get their configuration from the cloud infrastructure upon powering-up)
- ✓ Bolting down gate
- ✓ Running 3 pairs of cables from SmartStation Kiosk to gate for (a) gate vend, (b) arming loop detection, and (c) closing loop detection
- ✓ Replacing or installing new ballers
- ✓ Clean up: placing old machine and gate in a designated area or disposing of them
- ✓ Painting island and/ or ballers
- ✓ Testing all components: getting a ticket, and every entry or exit method including real credit card payment transaction, microphone & speakers (placing a support call), barcode scanner, prox card reader, Bluetooth access, vending gate and loop detection
- ✓ Complete documentation

SURVISION

LICENSE PLATE RECOGNITION

SURVISION
LICENSE PLATE RECOGNITION

LPR Experts

Cutting edge video solutions for vehicle detection and identification.

We develop, manufacture and sell the best all-integrated real-time License Plate Recognition (LPR) Technology.

Our focus is on creating intelligent, reliable and seamless devices that will help you take vehicle management to the future, today.

Datasheets, Case Studies and much more at our website **www.survisiongroup.com**

Compact

High accuracy

Free-flow or triggered

Flexible installation

Shared SDK

All license plates

	NANOPAK	MICROPAK
	Ground or in-barrier installation for parking and access control	*Pole, wall or ceiling installation for Tolling and parking*
Recognition Engine	Embedded	Embedded
Recognition Distance	From 2 to 8 m / 6 to 26 ft	From 2,5 to 15 m / 8 to 50 ft
Coverage Width	Up to 4 m / 13 ft	Up to 4 m / 13 ft
Image Analysis	60 fps	60 fps
Material	Aluminium	Aluminium - IP67
Instant Speed		√
Dangerous Goods plates		√

VISIPAK

Pole or gantry installation for ITS and Tolling

PICOPAK

Mobile mounting for Security and on-street parking

VISIPAK	PICOPAK	
Embedded	Embedded	Recognition Engine
From 3 to 30 m / 98 ft	From 2 to 10 m / 32.8 ft	Recognition Distance
Up to 7 m / 23 ft	Up to 4 m / 13 ft	Coverage Width
60 fps	60 fps	Image Analysis
Aluminium - IP67	Aluminium - IP67	Material
√		Instant Speed
		Dangerous Goods plates

APPLICATIONS

PARKING

Revenue control and customer satisfaction

- Automatic access for monthly subscribers
- Fast Exit
- Fraud control
- Lost Tickets management
- On-street parking mobile enforcement

ACCESS CONTROL

Security and comfort for parking

- Quick VIP Access for authorized users
- Elimination of unwanted vehicles
- Easy access management for visitors
- Vehicle counting

SECURITY

Efficiency in combating crime and securing roads

- Fixed or Mobile enforcement
- Detection of stolen vehicles
- Judicial inquiries
- Roadside enforcement
- Border and customs control

ITS & TOLLING

Road revenue and traffic control

- Free-Flow tolling
- Stop&Go tolling
- Weight in Motion
- Pollution and traffic control
- Tunnel and bridge safety

SURVISION EUROPE

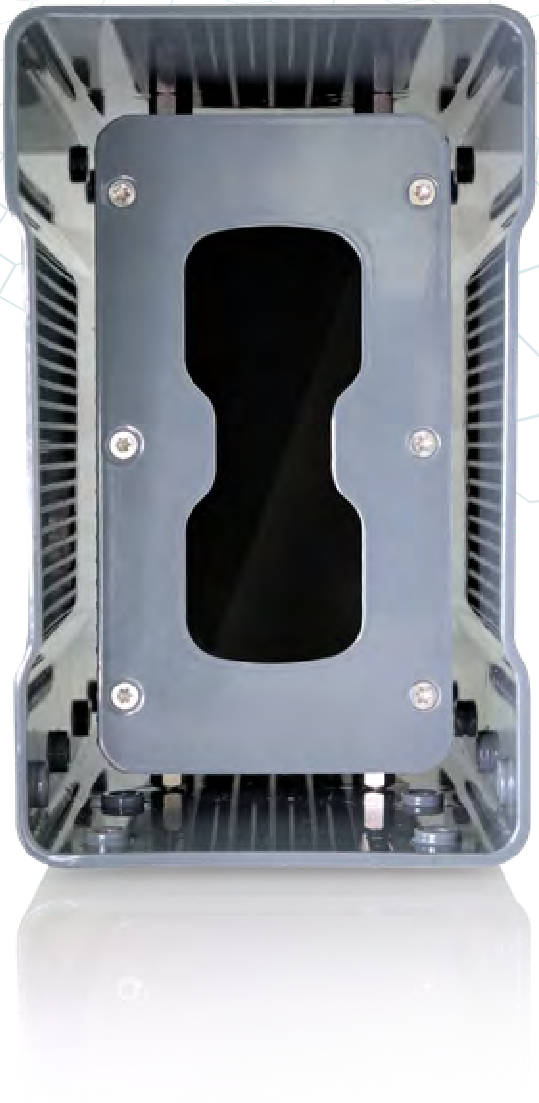
22 rue d'Arras,
92000, Nanterre (París) France
+33 (0)1 47 51 04 80
contact@survision.eu

SURVISION AMERICAS

11251 Nw 20th Street.#116,
Miami, Fl. 33172
+1 (786) 362.5471
contact@survisiongroup.com

WWW.SURVISIONGROUP.COM

SURVISION
LICENSE PLATE RECOGNITION



MICROPAK

- **ALL-INTEGRATED:** The Licence Plate Recognition or the Dangerous Goods plate recognition is carried out entirely in the camera.

- **EASY TO INSTALL:** The camera automatically adjusts its filming and lighting parameters in order to be able to provide an optimal performance regardless of the conditions. The camera settings (compression, frequency,...) can be carried out remotely.

- **HIGH SPEED:** Supports vehicle speeds up to 250 km/h (155 miles/ hour)

- **IP67 CASING** For Indoor and Outdoor installations

- **VIDEO STREAM** provided in real time (Standard RTSP streaming)

- **DRY CONTACT** to directly control a barrier

- **FAST:** 60 frames per second

APPLICATIONS

ACCESS CONTROL

PARKING

TOLLING

SECURITY

MICROPAK
TECHNICAL SPECIFICATIONS

LICENSE PLATE RECOGNITION

	European plates (long)	Americas Plates (short)
Recognition distance (see part number for more details)	From 4 to 15.5m - From 13 to 51ft	From 3 to 10 meters - From 10 to 33ft
Coverage width	Up to 4m - Up to 13ft	Up to 3m - Up to 10ft
Recognition Engine	SURVISION REALTIME EMDEDDED IA ENGINE (SREIE)	
Recognition framerate	60fps	
Recognition direction	Both (Rear and Front)	
Max vehicle speed	Up to 250km/h - 155mp/h	
Triggering	Free Running (no trigger) - Software Trigger - Hardware Trigger	
Confidence Ratio	Yes	
Recognition JPEG	Yes (4 different formats), setable quality	
Square plate formats supported	Yes	
Countries supported	All countries supported supplied at once (ask SURVISION for up-to-date list) Confidence Ratio	
Other data supplied	Coordinates of the plate, Direction, Country, Juridication, Type	

VIDEO AND ILLUMINATION FEATURES

Lightning	4 strong power pulsed IR (850nm) or White Light LEDs
CMOS	HD 1.3MPixels Black&White
Compression	H264
Transport Protocole	RTSP
Available settings	Display framerate (up to 30fps), Bitrate

ELECTRIC CHARACTERISTICS

Power supply	24V +/- 3V
Power Consumption	Average 10W, max 15W

MECHANICAL CHARACTERISTICS

Weight (without sunshield)	1050Gr - 2.3lbs
Dimension (LxWxH)	130x115x70 mm - 5.12x4.53x2.76 inches
Material	Aluminium
Coating	Epoxy painting RAL 7031
Water&Dust protection	IP67
Connectors	Amphenol RJ45 + Amphenol DB10 LTW
Operating and storage temperature	From -40°C to +55°C - From -40°F to +131°F

SECURITY, ENVIRONMENTAL AND TECHNICAL CERTIFICATIONS

Security	SSL, 802.1x, 802.1q
Photobiological Safety	IEC62471
Homologation	EMC EN 55032, CE Marking, FCC Part 15, CB Scheme, CEI 61000-4
MTBF	70.000 hours minimum
Time Snchronisation	NTP Protocol

DATA OUTPUT AND INPUT

TCP/IP	SURVISION Open Camera Development Kit (CDK), available for free
FTP	Embedded FTP Client
Ethernet	Gigabit Ethernet 10/100/1000
Serial	Insulated RS485
WIEGAND	Through external board connected to the RS485
IO/IN	Optocoupler. Tension min 15V max 30V
IO/OUT	Relay 220 VDC 2A
Other protocols	OSDP, NEDAP

ACCESSORIES AND OPTIONS

Power cable	3, 10, 30m - 10, 33, 98ft
Full signal cable (Power, RS485, IO)	10m - 33ft
Wiegand	External board on RS485 serial connection
Fixation parts	Pole Mounting Kit and 3D adjusting Bracket

PART NUMBERS

	MICROPAK - 12mm	**MICROPAK - 16mm**	**MICROPAK - 25mm**
Recognition distance European plates (long)	From 4 to 8m - From 13 to 26ft	From 6 to 10m - From 20 to 33ft	From 9 to 15.5m - From 29 to 51ft
Recognition distance American plates (short)	From 3 to 5.5m - From 10 to 18ft	From 4 to 7.5m - From 13 to 25ft	From 7 to 10m - From 22 to 33ft
Essential (single country or state) IR (Black characters)	MPK3IRAMCV12	MPK3IRAMCV16	MPK3IRAMCV25
Essential (single country or state) White Light (colored characters)	MPK3LBAMC12	MPK3LBAMC16	MPK3LBAMC25
Plus (all countries) IR (Black characters)	MPK3IRAMPV12	MPK3IRAMPV16	MPK3IRAMPV25
Plus (all countries) White Light (Colored characters)	MPK3LBAMP12	MPK3LBAMP16	MPK3LBAMP25
Dangerous Goods (ADR plates) IR	MPK3IRFBAMP12	MPK3IRFBAMP16	MPK3IRFBAMP25

Supplier: **FlashParking**

Standard Instructions to Vendors
Request for Proposals, Request for Qualifications, or Request for Letters of Interest

Vendors are instructed to read and follow the instructions carefully, as any misinterpretation or failure to comply with instructions may lead to a Vendor's submittal being rejected.

