CITY OF VANCOUVER

CITY CLERK'S DEPARTMENT
Access to Information & Privacy Division

File No.: 04-1000-20-2021-062

December 17, 2021

s.22(1)

Dear s.22(1)

Re: **Request for Access to Records under the Freedom of Information and Protection of Privacy Act (the "Act")**

I am responding to your request of January 29, 2021 for:

Current and past contracts the City has with PayByPhone.

All responsive records are attached.

Please note: the City was just informed by the OIPC that mediation with a third party, who objected to the release, is now complete. The OIPC agrees with the City that there are no grounds for withholding these records.

Under section 52 of the Act, and within 30 business days of receipt of this letter, you may ask the Information & Privacy Commissioner to review any matter related to the City's response to your FOI request by writing to: Office of the Information & Privacy Commissioner, info@oipc.bc.ca or by phoning 250-387-5629.

If you request a review, please provide the Commissioner's office with: 1) the request number (#04-1000-20-2021-062); 2) a copy of this letter; 3) a copy of your original request; and 4) detailed reasons why you are seeking the review.

Yours truly,

Cobi Falconer, FOI Case Manager, for

[Signature on file]

Barbara J. Van Fraassen, BA
Director, Access to Information & Privacy
Barbara.vanfraassen@vancouver.ca
453 W. 12th Avenue Vancouver BC V5Y 1V4

If you have any questions, please email us at foi@vancouver.ca and we will respond to you as soon as possible. Or you can call the FOI Case Manager at 604.871.6584.

Encl.

:ma

CITY OF VANCOUVER

PROFESSIONAL SERVICES AGREEMENT

THE SUPPLY OF PARKING METER PAYMENT BY PHONE SYSTEM

THIS AGREEMENT made as of the **25** day of **October, 2012** (the **"Effective Date"**)

BETWEEN:

CITY OF VANCOUVER
453 West 12th Avenue
Vancouver, British Columbia
V5Y 1V4

(the "City")

OF THE FIRST PART

AND:

PayByPhone Technologies Inc.
Suite 1700, Park Place, 666 Burrard Street,
Vancouver, British Columbia
V6C 2X8

(the "Contractor")

OF THE SECOND PART

(City and Contractor are hereinafter sometimes referred to individually as "Party" and collectively as "Parties")

WHEREAS:

A. Pursuant to the Request for Proposal, Proposal No.PS20120106 (the "RFP") the City invited proposals from qualified Proponents for the supply of a payment by phone parking system that meets the Requirements (as defined below);

City of Vancouver - FOI 2021-062 - Page 1 of 191

B. Contractor has agreed to perform such Requirements on the terms and conditions of the RFP as modified or expanded by Contractor's Proposal and subject to the following terms and conditions

C. The Contractor is currently under contract to provide similar services pursuant to an Agreement entitled "The Supply of Parking Meter Pay By Phone System" (the "Current Contract") between the City and the Vendor dated Oct 25th, 2006 which agreement is set to expire on October 24, 2012;

D. The City and Contractor have agreed that this Agreement will replace the Current Contract as of and on the terms set out below.

NOW THEREFORE this Agreement witnesses that in consideration of the premises and the covenants and agreements herein contained, the parties hereby covenant and agree as follows:

1.0 DEFINITIONS

1.1 The following words and terms, unless the context otherwise, shall have the meanings set out below. Words including the singular number include the plural and vice versa.

"Agreement" means the agreement between the City and Contractor as set out in the contract documents, excluding the Current Contract;

"BizTalk" means a Microsoft middleware that allows organizations to more easily connect disparate systems;

"City" means the municipal corporation, generally known as the City of Vancouver, as continued pursuant to the Vancouver Charter;

"City's Designated Representatives" means the City's employees or representatives who are authorized in writing to deal with Contractor on behalf of the City in connection with the goods and services or to make decisions in connection with the Contract;

"City's Wireless Parking/Ticketing System" means the City's hardware, software and related system components that enable the City's parking enforcement officers to monitor compliance and ticket parking violations within the City of Vancouver in real time using GSM mobile communications, and for certainty, currently includes as components of same, TicketManager and the Progress Database, but for certainty, includes all updates, upgrades, and routine replacements to same.

"Contract Documents" means this Form of Agreement, Contractor's Proposal Documents, the RFP and such other documents as listed in this Form of Agreement, including all amendments or addenda agreed between the parties;

City of Vancouver - FOI 2021-062 - Page 2 of 191

"Contractor" means the entity defined as such on the front page of the Contract Documents;

"Credit Card Processing Fee" has the meaning set out in Schedule A;

"Current Contract" has the meaning set out above in Recital C;

"City Customer Service" means those services to be provided by the City to members of the public who use the System, as set out in Addendum No. 1 of the RFP;

Code: "CCI" means Item requires customization, cost of customization included in system cost;

Code: "CCX" Item requires customization, cost of customization extra;

"Customer Service Web Application" means utilities and tools that customer service agent uses to create and edit customer accounts

"Effective Date" means the date on which the System is, in the sole opinion of the City Engineer, fully operational and which date is certified by the City Engineer in a written notice to the Contractor;

"FOIPOP" means Freedom of Information and Protection of Privacy. It is an Act of the provincial government that requires public institutions to prevent and protect the unauthorized collection, use, or disclosure of personal information;

"GSM" means Global System for Mobile Communications, is a standard set developed by the European Telecommunications Standards Institute (ETSI) to describe technologies for second generation (2G) digital cellular networks;

"GST" means the tax payable and imposed pursuant to Part IX of the Excise Tax Act (Canada), as amended or replaced from time to time, but excluding any provincial component collected by Canada on behalf of British Columbia, such as by way of example the provincial component authorized as of and from July 1, 2010 pursuant to the Consumption Tax Rebate and Transition Act (British Columbia);

"Hosted Service" means a service that delivers a combination of traditional information technology functions such as infrastructure, applications, security, monitoring, storage, Web development, website hosting, over the Internet or other wide area networks;

"HST" means the tax payable and imposed pursuant to Part IX of the Excise Tax Act (Canada), as amended or replaced from time to time, including any provincial component collected by Canada on behalf of British Columbia, such as by way of example the provincial component authorized as of and from July 1, 2010 pursuant to the Consumption Tax Rebate and Transition Act (British Columbia);

"IPS" means IPS Group, Inc. a manufacturer of credit card enabled parking meters;

"IVR" means Interactive Voice Response, a software application that accepts a combination of voice telephone input and touch-tone keypad selection and provides appropriate responses in the form of voice, fax, callback, email and perhaps other media. IVR is usually part of a larger application that includes database access;

"NFC" means Near Field Communication, is a set of standards for smartphones and similar devices to establish radio communication with each other by touching them together or bringing them into close proximity, usually no more than a few centimeters. Present and anticipated applications include contactless transactions, data exchange, and simplified setup of more complex communications such as Wifi;

"Pay Station" means an unattended machine that can accept payment for a service;

"Progress Database" means the relational database management system;

"Payment Card Association" means a network of issuing banks and acquiring banks that process payment cards of a specific brand which is the developer and publisher of the PCI-DSS;

"PCI - DSS" means Payment Card Association's data security standard;

"PDA" means Personal Digital Assistant, a term for any small mobile hand-held device that provides computing and information storage and retrieval capabilities for personal or business use. Increasingly, PDA's are combined with telephones and paging systems;

"Phone Payment" has the meaning set out in Section 3.2(2);

"PIN" means personal identification number;

"PKI" means public key infrastructure and enables users of a basically unsecured public network such as the Internet to securely and privately exchange data and money through the use of a public and a private cryptographic key pair that is obtained and shared through a trusted authority;

"Proposal" means the proposal submitted in response to the RFP by Contractor, a copy of which is attached hereto as Schedule "A";

"Proponent" means the individual, partnership, corporation or combination thereof, including joint ventures, who or which sign the Proposal form set out in Part D of the RFP;