Vendor MUST submit its solicitation response electronically and MUST confirm its submittal in order for the County to receive a valid response through BidSync. Refer to the Purchasing Division website or contact BidSync for submittal instructions.

A. Responsiveness Criteria:

In accordance with Broward County Procurement Code Section 21.8.b.65, a Responsive Bidder [Vendor] means a person who has submitted a proposal which conforms in all material respects to a solicitation. The solicitation submittal of a responsive Vendor must be submitted on the required forms, which contain all required information, signatures, notarizations, insurance, bonding, security, or other mandated requirements required by the solicitation documents to be submitted at the time of proposal opening.

Failure to provide the information required below at the time of submittal opening may result in a recommendation Vendor is non-responsive by the Director of Purchasing. The Selection or Evaluation Committee will determine whether the firm is responsive to the requirements specified herein. The County reserves the right to waive minor technicalities or irregularities as is in the best interest of the County in accordance with Section 21.30.f.1(c) of the Broward County Procurement Code.

Below are standard responsiveness criteria; refer to **Special Instructions to Vendors**, for Additional Responsiveness Criteria requirement(s).

1. Lobbyist Registration Requirement Certification

Refer to **Lobbyist Registration Requirement Certification**. The completed form should be submitted with the solicitation response but must be submitted within three business days of County's request. Vendor may be deemed non-responsive for failure to fully comply within stated timeframes.

2. Addenda

The County reserves the right to amend this solicitation prior to the due date. Any change(s) to this solicitation will be conveyed through the written addenda process. Only written addenda will be binding. If a "must" addendum is issued, Vendor must follow instructions and submit required information, forms, or acknowledge addendum, as instructed therein. It is the responsibility of all potential Vendors to monitor the solicitation for any changing information, prior to submitting their response.

B. Responsibility Criteria:

Definition of a Responsible Vendor: In accordance with Section 21.8.b.64 of the Broward County Procurement Code, a Responsible Vendor means a Vendor who has the capability in all respects to perform the contract requirements, and the integrity and reliability which will assure good faith performance.

The Selection or Evaluation Committee will recommend to the awarding authority a determination of a Vendor's responsibility. At any time prior to award, the awarding authority may find that a Vendor is not responsible to receive a particular award.

Failure to provide any of this required information and in the manner required may result in a recommendation by the Director of Purchasing that the Vendor is non-responsive.

Below are standard responsibility criteria; refer to **Special Instructions to Vendors**, for Additional Responsibility Criteria requirement(s).

1. **Litigation History**

a. All Vendors are required to disclose to the County all "material" cases filed, pending, or resolved during the last three (3) years prior to the solicitation response due date, whether such cases were brought by or against the Vendor, any parent or subsidiary of the Vendor, or any predecessor organization. Additionally, all Vendors are required to disclose to the County all "material" cases filed, pending, or resolved against any principal of Vendor, regardless of whether the principal was associated with Vendor at the time of the "material" cases against the principal, during the last three (3) years prior to the solicitation response. A case is considered to be "material" if it relates, in whole or in part, to any of the following:

i. A similar type of work that the vendor is seeking to perform for the County under the current solicitation;
ii. An allegation of fraud, negligence, error or omissions, or malpractice against the vendor or any of its principals or agents who would be performing work under the current solicitation;
iii. A vendor's default, termination, suspension, failure to perform, or improper performance in connection with any contract;
iv. The financial condition of the vendor, including any bankruptcy petition (voluntary and involuntary) or receivership; or
v. A criminal proceeding or hearing concerning business-related offenses in which the vendor or its principals (including officers) were/are defendants.

b. For each material case, the Vendor is required to provide all information identified in the **Litigation History Form**. Additionally, the Vendor shall provide a copy of any judgment or settlement of any material case during the last three (3) years prior to the solicitation response. Redactions of any confidential portions of the settlement agreement are only permitted upon a certification by Vendor that all redactions are required under the express terms of a pre-existing confidentiality agreement or provision.

c. The County will consider a Vendor's litigation history information in its review and determination of responsibility.

d. If the Vendor is a joint venture, the information provided should encompass the joint venture and each of the entities forming the joint venture.

e. A vendor is required to disclose to the County any and all cases(s) that exist between the County and any of the Vendor's subcontractors/subconsultants proposed to work on this project during the last five (5) years prior to the solicitation response.

f. Failure to disclose any material case, including all requested information in connection with each such case, as well as failure to disclose the Vendor's subcontractors/subconsultants litigation history against the County, may result in the Vendor being deemed non-responsive.

2. **Financial Information**

a. All Vendors are required to provide the Vendor's financial statements at the time of submittal in order to demonstrate the Vendor's financial capabilities.

b. Each Vendor shall submit its most recent two years of financial statements for review. The financial statements are not required to be audited financial statements. The annual financial statements will be in the form of:

i. Balance sheets, income statements and annual reports; or
ii. Tax returns; or
iii. SEC filings.

If tax returns are submitted, ensure it does not include any personal information (as defined under Florida Statutes Section 501.171, Florida Statutes), such as social security numbers, bank account or credit card numbers, or any personal pin numbers. If any personal information data is part of financial statements, redact information prior to submitting a response the County.

c. If a Vendor has been in business for less than the number of years of required financial statements, then the Vendor must disclose all years that the Vendor has been in business, including any partial year-to-date financial statements.

d. The County may consider the unavailability of the most recent year's financial statements and whether the Vendor acted in good faith in disclosing the financial documents in its evaluation.

e. Any claim of confidentiality on financial statements should be asserted at the time of submittal. Refer to **Standard Instructions to Vendors**, Confidential Material/ Public Records and Exemptions for instructions on submitting confidential financial statements. The Vendor's failure to provide the information as instructed may lead to the information becoming public.

f. Although the review of a Vendor's financial information is an issue of responsibility, the failure to either provide the financial documentation or correctly assert a confidentiality claim pursuant the Florida Public Records Law and the solicitation requirements (Confidential Material/ Public Records and Exemptions section) may result in a recommendation of non-responsiveness by the Director of Purchasing.

3. **Authority to Conduct Business in Florida**

a. A Vendor must have the authority to transact business in the State of Florida and be in good standing with the Florida Secretary of State. For further information, contact the Florida Department of State, Division of Corporations.

b. The County will review the Vendor's business status based on the information provided in response to this solicitation.

c. It is the Vendor's responsibility to comply with all state and local business requirements.

d. Vendor should list its active Florida Department of State Division of Corporations Document Number (or Registration No. for fictitious names) in the **Vendor Questionnaire**, Question No. 10.

e. If a Vendor is an out-of-state or foreign corporation or partnership, the Vendor must obtain the authority to transact business in the State of Florida or show evidence of application for the authority to transact business in the State of Florida, upon request of the County.

f. A Vendor that is not in good standing with the Florida Secretary of State at the time of a submission to this solicitation may be deemed non-responsible.

g. If successful in obtaining a contract award under this solicitation, the Vendor must remain in good standing throughout the contractual period of performance.

4. **Affiliated Entities of the Principal(s)**

a. All Vendors are required to disclose the names and addresses of “affiliated entities” of the Vendor’s principal(s) over the last five (5) years (from the solicitation opening deadline) that have acted as a prime Vendor with the County. The Vendor is required to provide all information required on the **Affiliated Entities of the Principal(s) Certification Form**.

b. The County will review all affiliated entities of the Vendor’s principal(s) for contract performance evaluations and the compliance history with the County’s Small Business Program, including CBE, DBE and SBE goal attainment requirements. “Affiliated entities” of the principal(s) are those entities related to the Vendor by the sharing of stock or other means of control, including but not limited to a subsidiary, parent or sibling entity.

c. The County will consider the contract performance evaluations and the compliance history of the affiliated entities of the Vendor's principals in its review and determination of responsibility.

5. **Insurance Requirements**

The **Insurance Requirement Form** reflects the insurance requirements deemed necessary for this project. It is not necessary to have this level of insurance in effect at the time of submittal, but it is necessary to submit certificates indicating that the Vendor currently carries the insurance or to submit a letter from the carrier indicating it can provide insurance coverages.

C. Additional Information and Certifications

The following forms and supporting information (if applicable) should be returned with Vendor’s submittal. If not provided with submittal, the Vendor must submit within three business days of County’s request. Failure to timely submit may affect Vendor’s evaluation.

1. **Vendor Questionnaire**

Vendor is required to submit detailed information on their firm. Refer to the **Vendor Questionnaire** and submit as instructed.

2. **Standard Certifications**

Vendor is required to certify to the below requirements. Refer to the **Standard Certifications** and submit as instructed.

a. **Cone of Silence Requirement Certification**
b. **Drug-Free Workplace Certification**
c. **Non-Collusion Certification**
d. **Public Entities Crimes Certification**
e. **Scrutinized Companies List Certification**

3. **Subcontractors/Subconsultants/Suppliers Requirement**

The Vendor shall submit a listing of all subcontractors, subconsultants, and major material suppliers, if any, and the portion of the contract they will perform. Vendors must follow the instructions included on the **Subcontractors/Subconsultants/Suppliers Information Form** and submit as instructed.

D. Standard Agreement Language Requirements

1. The acceptance of or any exceptions taken to the terms and conditions of the County's Agreement shall be considered a part of a Vendor's submittal and will be considered by the Selection or Evaluation Committee.

2. The applicable Agreement terms and conditions for this solicitation are indicated in the **Special Instructions to Vendors.**

3. Vendors are required to review the applicable terms and conditions and submit the **Agreement Exception Form**. If the **Agreement Exception Form** is not provided with the submittal, it shall be deemed an affirmation by the Vendor that it accepts the Agreement terms and conditions as disclosed in the solicitation.

4. If exceptions are taken, the Vendor must specifically identify each term and condition with which it is taking an exception. Any exception not specifically listed is deemed waived. Simply identifying a section or article number is not sufficient to state an exception. Provide either a redlined version of the specific change(s) or specific proposed alternative language. Additionally, a brief justification specifically addressing each provision to which an exception is taken should be provided.

5. Submission of any exceptions to the Agreement does not denote acceptance by the County. Furthermore, taking exceptions to the County's terms and conditions may be viewed unfavorably by the Selection or Evaluation Committee and ultimately may impact the overall evaluation of a Vendor's submittal.

E. Evaluation Criteria

1. The Selection or Evaluation Committee will evaluate Vendors as per the **Evaluation Criteria.** The County reserves the right to obtain additional information from a Vendor.

2. Vendor has a continuing obligation to inform the County in writing of any material changes to the information it has previously submitted. The County reserves the right to request additional information from Vendor at any time.

3. For Request for Proposals, the following shall apply:

   a. The Director of Purchasing may recommend to the Evaluation Committee to short list the most qualified firms prior to the Final Evaluation.

   b. The Evaluation Criteria identifies points available; a total of 100 points is available.

   c. If the Evaluation Criteria includes a request for pricing, the total points awarded for price is determined by applying the following formula:

      (Lowest Proposed Price/Vendor's Price) x (Maximum Number of Points for Price)
      = Price Score

   d. After completion of scoring, the County may negotiate pricing as in its best interest.

4. For Requests for Letters of Interest or Request for Qualifications, the following shall apply:

   a. The Selection or Evaluation Committee will create a short list of the most qualified firms.

   b. The Selection or Evaluation Committee will either:

i. Rank shortlisted firms; or
ii. If the solicitation is part of a two-step procurement, shortlisted firms will be requested to submit a response to the Step Two procurement.

F. Demonstrations

If applicable, as indicated in Special Instructions to Vendors, Vendors will be required to demonstrate the nature of their offered solution. After receipt of submittals, all Vendors will receive a description of, and arrangements for, the desired demonstration. In accordance with Section 286.0113 of the Florida Statutes and pursuant to the direction of the Broward County Board of Commissioners, demonstrations are closed to only the vendor team and County staff.

G. Presentations

Vendors that are found to be both responsive and responsible to the requirements of the solicitation and/or shortlisted (if applicable) will have an opportunity to make an oral presentation to the Selection or Evaluation Committee on the Vendor's approach to this project and the Vendor's ability to perform. The committee may provide a list of subject matter for the discussion. All Vendor's will have equal time to present but the question-and-answer time may vary. In accordance with Section 286.0113 of the Florida Statutes and the direction of the Broward County Board of Commissioners, presentations during Selection or Evaluation Committee Meetings are closed. Only the Selection or Evaluation Committee members, County staff and the vendor and their team scheduled for that presentation will be present in the Meeting Room during the presentation and subsequent question and answer period.

H. Public Art and Design Program

If indicated in **Special Instructions to Vendors,** Public Art and Design Program, Section 1-88, Broward County Code of Ordinances, applies to this project. It is the intent of the County to functionally integrate art, when applicable, into capital projects and integrate artists' design concepts into this improvement project. The Vendor may be required to collaborate with the artist(s) on design development within the scope of this request. Artist(s) shall be selected by Broward County through an independent process. For additional information, contact the Broward County Cultural Division.

I. Committee Appointment

The Cone of Silence shall be in effect for County staff at the time of the Selection or Evaluation Committee appointment and for County Commissioners and Commission staff at the time of the Shortlist Meeting of the Selection Committee or the Initial Evaluation Meeting of the Evaluation Committee. The committee members appointed for this solicitation are available on the Purchasing Division's website under Committee Appointment.

J. Committee Questions, Request for Clarifications, Additional Information

At any committee meeting, the Selection or Evaluation Committee members may ask questions, request clarification, or require additional information of any Vendor's submittal or proposal. It is highly recommended Vendors attend to answer any committee questions (if requested), including a Vendor representative that has the authority to bind.

Vendor's answers may impact evaluation (and scoring, if applicable). Upon written request to the Purchasing Agent prior to the meeting, a conference call number will be made available for Vendor participation via teleconference. Only Vendors that are found to be both responsive and responsible to the requirements of the solicitation and/or shortlisted (if applicable) are requested to participate in a final (or presentation) Selection or Evaluation committee meeting.

K. Vendor Questions

The County provides a specified time for Vendors to ask questions and seek clarification regarding solicitation requirements. All questions or clarification inquiries must be submitted through BidSync by the date and time referenced in the solicitation document (including any addenda). The County will respond to questions via Bid Sync.

L. Confidential Material/ Public Records and Exemptions

1. Broward County is a public agency subject to Chapter 119, Florida Statutes. Upon receipt, all submittals become "public records" and shall be subject to public disclosure consistent with Chapter 119, Florida Statutes. Submittals may be posted on the County's public website or included in a public records request response, unless there is a declaration of "confidentiality" pursuant to the public records law and in accordance with the procedures in this section.

2. Any confidential material(s) the Vendor asserts is exempt from public disclosure under Florida Statutes must be labeled as "Confidential", and marked with the specific statute and subsection asserting exemption from Public Records.

3. To submit confidential material, three hardcopies must be submitted in a sealed envelope, labeled with the solicitation number, title, date and the time of solicitation opening to:

   Broward County Purchasing Division
   115 South Andrews Avenue, Room 212
   Fort Lauderdale, FL 33301

4. Material will not be treated as confidential if the Vendor does not cite the applicable Florida Statute(s) allowing the document to be treated as confidential.

5. Any materials that the Vendor claims to be confidential and exempt from public records must be marked and separated from the submittal. If the Vendor does not comply with these instructions, the Vendor's claim for confidentiality will be deemed as waived.

6. Submitting confidential material may impact full discussion of your submittal by the Selection or Evaluation Committee because the Committee will be unable to discuss the details contained in the documents cloaked as confidential at the publicly noticed Committee meeting.

M. Copyrighted Materials

Copyrighted material is not exempt from the Public Records Law, Chapter 119, Florida Statutes. Submission of copyrighted material in response to any solicitation will constitute a license and permission for the County to make copies (including electronic copies) as reasonably necessary for the use by County staff and agents, as well as to make the materials available for inspection or production pursuant to Public Records Law, Chapter 119, Florida Statutes.

N. State and Local Preferences

If the solicitation involves a federally funded project where the fund requirements prohibit the use of state and/or local preferences, such preferences contained in the Local Preference Ordinance and Broward County Procurement Code will not be applied in the procurement process.

O. Local Preference

Except where otherwise prohibited by federal or state law or other funding source restrictions, a local Vendor whose submittal is within 5% of the highest total ranked Vendor outside of the preference area will become the Vendor with whom the County will proceed with negotiations for a final contract. Refer to **Local Vendor Certification Form (Preference and Tiebreaker)** for further information.

P. Tiebreaker Criteria

In accordance with Section 21.31.d of the Broward County Procurement Code, the tiebreaker criteria shall be applied based upon the information provided in the Vendor's response to the solicitation. In order to receive credit for any tiebreaker criterion, complete and accurate information must be contained in the Vendor's submittal.

1. **Local Vendor Certification Form (Preference and Tiebreaker);**
2. **Domestic Partnership Act Certification (Requirement and Tiebreaker);**
3. **Tiebreaker Criteria Form: Volume of Work Over Five Years**

Q. Posting of Solicitation Results and Recommendations

The Broward County Purchasing Division's website is the location for the County's posting of all solicitations and contract award results. It is the obligation of each Vendor to monitor the website in order to obtain complete and timely information.

R. Review and Evaluation of Responses

A Selection or Evaluation Committee is responsible for recommending the most qualified Vendor(s). The process for this procurement may proceed in the following manner:

1. The Purchasing Division delivers the solicitation submittals to agency staff for summarization for the committee members. Agency staff prepares a report, including a matrix of responses submitted by the Vendors. This may include a technical review, if applicable.

2. Staff identifies any incomplete responses. The Director of Purchasing reviews the information and makes a recommendation to the Selection or Evaluation Committee as to each Vendor's responsiveness to the requirements of the solicitation. The final determination of responsiveness rests solely on the decision of the committee.

3. At any time prior to award, the awarding authority may find that a Vendor is not responsible to receive a particular award. The awarding authority may consider the following factors, without limitation: debarment or removal from the authorized Vendors list or a final decree, declaration or order by a court or administrative hearing officer or tribunal of competent jurisdiction that the Vendor has breached or failed to perform a contract, claims history of the Vendor, performance history on a County contract(s), an unresolved concern, or any other cause under this code and Florida law for evaluating the responsibility of a Vendor.

S. Vendor Protest

Sections 21.118 and 21.120 of the Broward County Procurement Code set forth procedural requirements that apply if a Vendor intends to protest a solicitation or proposed award of a contract and state in part the following:

1. Any protest concerning the solicitation or other solicitation specifications or requirements must be made and received by the County within seven business days from the posting of the solicitation or addendum on the Purchasing Division's website. Such protest must be made in writing to the Director of Purchasing. Failure to timely protest solicitation specifications or requirements is a waiver of the ability to protest the specifications or requirements.