"PST" means any tax similar to the tax previously payable and imposed pursuant to the Social Services Tax Act (British Columbia), as amended or replaced from time to time, such as by way of example the provincial sales tax anticipated to be authorized as of and from April 1, 2013 by way of the repeal of the Consumption Tax Rebate and Transition Act (British Columbia) and re-enactment, continuation, or amendment of the Social Services Tax Act (British Columbia);

"RFP" means Request for Proposal No. PS04050 including, but not limited to: Part B - Instructions to Proponents; Part C - Special Conditions; Part D - Proposal Form (with Attachment A - Legal Terms and Conditions); Appendix 1- Form of Agreement; Appendix 2 - Certificate of Insurance; Appendix 3 - Schedule of Rates; Appendix 4 - Response Notification Form; any additional attachments listed in the Table of Contents; and any amendments, Addenda, and/or clarifications pertaining to the RFP, a copy of which is appended hereto as Schedule "B";

"QR" means a Quick Response code, it is a 2 dimensional bar code that can be easily read by a cell phone. They are used to take a piece of information from a transitory media and put it in to your cell phone;

"Real time" means events simulated by a computer at the same speed that they would occur in real life;

"Requirements" means all of the specifications, requirements and services set out in the RFP and as modified or expanded by Contractor's Proposal or as further modified or expanded in this Agreement that describe the requirements that the services, goods, materials and equipment must meet and Contractor must provide;

"Security Clearance" means the security clearance level required of the City from time to time for personnel being allowed access to City sites;

"Services" means all the labour, materials, equipment, supplies, services and other items necessary for the execution, completion and fulfillment of the Requirements;

"Smartphone" means a mobile phone built on a mobile computing platform, with more advanced computing ability and connectivity than a regular cellular phone such as by way of example only, an iPhone, Blackberry, "Android", "Smart phone" and any other popular web-enabled WAP compatible cellular devices;

"Sub-Contractor" means all contractors, sub-contractors, suppliers and other agents of the Contractor;

City of Vancouver - FOI 2021-062 - Page 5 of 191

"System" means Contractor's payment by phone and payment by a web application system that incorporates a Hosted Service and that fulfils all of the Requirements including marketing;

"Term" means the time period starting on the execution of this Agreement and ending on the third anniversary of the Effective Date;

"TicketManager" means hand-held ticketing software running on Progress database. Licensed by Checker's is used by the City for enforcing parking regulations;

"Transaction" means a transaction by which a member of the public uses the System to pay City parking meter fees;

"Unavoidable Delay" has the meaning set out in Section 8 - Unavoidable Delay;

"VOIP" means Voice Over Internet Protocol, a standard specification for the transmission of voice, fax, and/or voice-messaging applications via the Internet and/or Intranets, as opposed to a switched telephone network;

"VPN" means a virtual private network (VPN), is a way to use a public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with secure access to their organization's network. A VPN works by using the shared public infrastructure while maintaining privacy through security procedures and tunneling protocols;

"Web Payment" has the meaning set out in Section 3.2(1)

"WAP" means Wireless Application Protocol, a standard specification for transmission of voice and data between wireless devices, such as cellular telephones and radio transceivers, and the Internet;

"WCB" means the Workers Compensation Act (British Columbia), including without limitation, the Occupational Health & Safety Regulation (BC Regulation 296/97, as amended by BC Regulation 185/99) enacted pursuant to such Act, all as such Act or Regulations are amended or re-enacted from time to time;

"WHMIS Legislation" are the laws governing the information that must be provided on labels of packaging containing hazardous materials;

"WorkSafeBC/OH&S Regulation" means the Workers Compensation Act (British Columbia), including without limitation, the Occupational Health & Safety Regulation (BC Regulation 296/97, as amended by BC Regulation 185/99) enacted pursuant to such Act, and as such Act or Regulations are amended or re-enacted from time to time;

"Work Site" means the site(s) where the Requirements are to be performed.

2.0 CONTRACT DOCUMENTS

2.1 The terms and conditions of the Contract Document, regardless of whether attached hereto, shall govern the terms of this Agreement. The Contract Documents are complementary, and what is called for by any one shall be as binding as if called for by all. In the event of any inconsistency or conflict between any of the terms and conditions within these Contract Documents, the provisions of the Contract Documents will take precedence and govern in the following priority:

(a) this Form of Agreement, including the schedules thereto;
(b) Contractor's Proposal;
(c) the RFP exclusive PART D - FORM OF AGREEMENT

3.0 REQUIREMENTS

Contractor will supply the City with the Requirements and all such other services and work as are necessary for or incidental thereto including all labour, supervision, management, overhead, materials, supplies and all other things necessary for or incidental to the Requirements and including, without limiting the generality of the foregoing, Contractor will, in addition to the other Requirements, at no extra cost to the City, comply with the following Requirements:

3.1 Contractor will continue to integrate into the System (as it has under the Current Contract), as soon as practicable after they are made available to any one of the Contractor's other customers, and provided they are compatible with the City's Wireless Parking/Ticketing System, any and all such improvements to the System as are acquired or developed and operated by the Contractor for use by the members of the public wishing to pay for parking meters by way of phone or web access.

3.2 Contractor will (as it has under the Current Contract) continue at all times to provide, operate and manage the System and ensure that it is continuously integrated with the City's Wireless Parking/Ticketing System.

There are two payment processing methods:

1) Web Payment:

a) Hosted Service provided by Contractor with link to City's website: vancouver.ca

b) Hosted Service provided by Contractor and specifically developed for "mobile applications" use namely accessible via Smartphone to City's website

c) Contractor to provide web services to customer

d) Hosted Services all fully integrated with City Customer Service

2) Phone Payment:

a) Hosted Service provided by Contractor

b) Hosted Services all fully integrated with City Customer Service

The Contractor will ensure that Phone Payment will continue at all times to be fully functional for all present and future City parking meters and will ensure that Web Payment will continue at all times to meet the Requirements set out in the City's RFP, Appendix 1 and as modified in Contractor's Proposal. The System must be able to be accessed by City of Vancouver's patrons by cellular phone, Smartphone, and via the Internet and the Contractor's website shall continue at all times to be designed and integrated to the satisfaction of the City Engineer to ensure that the Contractor's website makes it clear that the Contractor is authorized by the City to operate the System on behalf of the City.

3.3 The Contractor will also continue to at all times ensure that the design and interface including all rights necessary to use the interface between System and the City's Wireless parking/Ticketing System and this interface meet the Requirements set out in the City's RFP. The Contractor shall be responsible for maintaining data integrity and real-time sourcing to the City's Wireless Parking/Ticketing System as required.

3.4 The Contractor will continue at all times to ensure that the Phone Payment is fully integrated into the City's Customer Service function to the satisfaction of the City Engineer and without limiting the generality of the foregoing, Contractor will provide access to the Customer Service Web Application to City call centre for real time information and management reports on the transactions conducted using Phone Payment. The Contractor will continue to at all times ensure that the System provides standard reports for retrieving customer information and transactions by credit card, license plate or mobile phone number. In addition, Contractor will provide reports as tabled in section 2.3 General and Reporting Functionality, Appendix 1 Requirements in the RFP, at no extra cost to the City as and when requested by the City Engineer and within 7 days of each such request. The Contractor will ensure that at all times during the Term and at all times after the expiry or sooner termination of the Term, until the deletion of the data to the satisfaction of the City Engineer, all data received or generated by the System is stored in the manner required by FOIPOP. The Contractor will provide the City with continuous access to the System through a secure internet browser access point via City-owned computer equipment.

3.5 Subject always to Section 30.0 [No Promotion of Relationship], Contractor will execute a marketing program as outlined in Section 10.0 Requirements of the Contractor Proposal, subject to City approval.

3.5.1 Public Relations

Contractor and the City agree to develop a joint press strategy, acceptable to both parties, to promote the System's benefits within Vancouver.