2. Any protest concerning a solicitation or proposed award above the award authority of the Director of Purchasing, after the RLI or RFP opening, shall be submitted in writing and received by the Director of Purchasing within five business days from the posting of the recommendation of award for Invitation to Bids or the final recommendation of ranking for Request for Letters of Interest and Request for Proposals on the Purchasing Division's website.

3. Any actual or prospective Vendor who has a substantial interest in and is aggrieved in connection with the proposed award of a contract that does not exceed the amount of the award authority of the Director of Purchasing, may protest to the Director of Purchasing. The protest shall be submitted in writing and received within three (3) business days from the posting of the recommendation of award for Invitation to Bids or the final recommendation of ranking for Request for Letters of Interest and Request for Proposals on the Purchasing Division's website.

4. For purposes of this section, a business day is defined as Monday through Friday between 8:30 a.m. and 5:00 p.m. Failure to timely file a protest within the time prescribed for a proposed contract award shall be a waiver of the Vendor's right to protest.

5. As a condition of initiating any protest, the protestor shall present the Director of Purchasing a nonrefundable filing fee in accordance with the table below.

Estimated Contract Amount	Filing Fee
$30,000 - $250,000	$ 500
$250,001 - $500,000	$1,000
$500,001 - $5 million	$3,000
Over $5 million	5,000

If no contract proposal amount was submitted, the estimated contract amount shall be the County's estimated contract price for the project. The County may accept cash, money order, certified check, or cashier's check, payable to Broward County Board of Commissioners.

T. Right of Appeal

Pursuant to Section 21.83.d of the Broward County Procurement Code, any Vendor that has a substantial interest in the matter and is dissatisfied or aggrieved in connection with the Selection or Evaluation Committee's determination of responsiveness may appeal the determination pursuant to Section 21.120 of the Broward County Procurement Code.

1. The appeal must be in writing and sent to the Director of Purchasing within ten (10) calendar days of the determination by the Selection or Evaluation Committee to be deemed timely.

2. As required by Section 21.120, the appeal must be accompanied by an appeal bond by a Vendor having standing to protest and must comply with all other requirements of this section.

3. The institution and filing of an appeal is an administrative remedy to be employed prior to the institution and filing of any civil action against the County concerning the subject matter of the appeal.

U. Rejection of Responses

The Selection or Evaluation Committee may recommend rejecting all submittals as in the best interests of the County. The rejection shall be made by the Director of Purchasing, except when a solicitation was approved by the Board, in which case the rejection shall be made by the Board.

V. Negotiations

The County intends to conduct the first negotiation meeting no later than two weeks after approval of the final ranking as recommended by the Selection or Evaluation Committee. At least one of the representatives for the Vendor participating in negotiations with the County must be authorized to bind the Vendor. In the event that the negotiations are not successful within a reasonable timeframe (notification will be provided to the Vendor) an impasse will be declared and negotiations with the first-ranked Vendor will cease. Negotiations will begin with the next ranked Vendor, etc. until such time that all requirements of Broward County Procurement Code have been met. In accordance with Section 286.0113 of the Florida Statutes and the direction of the Broward County Board of Commissioners, negotiations resulting from Selection or Evaluation Committee Meetings are closed. Only County staff and the selected vendor and their team will be present during negotiations.

W. Submittal Instructions:

1. Broward County does not require any personal information (as defined under Section 501.171, Florida Statutes), such as social security numbers, driver license numbers, passport, military ID, bank account or credit card numbers, or any personal pin numbers, in order to submit a response for ANY Broward County solicitation. DO NOT INCLUDE any personal information data in any document submitted to the County. If any personal information data is part of a submittal, this information must be redacted prior to submitting a response to the County.

2. **Vendor MUST submit its solicitation response electronically and MUST confirm its submittal in order for the County to receive a valid response through BidSync.** It is the Vendor's sole responsibility to assure its response is submitted and received through BidSync by the date and time specified in the solicitation.

3. The County will not consider solicitation responses received by other means. Vendors are encouraged to submit their responses in advance of the due date and time specified in the solicitation document. In the event that the Vendor is having difficulty submitting the solicitation document through Bid Sync, immediately notify the Purchasing Agent and then contact BidSync for technical assistance.

4. Vendor must view, submit, and/or accept each of the documents in BidSync. Web-fillable forms can be filled out and submitted through BidSync.

5. After all documents are viewed, submitted, and/or accepted in BidSync, the Vendor must upload additional information requested by the solicitation (i.e. Evaluation Criteria and Financials Statements) in the Item Response Form in BidSync, under line one (regardless if pricing requested).

6. Vendor should upload responses to Evaluation Criteria in Microsoft Word or Excel format.

7. If the Vendor is declaring any material confidential and exempt from Public Records, refer to Confidential Material/ Public Records and Exemptions for instructions on submitting confidential material.

8. After all files are uploaded, Vendor must submit and **CONFIRM** its offer (by entering password) for offer to be received through BidSync.

9. If a solicitation requires an original Proposal Bond (per Special Instructions to Vendors), Vendor must submit in a sealed envelope, labeled with the solicitation number, title, date and the time of solicitation opening to:

   Broward County Purchasing Division
   115 South Andrews Avenue, Room 212
   Fort Lauderdale, FL 33301

   A copy of the Proposal Bond should also be uploaded into Bid Sync; this does not replace the requirement to have an original proposal bond. Vendors must submit the original Proposal Bond, by the solicitation due date and time.

Supplier: **FlashParking**

AFFILIATED ENTITIES OF THE PRINCIPAL(S) CERTIFICATION FORM

The completed form should be submitted with the solicitation response but must be submitted within three business days of County's request. Vendor may be deemed non-responsive for failure to fully comply within stated timeframes.

a. All Vendors are required to disclose the names and addresses of "affiliated entities" of the Vendor's principal(s) over the last five (5) years (from the solicitation opening deadline) that have acted as a prime Vendor with the County.

b. The County will review all affiliated entities of the Vendor's principal(s) for contract performance evaluations and the compliance history with the County's Small Business Program, including CBE, DBE and SBE goal attainment requirements. "Affiliated entities" of the principal(s) are those entities related to the Vendor by the sharing of stock or other means of control, including but not limited to a subsidiary, parent or sibling entity.

c. The County will consider the contract performance evaluations and the compliance history of the affiliated entities of the Vendor's principals in its review and determination of responsibility.

The Vendor hereby certifies that: (select one)

☑ No principal of the proposing Vendor has prior affiliations that meet the criteria defined as "Affiliated entities"

□ Principal(s) listed below have prior affiliations that meet the criteria defined as "Affiliated entities"

Principal's Name:

Names of Affiliated Entities:

Principal's Name:

Names of Affiliated Entities:

Principal's Name:

Names of Affiliated Entities:

Authorized Signature Name: **Sam Goodner**

Title: **Chief Strategy Officer**

Vendor Name: **FlashParking, Inc**

Date: **2/13/20**

Supplier: **FlashParking**

AGREEMENT EXCEPTION FORM

The completed form(s) should be returned with the Vendor's submittal. If not provided with submittal, it shall be deemed an affirmation by the Vendor that it accepts the terms and conditions of the County's Agreement as disclosed in the solicitation.

The Vendor must either provide specific proposed alternative language on the form below. Additionally, a brief justification specifically addressing each provision to which an exception is taken should be provided.

□ There are no exceptions to the terms and conditions of the County Agreement as referenced in the solicitation; or

☑ The following exceptions are disclosed below: (use additional forms as needed; separate each Article/ Section number)

Term or Condition Article / Section	Insert version of exception or specific proposed alternative language	Provide brief justification for change
3.2.1. Software License	**Remove this section entirely.**	**FlashParking is providing the County a SaaS subscription, not an installed software solution. Section 3.2.2 (Subscription rights) applies.**
3.5 Updates, Upgrades and Releases	**Remove the words "with advance notice"**	**FlashParking is constantly updating the hosting system and cannot provide advance notice to its customers.**
3.9 Escrow Agreement	**Remove this section entirely**	**FlashParking will not place its source code in escrow.**
5.7 Foreign Entity Tax Withholding	**Remove this section entirely**	**FlashParking is a US company.**
8.4 ADA Compliance	**Remove this section entirely**	**While FlashParking parking equipment (kiosks) are ADA compliant, the software portal used by the County's employees is not Section 504 certified.**

Vendor Name: **FlashParking, Inc**

Supplier: **FlashParking**

DOMESTIC PARTNERSHIP ACT CERTIFICATION FORM (REQUIREMENT AND TIEBREAKER)

Refer to Special Instructions to identify if Domestic Partnership Act is a requirement of the solicitation or acts only as a tiebreaker. If Domestic Partnership is a requirement of the solicitation, the completed and signed form should be returned with the Vendor's submittal. If the form is not provided with submittal, the Vendor must submit within three business days of County's request. Vendor may be deemed non-responsive for failure to fully comply within stated timeframes. To qualify for the Domestic Partnership tiebreaker criterion, the Vendor must currently offer the Domestic Partnership benefit and the completed and signed form must be returned at time of solicitation submittal.

The Domestic Partnership Act, Section 16 ½ -157, Broward County Code of Ordinances, requires all Vendors contracting with the County, in an amount over $100,000 provide benefits to Domestic Partners of its employees, on the same basis as it provides benefits to employees' spouses, with certain exceptions as provided by the Ordinance.

For all submittals over $100,000.00, the Vendor, by virtue of the signature below, certifies that it is aware of the requirements of Broward County's Domestic Partnership Act, Section 16-½ -157, Broward County Code of Ordinances; and certifies the following: (check only one below).

☑ 1. The Vendor currently complies with the requirements of the County's Domestic Partnership Act and provides benefits to Domestic Partners of its employees on the same basis as it provides benefits to employees' spouses

□ 2. The Vendor will comply with the requirements of the County's Domestic Partnership Act at time of contract award and provide benefits to Domestic Partners of its employees on the same basis as it provides benefits to employees' spouses.