3.5.2 Point of Purchase Signage

Contractor agrees to pay for the design, manufacture and installation of signage to promote the payment by phone service. This work may be done by City forces or the Contractor, at the City's discretion. The City agrees to provide adequate space for signage or stickers at each parking meter at which the System is enabled. Signage will incorporate marks from the City, Contractor and optionally co-marketing partners engaged in promotion of the System. The size and the form of such signage shall be to the satisfaction of both Contractor and the City. Following installation, the City agrees to provide a commercially reasonable level of maintenance to signage as may be reasonably required from time to time.

3.5.3 Co-Marketing Strategy

Subject always to Section 30.0 [No Promotion of Relationship], Contractor and the City may agree (but for certainty are not obligated) to jointly develop and execute a co-marketing strategy that engages partners that include but are not limited to wireless carriers, automobile associations, rental car agencies and others.

3.5.4 Other Promotional Activities

Subject always to Section 30.0 [No Promotion of Relationship], Contractor and the City may agree (but for certainty are not obligated) to jointly develop and exploit other promotional channels including, but not limited to:

City Enabled Channels

- Telephone on-hold messaging
  - Ticket enquiries / dispute lines
  - Parking enquiries
  - Towing & enforcement enquiries
  - Customer activation lines
- Inclusion of Payment by phone printed literature upon issuance of parking violations

- City Parking Web Site Messaging

Contractor Enabled Channels

- Incentive-based referral activities to encourage existing and new users to refer friends
- Contractor Web Site Messages
- Contractor parking activation
- Contractor broad print media advertising campaign in local media on a yearly basis in conjunction with new parking features

3.6 Contractor will provide, at no cost to the City, and as soon as reasonably practical once implemented for any other customer of the Contractor but subject to compatibility with the City's Wireless Parking/Ticketing System, any and all future enhancements to the System's functionality and will not invoice the City for any additional charges such as license, implementation or hosting fees, for any functionality that is available to other customers at no extra cost (as defined in Contractor's Proposal, Section 10.0 Requirements, 2.7 Future Functionality noted with codes CCI & A). The Contractor will detail the cost and delivery date of functionalities tabled with code CCX by December 31, 2012 but the City will not be obligated to receive or pay for same unless and until the City has agreed in writing to do so.

3.7 The Contractor will continue to ensure that the System remains fully functional and operational at all times including for certainty all required hardware and software maintenance and replacement, all at no extra cost to the City, and all in accordance with the RFP and Contractor's Proposal.

3.8 The City will provide City Customer Service and the Contractor will, as part of the customer service, administer and provide security for customer accounts.

3.9 The Contractor will deliver to the City Engineer on or before October 25, 2012, a detailed implementation plan and schedule describing how the Requirements described in the Project Plan, Section 10 of Contractor's Proposal (the "Start-up Plan") will be performed and then the City Engineer will review and comment or approve within 5 days of receipt and then the Contractor will revise and re-deliver within 5 days of receipt from the City Engineer, and in any event, the Contractor will complete all milestones and deliverables set out in the Start-up Plan by the December 31, 2012.

3.10 The Contractor confirms that it will provide training to City staff in accordance with Contractor's Proposal, Section 10.0 Requirements, 4.25 Training and that this training will be provided in a manner that allows same to be fully completed by City staff on or before December 21, 2012.

3.11 Contractor shall bear all costs of providing the Requirements and Services and save and except as expressly provided otherwise, is not entitled to any compensation or reimbursement from the City.

3.12 All money received by the Contractor for Transactions will be received in trust for the City and held in a separate bank account (at a Canadian Chartered Bank and in a branch located within Vancouver) by the Contractor (and expressly labelled and denoted by the Contractor's bank as being in trust for the City of Vancouver) and then every 7 calendar days or whenever the trust account balance exceeds Fifty Thousand ($50,000.00) Dollars, whichever occurs the soonest, pay to the City the full trust account balance and transfer to the account of the Contractor, the Contractor's fees in accordance with Schedule A. The Contractor will also deliver to the City every seven calendar days a summary of all Transactions and provide the City with access to any and all banking and financial records relating to or associated with the Transactions occurring within the summary report period(s). The Contractor will continuously provide the City with online access to Contractor's Transactions trust account and any related bank accounts.

3.13 If at any time during the Term of this Agreement, the City notifies Contractor that the City requires that all Transactions are to be paid directly to City-owned bank accounts, the Contractor will immediately take all steps necessary to accommodate this change and ensure that all subsequent payments for all Transactions are made directly to the City's bank and/or credit card processing account. The City will then pay to Contractor (within 30 days of receipt of the Transactions revenue and an invoice for same from the Contractor) from such payments received on account of such Transactions the fees payable to Contractor in accordance with Schedule A less any debit or credit card costs incurred by the City and any refunds due to the City on account of any service level defaults. The City will not be entitled to any mark-up on any debit or credit card processing costs and will not deduct processing costs to the extent that same are more than that which the Contractor was paying just prior to the notice given under this Section to pay Transactions revenue directly to the City's account.

4.0 LICENCE OF SOFTWARE

4.1 Contractor grants to the City a non-exclusive, non-transferable licence to use the System and any related documentation for the Term.

4.2 Contractor retains ownership of the System and the items supplied by Contractor with this Agreement are for the sole use of the City. The City agrees that it will not assign, sub-license, distribute, or transfer the System to any other person, firm, corporation or other organization without the prior written consent of Contractor. To the extent that Contractor discloses proprietary data and any information pursuant to this Agreement, the City acknowledges that Contractor claims and reserves all rights and benefits afforded proprietary information at law,

City of Vancouver - FOI 2021-062 - Page 11 of 191

that this Agreement does not transfer any title or interest in or to any proprietary data or information of the Contractor's to the City and that the licence of the System is granted only for the limited use of such proprietary data and information as set forth in this Agreement.

4.3 Subject to the requirements of Section 26.3 of this Agreement, Contractor and the City will jointly own any and all information and data collected by Contractor ("System Information") from customers engaging in Transactions and/or using the System or otherwise collected during the process of performing the Requirements and Services. Contractor and the City shall protect and only use the personal information (as defined by FOIPOP) within the System Information in accordance with the written consent of the customers, or as may otherwise be permitted by law. Notwithstanding the foregoing, but subject to Section 26.3, Contractor shall not under any circumstances release any System Information to any third party without the prior written consent of the other except that upon expiry or sooner termination of this Agreement this restriction on use and release will also cease and no longer apply. In the event of any conflict between this Section 4.3 and Section 26.6 of this Agreement, Section 26.6 shall take precedence.

5.0 TERM OF CONTRACT

5.1 This Agreement will be in full force and effect for the duration of the Term as defined in Section 1.1 [Definitions].

5.2 As of the start of the Term, the Current Contract will be deemed to have expired immediately and just prior to the start of the Term, and will then be automatically superceded and replaced by this Agreement.

5.3 This Agreement may be extended by the mutual written agreement of the parties for 2 additional one year periods. Where the Term (or any mutually agreed extension of same) expires, and the parties continue to deal with each other as though this Agreement has not expired, this Agreement will not be deemed to be renewed for an additional 3 year or 1 year period, but only on a month-to-month basis terminable on 30 days' prior written notice by either party.

6.0 FEES AND PAYMENT

6.1 The total compensation payable to the Contractor for the Requirements and Services (the "Contract Price") is fixed for the Term (and any extension) and will be paid in accordance with Section 3.12 in the amounts set out in Schedule A.

City of Vancouver - FOI 2021-062 - Page 12 of 191

7.0 TAXES

7.1 The Contractor will be responsible for and will collect and remit any and all HST, GST or PST imposed on the fees and payments received by them for the Services, namely, the fees set out in the Table in Schedule "A" to this Agreement while the City will be responsible for and will collect and remit any and all HST, GST or PST imposed on the payments received by the City for the Transactions.

7.2 Subject to the above clause 7.1, the Contractor will pay all HST, GST, PST and any other sales or excise taxes in force during the Term, as modified by any repeal, enactment, increase or decrease in such taxes.

7.3 The Contractor's invoices to the City will show the appropriate amounts for HST, GST, and PST as applicable.

7.4 For further certainty, the anticipated transition from HST to GST/PST in April, 2013 will not entitle the Contractor to any adjustment in the Contract Price on account of the loss of input tax credits or other residual impacts and similarly Section 7.2 above will not be applied or interpreted to entitle either party to any other changes to the Contract Price during the Term on account of the residual effects of changes in HST, GST and PST.

8.0 UNAVOIDABLE DELAY

8.1 Subject to Section 8.2, except for the performance of obligations to pay money, time periods for the City and Contractor's performance under the Contract will be extended for periods of time during which their performance is delayed or prevented due to an Unavoidable Delay. For the purposes of this section, an "Unavoidable Delay" means any circumstances beyond the reasonable control of the party trying to perform (such as, for example, strikes/lockouts, acts of God, war or other strife or governmental action) but expressly excludes any and all delays caused by Contractor's lack of financial resources or insolvency, strikes, lockouts or labour affiliations of Contractor's employees or Sub-Contractors, or governmental action taken in the enforcement of law specifically against Contractor.

8.2 Despite Section 8.1, nothing in this Section 8.2 will release Contractor from the obligation to pay the City concessions or rebates for Services interrupted or delayed by an Unavoidable Delay.

9.0 CHANGES IN REQUIREMENTS

9.1 The City Engineer may, by giving written notice to Contractor, request amendments to the Requirements. Upon receipt of such notice, Contractor will, as soon as practicable and in no event later than twenty (20) days after receipt of such notice, inform the City Engineer of any adjustments to the Contract Price, either increasing or decreasing the

Contract Price, that would be necessitated by such change in the Requirements, or alternatively, will notify the City Engineer that no adjustment is necessary. If adjustments to the Contract Price are necessary and the City Engineer confirms in writing that such adjustments are acceptable to it, the Requirements and the Contract Price will then be deemed to be amended as agreed by the City Engineer. If the City Engineer determines that such adjustments, or no adjustments, to the Contract Price are unacceptable and the City Engineer and Contractor are unable to agree on an acceptable price, the City Engineer shall be entitled to refer such issue to arbitration (pursuant to Article 21.0 [Dispute Resolution] to determine the price for such amendments to the Requirements or it may elect either to proceed with this Agreement without the proposed change or it may elect to cancel this Agreement, on 10 days prior written notice without further liability, or recourse, except to pay Contractor for all work duly performed and supplied to the City prior to the effective date of cancellation.

10.0 DISPUTES AS TO REQUIREMENTS

10.1 All reasonable orders or instructions with respect to the Requirements issued by the City Engineer to Contractor will be obeyed, performed and complied with by Contractor promptly, efficiently and to the satisfaction of the City Engineer. However, if Contractor is of the opinion that such orders or instructions are not authorized under the provisions of the Contract Documents or involve a change in the Requirements, it must so notify the City Engineer in writing before proceeding to carry them out and, in any event, within five (5) days of the receipt of such orders or instructions. The giving of such notice to and receipt by the City will not constitute an acknowledgement by the City as to the validity of Contractor's claim, and the City now reserves all rights to contest or dispute Contractor's claim. If Contractor does not so notify the City Engineer within the time so limited, it will not be entitled to claim at any time thereafter, that the orders or instructions were not so authorized or involved a change in the Requirements. Nevertheless, the giving of such notice to the City Engineer will not relieve Contractor of its obligation to carry out and to obey such orders or instructions.

11.0 ASSIGNMENT

11.1 Contractor acknowledges and agrees that the existing qualifications, experience and Security Clearances of its owners and managers is an important component of the Services and one of the key factors in the City's decision to accept Contractor's Proposal and enter into this Agreement. Accordingly, any material changes to its key personnel or any proposed changes to Contractor's shareholders, or any proposed assignment, franchising, licensing, subletting or other transfer of this Agreement will be of significant concern and interest to the City and the Contractor must immediately notify the City of any such change or

proposed change as soon as reasonably possible.

11.2 Contractor may not assign, sublet, transfer or let out as task work any part of the Services, and will not assign any interest or any right to payment under this Agreement without first having had and obtained the consent in writing of the City, which consent the City may elect to withhold in its sole discretion. If the City consents to any such assignment, subletting or letting out as task work of all or any part of the Services, Contractor will in no way be relieved from its responsibility for the fulfillment of the Services, but will continue to be responsible for the same in the same manner as if all the Services had been performed by Contractor.

11.3 The Contractor cannot Transfer (as defined in Section 11.4) without the prior written consent of the City, which consent may not be unreasonably withheld but which may be withheld unless and until the City is provided all relevant and material corporate, trust and legal documentation relating to the Transfer and the Contractor agrees with the City in writing that despite the Transfer, the Contractor and any new entity assuming the Contractor's obligations under the Transfer will be jointly and severally liable for all of the obligations of the Contractor under this Agreement both before and after the Transfer.

11.4 For the purposes of Article 11.3, the following events constitute a Transfer:

(a) any amalgamation of Contractor with any other party;

(b) change of control of Contractor including any transfer, voluntary or involuntary, direct or indirect, which results any change in the person or persons exercising or who might exercise effective control or management of Contractor or the business required to be carried on by Contractor in and from Contractor's existing business premises and the Work Sites. However, change of control of Contractor does not include a change of non-shareholder or non-director management staff or other employees unless such changes are accompanied by a change in the directors, shareholders or anyone else exercising or who might exercise effective control or management of Contractor or Contractor's business. Contractor will on request (from time to time or at any time) promptly provide the City with all such corporate, trust and legal information and documentary evidence necessary to satisfy the City that Contractor is complying with Section 11.3;

(c) Any assignment of this Agreement in whole or in part including any subletting, franchising, licensing or parting with possession of all or part of Contractor's existing business premises or moving the location of Contractor's existing business premises directly or indirectly outside the Greater Vancouver Regional District.

City of Vancouver - FOI 2021-062 - Page 15 of 191

12.0 LAWS, PERMITS AND REGULATIONS

12.1 The laws of British Columbia will govern this Agreement and the parties irrevocably attorn to the exclusive jurisdiction of the courts of British Columbia.

12.2 All provisions of the International Sale of Goods Act are specifically excluded from application to this Agreement

12.3 In carrying out its obligations hereunder, Contractor will familiarize itself and comply with all applicable laws, bylaws, regulations, ordinances, codes, specifications and requirements of all regulatory authorities, and shall obtain all necessary licenses, permits and registrations as may be required by law.

13.0 WARRANTY, SERVICE LEVELS

13.1 The City's obligations to pay the Contract Price are subject to the System being fully operational and functional at least 99.9% of the time as measured on a 24 hour 7 day a week basis over each calendar month of the Term, but not including:

(a) downtime (as agreed upon between the City and Contractor, acting reasonably, in advance of and limited to the time allocated for and agreed to for same) for Contractor to install updates for making mutually agreed corrections; and

(b) downtime arising due to Unavoidable Delay, including for certainty but not limited to, interruptions in service by public utilities and third party telecommunications services providers but only to the extent that such service interruptions directly interrupt the System.

13.2 Service Levels

(a) The parties acknowledge that service level targets have been established with respect to the Services, Maintenance Services and Software and will be used to assess the performance of the Contractor in delivering the Requirements at an optimal service level for the City. The minimum service levels as well as the optimal service level targets are set forth in Schedule B [Service Level Agreement].

(b) Service Level Reports
The Contractor will prepare and deliver to the City a report, upon the City's request, on the Contractor's actual performance levels measured against the minimum service levels and optimal service level targets during the Term including the term of the Maintenance Agreement and the cost of preparing and delivering

City of Vancouver - FOI 2021-062 - Page 16 of 191

and responding to City enquiries on same will be deemed to be included in the Contract Price.