□ 3. The Vendor will not comply with the requirements of the County's Domestic Partnership Act at time of award.

□ 4. The Vendor does not need to comply with the requirements of the County's Domestic Partnership Act at time of award because the following exception(s) applies: **(check only one below)**.

- □ The Vendor is a governmental entity, not-for-profit corporation, or charitable organization.
- □ The Vendor is a religious organization, association, society, or non-profit charitable or educational institution.
- □ The Vendor provides an employee the cash equivalent of benefits. (Attach an affidavit in compliance with the Act stating the efforts taken to provide such benefits and the amount of the cash equivalent).
- □ The Vendor cannot comply with the provisions of the Domestic Partnership Act because it would violate the laws, rules or regulations of federal or state law or would violate or be inconsistent with the terms or conditions of a grant or contract with the United States or State of Florida. Indicate the law, statute or regulation (State the law, statute or regulation and attach explanation of its applicability).

Sam Goodner	**Chief Strategy Officer**	**FlashParking, Inc**	**2/13/20**
Authorized Signature/Name	**Title**	**Vendor Name**	**Date**

6

Supplier: **FlashParking**

LITIGATION HISTORY FORM

The completed form(s) should be returned with the Vendor's submittal. If not provided with submittal, the Vendor must submit within three business days of County's request. Vendor may be deemed non-responsive for failure to fully comply within stated timeframes.

□ There are no material cases for this Vendor; or

☑ Material Case(s) are disclosed below:

Is this for a: (check type) □ Parent, □ Subsidiary, or □ Predecessor Firm?	If Yes, name of Parent/Subsidiary/Predecessor:
	Or No ☑
Party	
Case Number, Name, and Date Filed	**Case Number D-1-GN-19-003816, filed 7-9-2019**
Name of Court or other tribunal	**Travis County District Court**
Type of Case	Bankruptcy □ Civil ☑ Criminal □ Administrative/Regulatory □
Claim or Cause of Action and Brief description of each Count	**FlashParking is currently involved in a dispute with a former supplier called Scientific Machine & Welding Inc. in which they claim that FlashParking breached a contract for canceling an order. The case has been submitted to the judge for summary judgement, which is still pending.**
Brief description of the Subject Matter and Project Involved	**FlashParking is currently involved in a dispute with a former supplier called Scientific Machine & Welding Inc. in which they claim that FlashParking breached a contract for canceling an order. The case has been submitted to the judge for summary judgement, which is still pending.**
Disposition of Case (Attach copy of any applicable Judgment, Settlement Agreement and Satisfaction of Judgment.)	Pending ☑ Settled □ Dismissed □ Judgment Vendor's Favor □ Judgment Against Vendor □ If Judgment Against, is Judgment Satisfied? □ Yes □ No
Opposing Counsel	Name: **Brent A. Devere** Email: **bdevere@1411west.com** Telephone Number: **(512) 797-0100**

Vendor Name: FlashParking, Inc

Supplier: **FlashParking**

LOBBYIST REGISTRATION REQUIREMENT CERTIFICATION FORM

The completed form should be submitted with the solicitation response but must be submitted within three business days of County's request. Vendor may be deemed non-responsive for failure to fully comply within stated timeframes.

The Vendor certifies that it understands if it has retained a lobbyist(s) to lobby in connection with a competitive solicitation, it shall be deemed non-responsive unless the firm, in responding to the competitive solicitation, certifies that each lobbyist retained has timely filed the registration or amended registration required under Broward County Lobbyist Registration Act, Section 1-262, Broward County Code of Ordinances; and it understands that if, after awarding a contract in connection with the solicitation, the County learns that the certification was erroneous, and upon investigation determines that the error was willful or intentional on the part of the Vendor, the County may, on that basis, exercise any contractual right to terminate the contract for convenience.

The Vendor hereby certifies that: (select one)

☑ It has not retained a lobbyist(s) to lobby in connection with this competitive solicitation; however, if retained after the solicitation, the County will be notified.

□ It has retained a lobbyist(s) to lobby in connection with this competitive solicitation and certified that each lobbyist retained has timely filed the registration or amended registration required under Broward County Lobbyist Registration Act, Section 1-262, Broward County Code of Ordinances.

It is a requirement of this solicitation that the names of any and all lobbyists retained to lobby in connection with this solicitation be listed below:

Name of Lobbyist:
Lobbyist's Firm:
Phone:
E-mail: **julie.thiers@flashparking.com**

Name of Lobbyist:
Lobbyist's Firm:
Phone:
E-mail:

Authorized Signature/Name: Sam Goodner   Date: 2/13/20

Title: Chief Strategy Officer

Vendor Name: FlashParking, Inc

Supplier: **FlashParking**

VENDOR QUESTIONNAIRE AND STANDARD CERTIFICATIONS
Request for Proposals, Request for Qualifications, or Request for Letters of Interest

Vendor should complete questionnaire and complete and acknowledge the standard certifications and submit with the solicitation response. If not submitted with solicitation response, it must be submitted within three business days of County's request. Failure to timely submit may affect Vendor's evaluation.

If a response requires additional information, the Vendor should upload a written detailed response with submittal; each response should be numbered to match the question number. The completed questionnaire and attached responses will become part of the procurement record. It is imperative that the person completing the Vendor Questionnaire be knowledgeable about the proposing Vendor's business and operations.

1. Legal business name:**FlashParking, Inc**

2. Doing Business As/ Fictitious Name (if applicable):

3. Federal Employer I.D. no. (FEIN):**45-1867889**

4. Dun and Bradstreet No.:**968547393**

5. Website address (if applicable): **www.flashparking.com**

6. Principal place of business address: **3801 S Capital of Texas Hwy #250,
Austin, TX 78704**

7. Office location responsible for this project: **3801 S Capital of Texas Hwy #250,
Austin, TX 78704**

8. Telephone no.:**512-547-9998** Fax no.:

9. Type of business (check appropriate box):

☑ Corporation (specify the state of incorporation):**C Corporation**

☐ Sole Proprietor

☐ Limited Liability Company (LLC)

☐ Limited Partnership

☐ General Partnership (State and County Filed In)

☐ Other - Specify

10. List Florida Department of State, Division of Corporations document number (or registration number if fictitious name): **5573004**

11. List name and title of each principal, owner, officer, and major shareholder:

a) **L Catterton**
b) **G51 Capital**
c) **Geekdom Fund**
d) **Austin Ventures**

12. AUTHORIZED CONTACT(S) FOR YOUR FIRM:

Name: **Sam Goodner**

Title: **Chief Strategy Officer**

E-mail: **sam.goodner@flashparking.com**

Telephone No.: **888-737-7465**

Name: **Jim DuFon**

Title: **Vice President- Government Projects**

E-mail: **james.dufon@flashparking.com**

Telephone No.: **512-547-9998**

13. Has your firm, its principals, officers or predecessor organization(s) been debarred or suspended by any government entity within the last three years? If yes, specify details in an attached written response. □ Yes ☑ No

14. Has your firm, its principals, officers or predecessor organization(s) ever been debarred or suspended by any government entity? If yes, specify details in an attached written response, including the reinstatement date, if granted. □ Yes ☑ No

15. Has your firm ever failed to complete any services and/or delivery of products during the last three (3) years? If yes, specify details in an attached written response. □ Yes ☑ No

16. Is your firm or any of its principals or officers currently principals or officers of another organization? If yes, specify details in an attached written response. □ Yes ☑ No

17. Have any voluntary or involuntary bankruptcy petitions been filed by or against your firm, its parent or subsidiaries or predecessor organizations during the last three years? If yes, specify details in an attached written response. □ Yes ☑ No

18. Has your firm's surety ever intervened to assist in the completion of a contract or have Performance and/or Payment Bond claims been made to your firm or its predecessor's sureties during the last three years? If yes, specify details in an attached written response, including contact information for owner and surety. □ Yes ☑ No

19. Has your firm ever failed to complete any work awarded to you, services and/or delivery of products during the last three (3) years? If yes, specify details in an attached written response. □ Yes ☑ No

20. Has your firm ever been terminated from a contract within the last three years? If yes, specify details in an attached written response. □ Yes ☑ No

21. Living Wage solicitations only: In determining what, if any, fiscal impacts(s) are a result of the Ordinance for this solicitation, provide the following for informational purposes only. Response is not considered in determining the award of this contract.
Living Wage had an effect on the pricing. □ Yes ☑ No □ N/A

If yes, Living Wage increased the pricing by% or decreased the pricing by%.

Cone of Silence Requirement Certification:

The Cone of Silence Ordinance, Section 1-266, Broward County Code of Ordinances prohibits certain communications among Vendors, Commissioners, County staff, and Selection or Evaluation Committee members. Identify on a separate sheet any violations of this Ordinance by any members of the responding firm or its joint ventures. After the application of the Cone of Silence, inquiries regarding this solicitation should be directed to the Director of Purchasing or designee. The Cone of Silence terminates when the County Commission or other awarding authority takes action which ends the solicitation.

The Vendor hereby certifies that: (check each box)

☑ The Vendor has read Cone of Silence Ordinance, Section 1-266, Broward County Code of Ordinances; and

☑ The Vendor understands that the Cone of Silence for this competitive solicitation shall be in effect beginning upon the appointment of the Selection or Evaluation Committee, for communication regarding this solicitation with the County Administrator, Deputy County Administrator, Assistant County Administrators, and Assistants to the County Administrator and their respective support staff or any person, including Evaluation or Selection Committee members, appointed to evaluate or recommend selection in this RFP/RLI process. For Communication with County Commissioners and Commission staff, the Cone of Silence allows communication until the initial Evaluation or Selection Committee Meeting.