14.0 CONTRACTOR'S REPRESENTATIONS AND WARRANTIES

14.1 Contractor represents and warrants as follows:

(a) The System and the Requirements will be designed and carried out in accordance with good, generally accepted engineering and design practices and shall be maintained in good working order in accordance with the software maintenance procedures and Requirements contained in the RFP and the Proposal. Contractor will perform the Requirements with the degree of care, skill and diligence normally applied in the performance of services similar in nature and in accordance with sound current professional practices and conforming to the Requirements;

(b) Contractor represents and warrants that it either holds the entire right, title and interest in and to all intellectual property provided to the City under this Agreement, free and clear of claims and interest of any third party, or has the full right and power to license the intellectual property to the City as provided in this Agreement;

(c) Contractor will use its best efforts to ensure that any software licensed to the City under this Agreement does not contain any "viruses" which would materially adversely affect the City's ability to use the software;

(d) performance of the Requirements and the licence and use of any software to fulfil the Requirements, shall not infringe any patent, copyright, trademark. Industrial design or other intellectual property rights or liens of third parties;

(e) Contractor is the sole owner or authorized licensee of all intellectual property rights in and to the System, and the Contractor has the right to enter into this Agreement and to perform all of its obligations including delivery of any software and granting of any licences in relation to the Services and the System;

(f) the System does not contain any disabling or other device that would allow the Contractor or any third party to in any way reduce or interrupt the use and operation of the System by the City.

15.0 USING THE CITY AS A FUTURE ACCOUNT REFERENCE

15.1 Subject always to Section 30.1 [No Promotion of Relationship], and provided always that the prior written approval of the City Engineer has been obtained, the Contractor may:

(a) identify the City as a customer of Contractor and describe in a mutually agreeable customer case study the services and solutions delivered by Contractor to the City, and

(b) issue one or more press releases containing an announcement of the execution and delivery of this Agreement and/or the implementation of the payment by phone system by the City.

No such document or release shall include any of the City's Proprietary Information (as defined in Section 26). The City's approval to any such document or release may be unreasonably withheld or delayed.

16.0 INDEMNIFICATION

16.1 Contractor will indemnify, hold and save harmless the City from and against all claims, losses, damages, costs, actions and other proceedings made, sustained, brought or prosecuted in a manner based upon, occasioned by or attributable to any injury, including death, property damage, infringement or damage arising from any act or omission of Contractor, its employees, officers, volunteers, Sub-Contractors, or any other persons for whom Contractor has assumed responsibility in the performance or purported performance of the Requirements and Services.

16.2 Contractor will pay all royalties and license fees and will indemnify and save the City harmless from loss on account of suits or claims of infringement of patents in the performance of the Requirements and Services.

16.3 Contractor will assume the defence of, and indemnify and hold harmless the City and its officers, employees and agents, from and against all claims relating to materials furnished and to inventions, copyrights, trade marks, or patents and rights thereto used by Contractor in the execution of this Agreement and in subsequent use and/or operation by the City.

17.0 INSURANCE REQUIREMENTS

17.1 Without limiting any of its obligations or liabilities under this Agreement, Contractor and its Sub-Contractors will obtain and continuously carry during the term of the Contract at their own expense and cost, the following insurance coverage with minimum limits of not less than those shown in the respective items set out below.

17.2 All insurance policies will be in a form and in amounts satisfactory from time-to-time and with insurers acceptable to the City's Director of Risk and Emergency Management and will provide the City's Director of Risk and Emergency Management with sixty (60) days prior written notice of material change, lapse or cancellation. Notice must identify the Contract title, number, policyholder, and scope of work.

17.3 Contractor and each of its Sub-Contractors will provide at its own cost any additional insurance which it is required by law to provide or which it considers necessary.

17.4 Neither the providing of insurance by Contractor in accordance with the requirements hereof, nor the insolvency, bankruptcy or the failure of any insurance company to pay any claim accruing will be held to relieve Contractor from any other provisions of the Contract Documents with respect to liability of Contractor or otherwise.

17.5 The insurance coverage will be primary insurance as respects the City. Any insurance or self-insurance maintained by or on behalf of the City, its officers, officials, employees, or agents will be excess of this insurance and shall not contribute with it.

17.6 Prior to or on the date of execution of this Agreement, Contractor will provide the City with evidence of all required insurance to be taken out in the form of the Certificate of Insurance required by City supported by a certified copy(s) of the policy(s). The Certificate of Insurance will identify the Contract title, number, policyholder and scope of work and must not contain any disclaimer whatsoever. At all times thereafter, during the Term, Contractor must comply with all its insurance obligations described herein. Proof of insurance, in the form of a certificate of insurance or certified copies of all insurance policies will be made available to the City's Director of Risk and Emergency Management at any time during the Term upon request.

17.7 Contractor will provide in its agreements with its Sub-Contractors clauses in the same form as those found herein. Upon request, Contractor will deposit with the City's Director of Risk and Emergency Management detailed certificates of insurance for the policies it has obtained from its Sub-Contractors and a copy of the insurance clauses so provided in the said agreements.

17.8 Contractor will obtain and maintain in full force and effect during the Term, insurance not less than that set out below and provide proof of such insurance provided by a company duly registered and authorized to conduct insurance business in the Province of British Columbia.

(a) a Professional (Errors and Omissions) Liability insurance policy with limits of not less than two million dollars ($2,000,000) per occurrence with an aggregate of not less than five million dollars ($5,000,000) and a deductible of not more than fifty thousand dollars ($50,000), protecting the Contractor against all claims for loss or damage arising out of any error or omission of the Contractor or the Contractor's agents in the performance of the Services.

(b) Commercial General Liability insurance in sufficient amounts and description to protect Contractor, its Sub-Contractors, the City and its respective officers, officials, employees, and agents

against claims for damages, personal injury including death, bodily injury and property damage which may arise under this Contract

(c) The limit of commercial general liability insurance shall be not less than five million dollars (5,000,000) per occurrence inclusive for personal injury, death, bodily injury or property damage and in the aggregate with respect to products and complete operations. The deductible per occurrence shall not exceed five thousand dollars ($5,000) per occurrence

(d) The policy of commercial general liability insurance shall:

(i) be on an occurrence form;
(ii) add the City and its officials, officers, employees and agents as additional insureds;
(iii) contain a cross-liability or severability of interest clause
(iv) extend to cover non-owned automobile, contingent employer's liability, blanket contractual liability, contractor's protective liability, broad form property damage, broad form completed operations and operations of attached machinery.

17.9 Contractor will ensure that vehicles owned and/or operated by Contractor in connection with the Contract maintain Third Party Legal Liability Insurance in an amount not less than three million dollars ($3,000,000) per occurrence.

18.0 WORKERS' COMPENSATION

18.1 Prior to commencing any Services, Contractor must provide evidence that it is in good standing with the Workers' Compensation Board of British Columbia ("WCB"). Contractor is responsible for having the Work Site secured in accordance with WCB safety regulations and ensures that no danger shall befall the public at any time during the performance of the Work.

18.2 Contractor is now appointed and now accepts appointments as the Prime Contractor for the purpose of this Agreement and as such, has the responsibility to:

(a) ensure the Services are performed in a safe manner that complies with all the regulatory requirements

(b) direct and coordinate the work activities related to the health and safety of all Contractor's Sub-Contractors and any other workers in the Contractor's workplace and immediately give notice

(c) where performing Services on City premises, obtain from the City written information on hazards and conditions and the methods to address the hazards and conditions and will circulate

City of Vancouver - FOI 2021-062 - Page 20 of 191

this information.

18.3 Prior to starting any Services at the Work Site Contractor must:

(a) have its own safety program and have written safe work procedures specific to the work being performed available at the Work Site; and

(b) ensure the safety program meets the requirements of Part 3 of the Workers' Compensation Act and Part 3 of the WCB OHS Regulation

(c) advise the City of any accidents or incidents at the workplace that must be reported to the Workers' Compensation Board; and

18.4 Contractor shall:

(a) advise the City of any accidents or incidents at the workplace that must be reported to the Workers' Compensation Board; and

(b) inform all persons working under this Agreement on the workplace of the health and safety requirements at the workplace.

18.5 At all times Contractor will ensure that its workers and Sub-Contractors, and all other workers coming onto the workplace will comply with:

(a) the Workers' Compensation Act and the WCB OHS Regulation;
(b) Contractor's safety program; and
(c) all Work Site safety requirements.

19.0 SECURITY CLEARANCE FOR WORKERS

19.1 On the written request of the City, Contractor will remove any employee from further involvement with this Agreement, Sub-Contractor or agent for any reason including but not limited to the following:

(a) loss of or failure to obtain appropriate or required Security Clearance;
(b) intoxication;
(c) use of foul, profane, vulgar or obscene language or gestures;
(d) solicitation of gratuities or tips from any person for services performed under this Agreement;
(e) wilful, negligent or reckless action in disregard of safety or sanitary requirements or regulations; or
(f) any action which may constitute a public nuisance or disorderly conduct

19.2 Contractor shall promptly comply with each such request and shall satisfy the City that the employee, Sub-Contractor or agent has been removed from further involvement with this Agreement.

20.0 CITY'S RIGHT TO REMEDY

20.1 Should Contractor neglect to execute the Services or Requirements properly or fail to perform any provision of this Agreement, the City may, without prejudice to any other right or remedy it may have, make good such deficiencies and may deduct the cost thereof from the payment due to Contractor.

21.0 DISPUTE RESOLUTION

21.1 All claims, disputes or issues in dispute between the City and Contractor shall be decided by mediation or arbitration, if the parties agree, or failing agreement, in a court of competent jurisdiction within British Columbia.

21.2 In the event that (a) the parties agree to arbitration pursuant to the above, or (b) matter is referred to arbitration by City Engineer, pursuant to Article 10.0, the arbitration will conducted pursuant to the *Commercial Arbitration Act* (British Columbia) and will be governed by the rules of the British Columbia International Commercial Arbitration Centre, except that the arbitrator or arbitrators shall be agreed upon by the parties, and failing agreement by the parties, shall be appointed by a court of competent jurisdiction with the Province of British Columbia.

21.3 In the event that the parties agree to arbitration, the arbitration shall take place in within the City of Vancouver.

21.4 The procedure set out in this section is not meant to preclude or discourage informal resolution of disagreements between the City and Contractor.

22.0 TERMINATION

22.1 The City may, by written notice to Contractor, immediately cancel the whole or any part of this Agreement in any one of the following circumstances:

(a) Pursuant to Article 9.0;

(b) If Contractor fails to perform the Requirements or Services within the time specified, or fails to perform any other provisions, terms or conditions of the Contract within the time specified, or within a reasonable time if no time is specified;

(c) if Contractor performs any act or does anything by which the City shall incur any material financial liability whatsoever;

(d) if Contractor fails to meet the safety requirements of this Agreement;

(e) if any creditor of Contractor causes a writ of execution or similar writ or court order to be served upon the City requiring the City to pay any portion due to Contractor under this Agreement;

(f) if Contractor is adjudged bankrupt or if it makes a general assignment for the benefit of creditors or if it becomes insolvent or if it should take the benefit of any Act that may be in force for bankrupt or insolvent debtors; or

(g) if Contractor breaches any other term of this Agreement.

22.2 Upon cancellation of this Agreement, the City shall have no obligation to Contractor except for such Services as have been supplied up to the date of the cancellation of this Agreement.

23.0 SET-OFF

23.1 The City may at its option, withhold and set-off against any amount owing to Contractor (whether under this Agreement or otherwise) the amount of any damages suffered or claims made or to be made by the City as a result of any other claim it may have against Contractor for the breach of any covenant or warranty contained herein.

24.0 JOINT VENTURE OR PARTNERSHIP

24.1 If a joint venture or partnership, Contractor represents and warrants that all members of the joint venture or partnership are as indicated on the execution page of this Agreement and have duly executed same. The obligations and liabilities of each member of a joint venture or partnership executing this Agreement as Contractor shall be joint and several with all other members thereof.

25.0 LETTER OF CREDIT

25.1 On or before the Effective Date, Contractor will deliver to the City, a clean, unconditional irrevocable demand letter of credit payable in the amount of One Hundred and Fifty Thousand ($150,000) Dollars, (the "Letter of Credit") issued in favour of the City by a Schedule I Canadian chartered bank or Schedule II Canadian chartered bank and on terms satisfactory to the City's Director of Legal Services.

25.2 The Letter of Credit will be in an amount $150,000 for the first 12 months following the Effective Date. The Letter of Credit will have an expiry date no earlier than one year from its issuance and will state that it is deemed to be automatically renewed for further periods of at least 12 months unless prior to any given expiry date the issuing bank gives the City at least 60 days' prior written notice of its expiry or cancellation.

City of Vancouver - FOI 2021-062 - Page 23 of 191

25.3 On and after the one year anniversary of the Effective Date, the Letter of Credit will remain at in effect and at $150,000, unless and until either party, acting reasonably, requests an adjustment upwards or downwards in proportion to any substantial change in the estimated Transactions and resulting payments for any upcoming 12 month period. Where either party disputes the other party's request for a change, the Letter of Credit amount will stay the same unless and until subsequently varied by an arbitrator pursuant to Section 21.0 - Dispute Resolution.

25.4 The Letter of Credit is to be held by the City during the Term as partial security for the Contractor's due performance of the Requirements and Services and will be returned to the Contractor within 90 days following the expiry or sooner termination of the Term where no event entitling the City to draw down on the Letter of Credit has occurred or if it has occurred, then Contractor has remedied the event to the reasonable satisfaction of the City. The City may draw down on the Letter of Credit in part or whole in any of the following events:

(a) if, at any time Contractor does not make payments to the City in accordance with Section 3.12;

(b) if, at any time prior to it being returnable to the Contractor under this Agreement, the expiry date on the Letter of Credit is less than 30 days and a replacement letter of credit has not been issued;

(c) if Contractor makes a general assignment for the benefit of Creditors, or if Contractor institutes proceedings to have itself adjudicated as bankrupt or insolvent, including, without limitation, any application or order under the Companies Creditors Arrangement Act (Canada)(or any legislation in *pari material* therewith) or, if Contractor becomes the subject of bankruptcy or insolvency proceedings, or if a judgment, decree or order be entered by a court of competent jurisdiction judging Contractor bankrupt or insolvent, or if Contractor or its directors shall pass any resolution authorizing the dissolution or winding up of Contractor, or if a Receiver, interim Receiver, Manager, Receiver-Manager, trustee or liquidator of all or any part of Contractor's property shall be appointed or applied for by Contractor or by one of more of Contractor's creditors; or

(d) if at any time after notice and an opportunity to cure, as defined herein, Contractor continues to be in breach of any provision of this Agreement or defaults in carrying out any of its obligations under the terms of this Agreement to any extent the City Engineer considers to be material.

26.0 CONFIDENTIAL AND PROPRIETARY INFORMATION

26.1 Contractor's Confidential and Proprietary Information - Defined

"Proprietary Information" means, with respect to Contractor,

(a) data files and any benchmark or survey results,

(b) any and all information obtained by the City from Contractor or its affiliates through the course of carrying out this Agreement, including any compilations of otherwise public information,

(c) any and all information the disclosure of which is restricted by the *Personal Information Protection and Electronic Documents Act* (Canada), *Personal Information Protection Act* (British Columbia), *Freedom of Information and Protection of Privacy Act* (British Columbia) or any other legislation similar in intent and effect to the above, and

(d) and any other information reasonably identifiable in writing as the confidential or proprietary information of Contractor.

26.2 City's Confidential and Proprietary Information - Defined

"Proprietary Information" means, with respect to the City,

(a) all City owned or licensed software or proprietary information including, by way of example only, City-made modifications or extensions, and related documentation, source code and any complete or partial copies of them in any media, the concepts, techniques, ideas, know-how embodied and expressed in any computer programs or modules included in such software including the structure sequence and organization, and any benchmark or survey results,

(b) any and all information obtained by Contractor from the City or its affiliated organizations through the course of carrying out this Agreement, including any compilations of otherwise public information,

(c) any and all information the disclosure of which is restricted by the *Protection of Privacy and Freedom of Information Act (British Columbia)*, and

(d) any other information reasonably identifiable in writing as the confidential or proprietary information of the City.