☑ The vendor understands that they may communicate with a representative of the Office of Economic and Small Business Development ("OESBD") at any time regarding a solicitation or regarding participation of Small Business Enterprises or County Business Enterprises in a solicitation. OESBD may be contacted at (954) 357-6400. The Cone of Silence also permits communication with certain other County employees (refer to the Cone of Silence Ordinance).

☑ The Vendor agrees to comply with the requirements of the Cone of Silence Ordinance.

Drug-Free Workplace Requirements Certification:
Section 21.31.a. of the Broward County Procurement Code requires awards of all competitive solicitations requiring Board award be made only to firms certifying the establishment of a drug free workplace program. The program must consist of:

1. Publishing a statement notifying its employees that the unlawful manufacture, distribution, dispensing, possession, or use of a controlled substance is prohibited in the offeror's workplace, and specifying the actions that will be taken against employees for violations of such prohibition;

2. Establishing a continuing drug-free awareness program to inform its employees about:
   a. The dangers of drug abuse in the workplace;
   b. The offeror's policy of maintaining a drug-free workplace;
   c. Any available drug counseling, rehabilitation, and employee assistance programs; and
   d. The penalties that may be imposed upon employees for drug abuse violations occurring in the workplace;

3. Giving all employees engaged in performance of the contract a copy of the statement required by subparagraph 1;

4. Notifying all employees, in writing, of the statement required by subparagraph 1, that as a condition of employment on a covered contract, the employee shall:
   a. Abide by the terms of the statement; and
   b. Notify the employer in writing of the employee's conviction of, or plea of guilty or nolo contendere to, any violation of Chapter 893 or of any controlled substance law of the United States or of any state, for a violation occurring in the workplace NO later than five days after such conviction.

5. Notifying Broward County government in writing within 10 calendar days after receiving notice under subdivision 4.b above, from an employee or otherwise receiving actual notice of such conviction. The notice shall include the position title of the employee;

6. Within 30 calendar days after receiving notice under subparagraph 4 of a conviction, taking one of the following actions with respect to an employee who is convicted of a drug abuse violation occurring in the workplace:
   a. Taking appropriate personnel action against such employee, up to and including termination; or
   b. Requiring such employee to participate satisfactorily in a drug abuse assistance or rehabilitation program approved for such purposes by a federal, state, or local health, law enforcement, or other appropriate agency; and

7. Making a good faith effort to maintain a drug-free workplace program through implementation of subparagraphs 1 through 6.

The Vendor hereby certifies that: (check box)

☑ The Vendor certifies that it has established a drug free workplace program in accordance with the above requirements.

Non-Collusion Certification:

Vendor shall disclose, to their best knowledge, any Broward County officer or employee, or any relative of any such officer or employee as defined in Section 112.3135 (1) (c), Florida Statutes, who is an officer or director of, or has a material interest in, the Vendor's business, who is in a position to influence this procurement. Any Broward County officer or employee who has any input into the writing of specifications or requirements, solicitation of offers, decision to award, evaluation of offers, or any other activity pertinent to this procurement is presumed, for purposes hereof, to be in a position to influence this procurement. Failure of a Vendor to disclose any relationship described herein shall be reason for debarment in accordance with the provisions of the Broward County Procurement Code.

The Vendor hereby certifies that: (select one)

☑ The Vendor certifies that this offer is made independently and free from collusion; or

☑ The Vendor is disclosing names of officers or employees who have a material interest in this procurement and is in a position to influence this procurement. Vendor must include a list of name(s), and relationship(s) with its submittal.

Public Entities Crimes Certification:

In accordance with Public Entity Crimes, Section 287.133, Florida Statutes, a person or affiliate placed on the convicted vendor list following a conviction for a public entity crime may not submit on a contract: to provide any goods or services; for construction or repair of a public building or public work; for leases of real property to a public entity; and may not be awarded or perform work as a contractor, supplier, subcontractor, or consultant under a contract with any public entity; and may not transact business with any public entity in excess of the threshold amount provided in s. 287.017 for Category Two for a period of 36 months following the date of being placed on the convicted vendor list.

The Vendor hereby certifies that: (check box)

☑ The Vendor certifies that no person or affiliates of the Vendor are currently on the convicted vendor list and/or has not been found to commit a public entity crime, as described in the statutes.

Scrutinized Companies List Certification:

Any company, principals, or owners on the Scrutinized Companies with Activities in Sudan List, the Scrutinized Companies with Activities in the Iran Petroleum Energy Sector List, or the Scrutinized Companies that Boycott Israel List is prohibited from submitting a response to a solicitation for goods or services in an amount equal to or greater than $1 million.

The Vendor hereby certifies that: (check each box)

☑ The Vendor, owners, or principals are aware of the requirements of Sections 287.135, 215.473, and 215.4275, Florida Statutes, regarding Companies on the Scrutinized Companies with Activities in Sudan List the Scrutinized Companies with Activities in the Iran Petroleum Energy Sector List, or the Scrutinized Companies that Boycott Israel List; and

☑ The Vendor, owners, or principals, are eligible to participate in this solicitation and are not listed on either the Scrutinized Companies with Activities in Sudan List, the Scrutinized Companies with Activities in the Iran Petroleum Energy Sector List, or the Scrutinized Companies that Boycott Israel List; and

☑ If awarded the Contract, the Vendor, owners, or principals will immediately notify the County in writing if any of its principals are placed on the Scrutinized Companies with Activities in Sudan List, the Scrutinized Companies with Activities in the Iran Petroleum Energy Sector List, or the Scrutinized Companies that Boycott Israel List.

I hereby certify the information provided in the Vendor Questionnaire and Standard Certifications:

Sam Goodner	**Chief Strategy Officer**	**2/19/20**
*AUTHORIZED SIGNATURE/NAME	TITLE	DATE

Vendor Name: **FlashParking, Inc**

* I certify that I am authorized to sign this solicitation response on behalf of the Vendor as indicated in Certificate as to Corporate Principal, designation letter by Director/Corporate Officer, or other business authorization to bind on behalf of the Vendor. As the Vendor's authorized representative, I attest that any and all statements, oral, written or otherwise, made in support of the Vendor's response, are accurate, true and correct. I also acknowledge that inaccurate, untruthful, or incorrect statements made in support of the Vendor's response may be used by the County as a basis for rejection, rescission of the award, or termination of the contract and may also serve as the basis for debarment of Vendor pursuant to Section 21.119 of the Broward County Procurement Code. I certify that the Vendor's response is made without prior understanding, agreement, or connection with any corporation, firm or person submitting a response for the same items/services, and is in all respects fair and without collusion or fraud. I also certify that the Vendor agrees to abide by all terms and conditions of this solicitation, acknowledge and accept all of the solicitation pages as well as any special instructions sheet(s).

6

Supplier: **FlashParking**

RFP-RLI-RFQ LOCAL PREFERENCE AND TIE BREAKER CERTIFICATION FORM

The completed and signed form should be returned with the Vendor's submittal to determine Local Preference eligibility, however it must be returned at time of solicitation submittal to qualify for the Tie Break criteria. If not provided with submittal, the Vendor must submit within three business days of County's request for evaluation of Local Preference. Proof of a local business tax should be submitted with this form. Failure to timely submit this form or local business tax receipt may render the business ineligible for application of the Local Preference or Tie Break Criteria.

In accordance with Section 21.31.d. of the Broward County Procurement Code, to qualify for the Tie Break Criteria, the undersigned Vendor hereby certifies that (check box if applicable):

□ The Vendor is a local Vendor in Broward County and:

a. has a valid Broward County local business tax receipt;
b. has been in existence for at least six-months prior to the solicitation opening;
c. at a business address physically located within Broward County;
d. in an area zoned for such business;
e. provides services from this location on a day-to-day basis, and
f. services provided from this location are a substantial component of the services offered in the Vendor's proposal.

In accordance with Local Preference, Section 1-74, et. seq., Broward County Code of Ordinances, a local business meeting the below requirements is eligible for Local Preference. To qualify for the Local Preference, the undersigned Vendor hereby certifies that (check box if applicable):

□ The Vendor is a local Vendor in Broward and:

a. has a valid Broward County local business tax receipt issued at least one year prior to solicitation opening;
b. has been in existence for at least one-year prior to the solicitation opening;
c. provides services on a day-to-day basis, at a business address physically located within the Broward County limits in an area zoned for such business; and
d. the services provided from this location are a substantial component of the services offered in the Vendor's proposal.

Local Business Address:

Vendor does not qualify for Tie Break Criteria or Local Preference, in accordance with the above requirements. The undersigned Vendor hereby certifies that (check box if applicable): The Vendor is not a local Vendor in Broward County.

Sam Goodner	**Chief Strategy Officer**	**FlashParking, Inc**	**julie.thiers@flashparking.com**
AUTHORIZED SIGNATURE/NAME	**TITLE**	**COMPANY**	**DATE**

Supplier: **FlashParking**

RFP-RFQ-RLI LOCATION ATTESTATION FORM (EVALUATION CRITERIA)

The completed and signed form and supporting information (if applicable, for Joint Ventures) should be returned with the Vendor's submittal. If not provided with submittal, the Vendor must submit within three business days of County's request. Failure to timely submit this form and supporting information may affect the Vendor's evaluation. Provided information is subject to verification by the County.

A Vendor's principal place of business location (also known as the nerve center) within Broward County is considered in accordance with Evaluation Criteria. The County's definition of a principal place of business is:

1. As defined by the Broward County Local Preference Ordinance, "Principal place of business means the nerve center or center of overall direction, control and coordination of the activities of the bidder [Vendor]. If the bidder has only one (1) business location, such business location shall be considered its principal place of business."

2. A principal place of business refers to the place where a corporation's officers direct, control, and coordinate the corporation's day-to-day activities. It is the corporation's 'nerve center' and in practice it should normally be the place where the corporation maintains its headquarters; provided that the headquarters is the actual center of direction, control, and coordination, i.e., the 'nerve center', and not simply an office where the corporation holds its board meetings (for example, attended by directors and officers who have traveled there for the occasion).

The Vendor's principal place of business in Broward County shall be the Vendor's "Principal Address" as indicated with the Florida Department of State Division of Corporations, for at least six months prior to the solicitation's due date.

Check one of the following:

□ The Vendor certifies that it has a principal place of business location (also known as the nerve center) within Broward County, as documented in Florida Department of State Division of Corporations (Sunbiz), and attests to the following statements:

1. Vendor's address listed in its submittal is its principal place of business as defined by Broward County;

2. Vendor's "Principal Address" listed with the Florida Department of State Division of Corporations is the same as the address listed in its submittal and the address was listed for at least six months prior to the solicitation's opening date. A copy of Florida Department of State Division of Corporations (Sunbiz) is attached as verification.

3. Vendor must be located at the listed "nerve center" address ("Principal Address") for at least six (6) months prior to the solicitation's opening date;

4. Vendor has not merged with another firm within the last six months that is not headquartered in Broward County and is not a wholly owned subsidiary or a holding company of another firm that is not headquartered in Broward County;

5. If awarded a contract, it is the intent of the Vendor to remain at the referenced address for the duration of the contract term, including any renewals, extensions or any approved

interim contracts for the services provided under this contract; and

6. The Vendor understands that if after contract award, the County learns that the attestation was erroneous, and upon investigation determines that the error was willful or intentional on the part of the Vendor, the County may, on that basis exercise any contractual right to terminate the contract. Further any misleading, inaccurate, false information or documentation submitted by any party affiliated with this procurement may lead to suspension and/or debarment from doing business with Broward County as outlined in the Procurement Code, Section 21.119.

If the Vendor is submitting a response as a Joint Venture, the following information is required to be submitted:

a. Name of the Joint Venture Partnership
b. Percentage of Equity for all Joint Venture Partners
c. A copy of the executed Agreement(s) between the Joint Venture Partners

☑ Vendor does not have a principal place of business location (also known as the nerve center) within Broward County.

Vendor Information:

Vendor Name: **FlashParking**

Vendor's address listed in its submittal is:

3801 S Capital of Texas Hwy #250,
Austin, TX 78704

The signature below must be by an individual authorized to bind the Vendor. The signature below is an attestation that all information listed above and provided to Broward County is true and accurate.

Sam Goodner	**Chief Strategy Officer**	**FlashParking, Inc**	**2/19/20**
Authorized Signature/Name	Title	Vendor Name	Date

Supplier: **FlashParking**

Office of Economic and Small Business Requirements: CBE Goal Participation

A. In accordance with the Broward County Business Opportunity Act of 2012, Section 1-81, Code of Ordinances, as amended (the "Business Opportunity Act"), the County Business Enterprise (CBE) Program is applicable to this contract. All Vendors responding to this solicitation are required to utilize CBE firms to perform the assigned participation goal for this contract.

B. The CBE participation goal will be established based on the expected expenditure amount for the proposed scope of services for the project. The Office of Economic and Small Business Development (OESBD) will not include alternate items, optional services or allowances when establishing the CBE participation goal. If the County subsequently chooses to award any alternate items, optional services or allowances as determined by OESBD and the Contract Administrator to be related to the scope of services, OESBD may apply the established CBE participation goal. In such an instance, the County will issue a written notice to the successful Vendor that the CBE participation goal will also apply to the alternate items, optional services or allowances. Vendor shall submit all required forms pertaining to its compliance with the CBE participation goal, as applicable. Failure by Vendor to submit the required forms may result in the rejection of Vendor's solicitation submittal prior to the award or failure to comply with the contract requirements may have an impact on the vendor performance evaluation post award, as applicable.

C. CBE Program Requirements: Compliance with CBE participation goal requirements is a matter of responsibility; Vendor should submit all required forms and information with its solicitation submittal. If the required forms and information are not provided with the Vendor's solicitation submittal, then Vendor must supply the required forms and information no later than three (3) business days after request by OESBD. Vendor may be deemed non-responsible for failure to fully comply with CBE Program Requirements within these stated timeframes.

1. Vendor should include in its solicitation submittal a **Letter Of Intent Between Bidder/Offeror and County Business Enterprise (CBE) Subcontractor/Supplier** for each CBE firm the Vendor intends to use to achieve the assigned CBE participation goal. The form is available at the following link: http://www.broward.org/EconDev/Documents/CBELetterOfIntent.pdf

2. If Vendor is unable to attain the CBE participation goal, Vendor should include in its solicitation submittal an **Application for Evaluation of Good Faith Efforts** and all of the required supporting information. The form is available at the following link: http://www.broward.org/EconDev/WhatWeDo/Documents/GoodFaithEffortEval.pdf

D. OESBD maintains an online directory of CBE firms. The online directory is available for use by Vendors at https://webapps4.broward.org/smallbusiness/sbdirectory.aspx.

E. For detailed information regarding the CBE Program contact the OESBD at (954) 357-6400 or visit the website at: http://www.broward.org/EconDev/SmallBusiness/

F. If awarded the contract, Vendor agrees to and shall comply with all applicable requirements of the Business Opportunity Act and the CBE Program in the award and administration of the contract.

1. No party to this contract may discriminate on the basis of race, color, sex, religion,

national origin, disability, age, marital status, political affiliation, sexual orientation, pregnancy, or gender identity and expression in the performance of this contract.

2. All entities that seek to conduct business with the County, including Vendor or any Prime Contractors, Subcontractors, and Bidders, shall conduct such business activities in a fair and reasonable manner, free from fraud, coercion, collusion, intimidation, or bad faith. Failure to do so may result in the cancellation of this solicitation, cessation of contract negotiations, revocation of CBE certification, and suspension or debarment from future contracts.

3. If Vendor fails to meet or make Good Faith Efforts (as defined in the Business Opportunity Act) to meet the CBE participation commitment (the "Commitment"), then Vendor shall pay the County liquidated damages in an amount equal to fifty percent (50%) of the actual dollar amount by which Vendor failed to achieve the Commitment, up to a maximum amount of ten percent (10%) of the total contract amount, excluding costs and reimbursable expenses. An example of this calculation is stated in Section 1-81.7, Broward County Code of Ordinances.

4. Vendor shall comply with all applicable requirements of the Business Opportunity Act in the award of this contract. Failure by Vendor to carry out any of these requirements shall constitute a material breach of the contract, which shall permit the County to terminate this contract or to exercise any other remedy provided under this contract, the Broward County Code of Ordinances, the Broward County Administrative Code, or other applicable laws, with all such remedies being cumulative.

5. Vendor shall pay its CBE subcontractors and suppliers, within fifteen (15) days following receipt of payment from the County, for all completed subcontracted work and supplies. If Vendor withholds an amount from CBE subcontractors or suppliers as retainage, such retainage shall be released and paid within fifteen (15) days following receipt of payment of retained amounts from the County.

6. Vendor understands that the County will monitor Vendor's compliance with the CBE Program requirements. Vendor must provide OESBD with a Monthly Utilization Report (MUR) to confirm its compliance with the Commitment agreed to in the contract; timely submission of the MUR every month throughout the term of the contract, including amendment and extension terms, is a condition precedent to the County's payment of Vendor under the contract.

Supplier: **FlashParking**

Security Requirements – Aviation Department

A. Consultant/contractor agrees to observe all security requirements and other requirements of the Federal Aviation Regulations applicable to Consultant/contractor, including without limitation, all regulations of the United States Department of Transportation, the Federal Aviation Administration and the Transportation Security Administration, and the Consultant/contractor agrees to comply with the County's Airport Security Program and the Air Operations area (AOA) Vehicle Access Program, and amendments thereto, and to comply with such other rules and regulations as may be reasonably prescribed by the County, and to take such steps as may be necessary or directed by the County to insure that sub lessees, employees, invitees and guests observe these requirements. If required by the Aviation Department, Consultant/contractor shall conduct background checks of its employees in accordance with applicable Federal regulations.

B. If as a result of the acts or omissions of Consultant/contractor, its sub lessees, employees, invitees or guests, the County incurs any fines and/or penalties imposed by any governmental agency, including without limitation, the United States Department of Transportation, the Federal Aviation Administration or the Transportation Security Administration, or any expense in enforcing any federal regulations, including without limitation, airport security regulations, or the rules or regulations of the County, and/or any expense in enforcing the County's Airport Security Program, then consultant/contractor agrees to pay and/or reimburse the County all such costs and expenses, including all costs of administrative proceedings, court costs, and attorneys' fees and all costs incurred by County in enforcing this provision. Consultant/contractor further agrees to rectify any security deficiency or other deficiency as may be determined as such by the County or the United States Department of Transportation, Federal Aviation Administration, the Transportation Security Administration, or any other federal agency. In the event consultant/contractor fails to remedy any such deficiency, the County may do so at the cost and expense of consultant/contractor. The County reserves the right to take whatever action is necessary to rectify any security deficiency or other deficiency.

C. Operation of Vehicles on the AOA: Before the consultant/contractor shall permit any employee of consultant/contractor or any sub consultant/subcontractor to operate a motor vehicle of any kind or type on the AOA (and unless escorted by an Aviation Department approved escort), the consultant/contractor shall ensure that all such vehicle operators possess current, valid, and appropriate Florida driver's licenses. In addition, any motor vehicles and equipment of consultant/contractor or of any sub consultant/subcontractor operating on the AOA must have an appropriate vehicle identification permit issued by the Aviation Department, which identification must be displayed as required by the Aviation Department.