26.3 Restrictions/Limitations on Obligations Respecting Proprietary Information

For further certainty, the obligations set out in Sections 26.1, 26.2 and 26.4 respecting Proprietary Information do not apply to any part of such information which:

(a) is or becomes publicly available through no act or failure of the recipient party, or

(b) was or is rightfully acquired by the recipient party from a source other than the disclosing party prior to receipt from the disclosing party, or

(c) becomes independently available to the recipient party as a matter of right (and such right is recorded in writing and is exercisable without any obligation of confidentiality), or

(d) is compelled to be disclosed pursuant to Canadian law, provided that if so compelled, the recipient party being ordered to disclose will only furnish that portion of the Proprietary Information that it is legally required to furnish.

26.4 Obligations of Recipient Party

(a) Contractor and the City now confirm and agree not to make use or permit any other party to make any use of the Proprietary Information except for the limited purposes necessary to carry out the intent of this Agreement. Prior to disclosing any Proprietary Information to any third party, the City and Contractor will obtain from that third party a written acknowledgment that the third party will be bound by Section 26 of this Agreement.

(b) The City and Contractor now agree to limit disclosure of the Proprietary Information to only those of its employees, officers, directors, or third parties, whose access in respect to the Proprietary Information. Contractor and the City will take all reasonable steps and the same protective precautions to protect the other's Proprietary Information from disclosure to third parties as it does with its own proprietary and confidential information provided that the standard of care utilized will not in any case be less than that which would be taken by a reasonable person to safeguard information of like commercial, personal, or public interest value.

26.5 Third Party Licences

For further certainty, Contractor now confirms to the City that Contractor has obtained all necessary contractual licenses and permits necessary from third party software licensors to ensure that the City will not be in breach of Contractor's Proprietary Information in the course of exercising the City's rights under this Agreement to receive the Services.

26.6 Ownership, Copyright, Custody and Control of Personal Information

(a) Contractor will safely store and then archive all of the City's and Contractor's Proprietary Information in respect to

(i) all personal information as defined by FOIPOP,

(ii) all data respecting the City and its customers and employees residing within any of Contractor's information system databases,

(iii) the services provided under prior contracts with the City, including without limitation the Current Contract,

(iv) the Services provided under this Agreement, and

(v) all sub-contractors referral information, status reports, reminder dates, follow up dates, and other data respecting any of the above,

(collectively, the "Contractor's City-Related Data") in the manner required by FOIPOP and without limitation and by way of example only the following requirements which apply to Contractor as an agent of the City:

(A) Only staff with a need-to-know may be provided access to the personal information,

(B) Security must be adequate to prevent unauthorized access. This includes proper encryption of information that is e-mailed to between the City and Contractor,

(C) Contractor must never access or store the personal information outside of Canada, except and then only where and to the extent expressly permitted by FOIPOP.

(b) Despite any other term of this Section 26.6, Contractor now agrees that, upon the expiry or sooner termination of this Agreement or any particular Service under this Agreement, Contractor will, upon the City's written request duly signed by the City Engineer transfer all or such requested portion of Contractor's City-Related Data to such third party Contractor or City employee as is named in the request by the City Engineer. Contractor and the City now agree that no fees or other amounts will be payable by the City or such third party for any transfer of Contractor's City-Related Data regardless of whether or not this Agreement is then in effect. Contractor further agrees to transfer Contractor's City-Related Data in the electronic format in which Contractor normally retains.

City of Vancouver - FOI 2021-062 - Page 27 of 191

(c) All reports and other documents or products produced and delivered by Contractor to the City as a result of the provision of the Services (the "Reports") and all of Contractor's City-Related Data will be the sole property of the City, and the City will have the right

(i) to utilize all of the Reports for its benefit in any way it sees fit without limitation, and

(ii) subject to compliance with all applicable laws and Section (b) above, to acquire custody of Contractor's City-Related Data and then utilize same for the benefit of the City and to the extent permitted by law and subject always to the confidentiality obligations respecting the personal information components of Contractor's City-Related Data, to utilize same in any other way it sees fit.

(d) Any and all Reports prepared but not yet delivered to the City will be delivered by Contractor to the City immediately on the expiration or sooner termination of this Agreement. The City may, at any time or times prior to the expiration or sooner termination of this Agreement, give written notice to Contractor requesting delivery by Contractor to the City of all or any particular Reports (whether completed or not) in which event Contractor will promptly comply with such request.

(e) Contractor now transfers title in and to Contractor's City-Related Data and the Reports and assigns to the City sole copyright in the Reports and Contractor's City-Related Data. Contractor agrees that title to Contractor's City-Related Data and the Reports is to be considered to have been transferred, and any copyright in Contractor's City-Related Data and the Reports is to be considered to have been assigned by Contractor to the City upon creation of Contractor's City-Related Data and the Reports. Contractor now irrevocably waives, in favour of the City, Contractor's moral rights in respect of Contractor's City-Related Data and the Reports. Contractor will obtain in writing, from its personnel, its permitted sub-Contractors or from any other source used, all required assignments, waivers, including waivers of moral rights, releases of interest and acknowledgements necessary to transfer title to and copyright in Contractor's City-Related Data and the Reports to the City.

(f) Contractor represents and warrants that Contractor's City-Related Data and the Reports will not infringe any patent or copyright or any other industrial or intellectual property rights including trade secrets.

27.0 TRADEMARKS, TRADE NAMES AND LOGOS

27.1 Except as expressly provided in this Agreement, no trademark, trade name, logo, trade dress, copyright or license therein, or other intellectual property rights (collectively, "Intellectual Property") are conveyed by this Agreement. Each party reserves the right to approve in advance the use of its Intellectual Property by the other party in each and every instance. All Intellectual Property owned by either party will remain the exclusive property of such party and will be returned to such party promptly after the expiration of this Agreement or destroyed, at the option of the other party. This section will survive the termination or expiration of this Agreement.

28.0 SOURCE CODE

28.1 Contractor will place such documents and software in escrow with the third party escrow agent as agreed to by the parties, such that in the event of termination by the City of this Agreement pursuant to Article 22.0, the City shall have a non-exclusive and non-transferable authorized licence to use for the remainder of the term of this Agreement (including any renewal term) without any fee the following property of Contractor which is reasonably required to operate the System in the manner and for the purposes contemplated by this Agreement:

(a) source code;

(b) test programs;

(c) program specifications;

(d) information about utilities and compilers; and

(e) instructions on generating the System

(collectively the "Source Code").

Any fees payable to the third party escrow agent for such escrow services will be born by Contractor and the City equally and the parties agree to enter in the form of escrow agreement with third party escrow agent.

Upon the occurrence of any of the events set out in this subsection, the City may exercise its rights under the Escrow Agreement and to take any steps reasonably necessary to obtain, possess and use the Source Code as may be permitted by the license set out above.

29.0 CITY'S RIGHT TO AUDIT AND INSPECT

29.1 The City reserves the right to examine, audit and take away copies of the books, records, documents and other data of Contractor at any time that relate to the System, Transactions, System Information, or the Services and Requirements. For greater certainty, without limiting the generality of the foregoing, the City's right hereunder shall include the right to examine books, records, bank account records, credit card records, documents and other data for the purpose of evaluating the accuracy, completeness and to verify parking meter revenue payments and transaction fees received from parking customers.

30.0 NO PROMOTION OF RELATIONSHIP

30.1 Despite any other term of this Agreement, including Section 3.5 [Joint Marketing],

(a) Contractor must not disclose or promote its relationship with the City, including by means of any verbal declarations or announcements and by means of any sales, web and mobile applications, marketing or other literature, letters, client lists, press releases, brochures or other written materials without the express written consent of the City (except as expressly required by the City and authorized by the City under the terms of this Agreement),

(b) Contractor undertakes not to use the "City of Vancouver" official emblem, logo or other marks or symbols or any reference or means of promotion or publicity, without the express written consent of the City,

(c) Contractor undertakes not to disclose or promote its relationship with the City in any communication or matter whatsoever as a basis to create an association, express or implied, between Contractor and the City except as expressly authorized and required by the City, and

(d) Contractor is prohibited from configuring, using, or permitting the System to be used in any way for any promotional or marketing purpose express or implied that is not first approved in writing by the City, which approval may be withheld by the City in its sole discretion.