D. Consent to Search/Inspection: The consultant/contractor agrees that its vehicles, cargo, goods, and other personal property are subject to being inspected and searched when attempting to enter or leave and while on the AOA. The consultant/contractor further agrees on behalf of itself and its sub consultant /subcontractors that it shall not authorize any employee or other person to enter the AOA unless and until such employee other person has executed a written consent-to-search/inspection form acceptable to the Aviation Department. Consultant/contractor acknowledges and understands that the forgoing requirements are for the protection of users of the Airport and are intended to reduce incidents of cargo tampering, aircraft sabotage, thefts and other unlawful activities at the Airport. For this reason, consultant/contractor agrees that persons not executing such consent-to-search/inspection form shall not be employed by the consultant/contractor or by any sub consultant/contractor at the Airport in any position requiring access to the AOA or allowed entry to the AOA by the consultant/contractor or by any sub consultant/contractors.

E. The provisions hereof shall survive the expiration or any other termination of this contract.

6

Supplier: **FlashParking**

SUBCONTRACTORS/SUBCONSULTANTS/SUPPLIERS REQUIREMENT FORM

Request for Proposals, Request for Qualifications, or Request for Letters of Interest

The following forms and supporting information (if applicable) should be returned with Vendor's submittal. If not provided with submittal, the Vendor must submit within three business days of County's request. Failure to timely submit may affect Vendor's evaluation.

A. The Vendor shall submit a listing of all subcontractors, subconsultants and major material suppliers (firms), if any, and the portion of the contract they will perform. A major material supplier is considered any firm that provides construction material for construction contracts, or commodities for service contracts in excess of $50,000, to the Vendor.

B. If participation goals apply to the contract, only non-certified firms shall be identified on the form. A non-certified firm is a firm that is not listed as a firm for attainment of participation goals (ex. County Business Enterprise or Disadvantaged Business Enterprise), if applicable to the solicitation.

C. This list shall be kept up-to-date for the duration of the contract. If subcontractors, subconsultants or suppliers are stated, this does not relieve the Vendor from the prime responsibility of full and complete satisfactory performance under any awarded contract.

D. After completion of the contract/final payment, the Vendor shall certify the final list of non-certified subcontractors, subconsultants, and suppliers that performed or provided services to the County for the referenced contract.

E. The Vendor has confirmed that none of the recommended subcontractors, subconsultants, or suppliers' principal(s), officer(s), affiliate(s) or any other related companies have been debarred from doing business with Broward County or any other governmental agency.

If none, state "none" on this form. Use additional sheets as needed. Vendor should scan and upload any additional form(s) in BidSync.

1. Subcontracted Firm's Name:

   Subcontracted Firm's Address:

   Subcontracted Firm's Telephone Number:

   Contact Person's Name and Position:
   Contact Person's E-Mail Address:

   Estimated Subcontract/Supplies Contract Amount:

   Type of Work/Supplies Provided:

2. Subcontracted Firm's Name:

   Subcontracted Firm's Address:

   Subcontracted Firm's Telephone Number:

   Contact Person's Name and Position:

   Contact Person's E-Mail Address:

   Estimated Subcontract/Supplies Contract Amount:

Supplier: **FlashParking**

VOLUME OF PREVIOUS WORK ATTESTATION FORM

The completed and signed form should be returned with the Vendor's submittal. If not provided with submittal, the Vendor must submit within three business days of County's request. Failure to provide timely may affect the Vendor's evaluation.

This completed form MUST be included with the Vendor's submittal at the time of the opening deadline to be considered for a Tie Breaker criterion (if applicable).

Points assigned for Volume of Previous Work will be based on the amount paid-to-date by the County to a prime Vendor **MINUS** the Vendor's confirmed payments paid-to-date to approved certified County Business Enterprise (CBE) firms performing services as Vendor's subcontractor/subconsultant to obtain the CBE goal commitment as confirmed by County's Office of Economic and Small Business Development. Reporting must be within five (5) years of the current solicitation's opening date.

Vendor must list all received payments paid-to-date by contract as a prime vendor from Broward County Board of County Commissioners. Reporting must be within five (5) years of the current solicitation's opening date.

Vendor must also list all total confirmed payments paid-to-date by contract, to approved certified CBE firms utilized to obtain the contract's CBE goal commitment. Reporting must be within five (5) years of the current solicitation's opening date.

In accordance with Section 21.31.d. of the Broward County Procurement Code, the Vendor with the lowest dollar volume of work previously paid by the County over a five-year period from the date of the submittal opening will receive the Tie Breaker.

The Vendor attests to the following:

Item No.	Project Title	Contract No.	Department/ Division	Date Awarded	Prime: Paid to Date	CBE: Paid to Date
1.	**Margaritaville Hollywood Beach FL**		**PARCS**	**6/28/2019**	**$210,575.63**	**N/A**
2.	**1001 Brickell bay**		**PARCS**	**11/26/2019**	**$78,425.24**	**N/A**
3.	**Wynwood Garage**		**PARCS**	**6/29/2018**	**$140,039.00**	**N/A**
4.	**The Tides**		**FlashValet**	**11/14/2017**	**Annual Prepaid - $5,964.60**	**N/A**
5.	**Sea Air Tower**		**FlashValet**	**12/15/2017**	**Monthly Recurring - $149.00 + overages**	**N/A**
6.	**Hyde Resort and Residences**		**FlashValet**	**2/18/2020**	**No billing as of yet**	**N/A**
7.	**Etaru**		**FlashValet**	**10/31/2018**	**Monthly**	**N/A**

	Hallandale				**recurring - $99.00 + overages**	
				Grand Total	**$448,484.47**	**N/A**

Has the Vendor been a member/partner of a Joint Venture firm that was awarded a contract by the County?

Yes ☐ No ☑

If Yes, Vendor must submit a **Joint Vendor Volume of Work Attestation Form**.

Vendor Name: FlashParking, Inc

Sam Goodner **Authorized Signature/Name**	**Chief Strategy Officer** **Title**	**3/4/20** **Date**

VOLUME OF PREVIOUS WORK ATTESTATION JOINT VENTURE FORM

If applicable, this form and additional required documentation should be submitted with the Vendor's submittal. If not provided with submittal, the Vendor must submit within three business days of County's request. Failure to timely submit this form and supporting documentation may affect the Vendor's evaluation.

If a Joint Venture, the payments paid-to-date by contract provided must encompass the Joint Venture and each of the entities forming the Joint Venture. Points assigned for Volume of Previous Work will be based on the amount paid-to-date by contract to the Joint Venture firm **MINUS** all confirmed payments paid-to-date to approved certified CBE firms utilized to obtain the CBE goal commitment. Reporting must be within five (5) years of the current solicitation's opening date. Amount will then be multiplied by the member firm's equity percentage.

In accordance with Section 21.31.d. of the Broward County Procurement Code, the Vendor with the lowest dollar volume of work previously paid by the County over a five-year period from the date of the submittal opening will receive the Tie Breaker.

The Vendor attests to the following:

Item No.	Project Title	Contract No.	Department/ Division	Date Awarded	JV Equity Percent	Prime: Paid to Date	CBE: Paid to Date
1.							
2.							
3.							
4.							
5.							
6.							
7.							
8.							
					Grand Total	**N/A**	**N/A**

Vendor is required to submit an executed Joint Venture agreement(s) and any amendments for each project listed above. Each agreement must be executed prior to the opening date of this solicitation.

Vendor Name:

Authorized Signature/Name **Title** **Date**

Finance and Administrative Services Department
PURCHASING DIVISION
115 S. Andrews Avenue, Room 212 • Fort Lauderdale, Florida 33301 • 954-357-6066 • FAX 954-357-8535

Summary of Vendor Rights Regarding Broward County Competitive Solicitations

The purpose of this document is to provide vendors with a summary of their rights to object to or protest a proposed award or recommended ranking of vendors in connection with Broward County competitive solicitations. These rights are fully set forth in the Broward County Procurement Code, which is available here: https://www.broward.org/purchasing.

1. Right to Object

The right to object is available for solicitations conducted through Requests for Proposals ("RFPs") or Requests for Letters of Interest ("RLIs"). In such solicitations, vendors may object in writing to a proposed recommendation of ranking made by a Selection or Evaluation Committee. Objections must be filed within three (3) business days after the proposed recommendation is posted on the Purchasing Division's website. The contents of an objection must comply with the requirements set forth in Section 21.84 of the Procurement Code. Failure to timely and fully meet any requirement will result in a loss of the right to object.

2. Right to Protest

The right to protest is available for RFPs and RLIs and in solicitations conducted through Invitations to Bid ("ITBs"). In RFPs and RLIs, vendors may protest a final recommendation of ranking made by a Selection or Evaluation Committee. In ITBs, vendors may protest a final recommendation for award made by the Broward County Purchasing Division.

In all cases, protests must be filed in writing within three (3) or five (5) business days after a recommended ranking or recommendation for award is posted on Purchasing Division's website. The timeframe for filing (*i.e.,* 3 or 5 business days) depends on the monetary value of the procurement. Additional requirements for a protest are set forth in Section 21.118 of the Procurement Code. Failure to timely and fully meet any requirement will result in a loss of protest rights.

Vendors may appeal the denial of a protest. Appeals may require payment of an appeal bond. Additional requirements for an appeal are set forth in Section 21.120 of the Procurement Code. Failure to timely and fully meet any requirement will result in a loss of appeal rights.

3. Cone of Silence; Right to Contact OESBD

Please be aware that a Cone of Silence remains in effect for competitive solicitations until a solicitation is completed or a contract is awarded. During that time period, vendors may not contact certain County officials and employees regarding a solicitation. Substantial penalties may result from even an unintentional violation. For further information, please contact the Purchasing Division at 954-357-6066 or refer to the Cone of Silence Ordinance which is available here: https://www.broward.org/Purchasing/Documents/ConeOfSilence.pdf.

However, vendors may communicate with a representative of the Office of Economic and Small Business Development ("OESBD") at any time regarding a solicitation or regarding participation of Small Business Enterprises or County Business Enterprises in a solicitation. OESBD may be contacted at (954) 357-6400. The Cone of Silence also permits communication with certain other County employees (please see the Cone of Silence Ordinance at the above link for further details).

6