31.0 MISCELLANEOUS

31.1 Mutual Representations and Warranties

Each party represents and warrants to the other that:

(a) it has the full corporate right and authority, and possesses all licences, permits, authorizations and rights to intellectual

property, necessary to enter into and perform this Agreement;

(b) its entry into and performance of this Agreement does not and will not conflict with or result in a breach or violation of any agreement or order by which it is bound and

(c) this Agreement constitutes its legal, valid and binding obligations enforceable against it in accordance with the terms of this Agreement.

31.2 Compliance with Laws

Contractor represents and warrants that in performing this Agreement, it will at all times comply with all applicable laws including, without limitation, laws governing the collection, protection, use and disclosure of personal information.

31.3 No Agency

Each party, in all matters relating to this Agreement, will act as an independent contractor and independent employers. Except as otherwise expressly set forth herein, neither party will have authority and will not represent that it has any authority to assume or create any obligation, express or implied, on behalf of the other, or to represent the other as an agent, employee or in any other capacity. Nothing in this Agreement will be construed to have established any agency, joint venture or partnership between the parties. Neither party will make any warranties or representations on behalf of the other party.

31.4 [Intentionally Deleted since already covered off above]

31.5 Severability

In the event that any provision of this Agreement will be unenforceable or invalid under any applicable law or be so held by applicable court decision, such unenforceability or invalidity will not render this Agreement unenforceable or invalid as a whole, and, in such event, such provision will be changed and interpreted so as to best accomplish the objectives of such unenforceable or invalid provision within the limits of applicable law or applicable court decisions.

31.6 Legal Fees

In any legal proceeding between the parties, the prevailing party will be entitled to recover reasonable legal fees and expenses if so awarded by a judge or arbitrator.

31.7 Entire Agreement

The Contract Documents constitute the entire agreement between the parties with respect to the subject matter hereof. This Agreement

City of Vancouver - FOI 2021-062 - Page 31 of 191

supersedes, and the terms of this Agreement govern any prior agreements with respect to the subject matter hereof. This Agreement may not be modified, amended or any provision waived except by the parties' mutual written agreement.

31.8 No Waiver

Failure by either party to enforce any provision of this Agreement (whether in any one or more instance) will not be deemed a waiver of future enforcement of that or any other provision.

31.9 Independent Contractor

Contractor, its Sub-Contractors, the officers, directors, shareholders, partners, personnel, affiliates and agents of Contractor and its Sub-Contractors are not, nor are they to be deemed to be, partners, appointees, employees or agents of the City.

31.10 Time of the Essence

For all obligations of Contractor pursuant to this Agreement, time is of the essence. The acceptance of a late performance, with or without objections or reservations by the City, will not waive the City's right to claim damages for such breach nor constitute a waiver of the requirement of timely performance of any obligation remaining to be performed.

31.11 Failure to Enforce

Any failure by the City to enforce or require the strict keeping and performance of any of the terms and conditions contained in the Agreement shall not constitute a waiver of such terms and conditions and will not affect or impair such terms and conditions in any way or the City's right at any time to avail itself of such remedies as the City may have for any breach or breaches of such terms and conditions.

31.12 Enurement

This Agreement will enure to the benefit of and be binding upon the parties hereto and their respective heirs, executors, administrators, successors and permitted assigns.

31.13 Notice

Any notices hereunder provided to any party will be given at the address specified on page 1 of this Agreement or at such other address as such party specifies in writing, and addressed to the attention of:

(a) for Contractor:

Buzz Hemphill, VP Sales, North America

Suite 1700, Park Place, 666 Burrard Street,
Vancouver, British Columbia
V6C 2X8
Telephone: (866) 783-7787 ext 112

(b) for the City:

Taryn Scollard, Manager, Parking Operations & Enforcement
#700 - 1125 Howe Street
Vancouver, B.C. V6Z 2K8
Telephone: (604) 257-8726

Any notice or other communication required to be given hereunder by either party will be deemed duly given (a) when personally delivered to the other party, or (b) on the date of receipt when such notice was mailed by certified mail, postage prepaid and return receipt requested, or by courier, addressed to the other party at the address set forth above, or such other address as either party may designate by giving written notice to the other; or (c) on the date of receipt when such notice was sent by facsimile or e-mail to the other party; provided the sending party receives a written or electronic notice of receipt from the other party of the facsimile or e-mail.

31.14 Counterparts

This Agreement may be executed in one or more counterparts, each of which will be deemed an original and all of which will be taken together and deemed to be one instrument.

31.15 Captions

The captions used in this Agreement are for convenience only and will not affect in any way the meaning or interpretation of the provision set forth herein.

31.16 Agreement Approval

Each party hereby represents and warrants that all necessary corporate and/or governmental approvals for this Agreement have been obtained, and the person whose signature appears below has the authority necessary to execute this Agreement on behalf of the party indicated.

31.17 Sophistication Parties

Each party to this Agreement represents that it is a sophisticated commercial party capable of understanding all of the terms of this Agreement, that it has had an opportunity to review this Agreement with its counsel, and that it enters this Agreement with full knowledge of the terms of the agreement.

IN WITNESS WHEREOF the parties hereto have executed and delivered this Agreement as of the day and year first above written.

CITY OF VANCOUVER

Date Oct 26, 2012

Authorized Signatory

Nick Kassam, Director Supply Chain, CPO

Print Name and Title

Date Oct 30, 2012

Authorized Signatory

Karyn Magnussun Director Dept Services Eng (Acting GM)

Print Name and Title

Date Oct. 30, 2012

Authorized Signatory

FRANCES J. CONNELL
Director of Legal Services

Print Name and Title

PAYBYPHONE TECHNOLOGIES INC.

Date 25 Oct 2012

Authorized Signatory

Margaret (Maggie) Clay VP Finance

Print Name and Title

SCHEDULE A - SERVICE CHARGES FOR PAYMENT BY PHONE

Items for Pricing	$ per transaction	Flat Fee ($)
Transaction Fee for Mobile Web & Smartphone App transactions	$0.135	N/A
Transaction Fee for IVR/Touchtone and SMS text transactions	$0.140	N/A
*Credit Card Processing Fee	$0.02 fixed component plus "at cost" component (currently estimated at 2.32% at most, but to be actually based during the Term on the actual rates charged by card type on each individual Transaction)	N/A

*Note: The fixed component of the Credit Card Processing Fee ($0.02) will be fixed for the Term. Despite Section 6.1 of this Agreement, the "at cost" component of the Credit Card Processing Fee will be charged to the City based on the actual cost without mark-up of any kind actually paid by the Contractor to the acquiring bank in respect of the Transactions where the Contractor acts as the merchant as opposed to the City and as such will likely vary during the Term based on the credit card types used by the customers of the System and the agreements entered into by the Contractor from time to time with the acquiring bank (currently Global Payment Inc.). The Contractor will at all times during the Term work cooperatively and promptly with the City to get quotes from prospective acquiring banks and to then enter into agreements with such acquiring banks as the City directs, either to utilize the Contractor as the merchant or, if the City so directs, to permit the City to act as the merchant so as to provide the City with the most cost-effective means of minimizing the "at cost" component of the Credit Card Processing Fee for Transactions. For certainty, the "at cost" component is not payable to the Contractor whenever and to the extent that the City is acting as the merchant with respect to any Transaction and therefore is paying the "at cost" amount to the acquiring bank in lieu of the Contractor.

SCHEDULE B - SERVICE LEVEL AGREEMENT

Performance & Service Expectations	
Incident	**Acceptable Response**
Account Maintenance - Update /Add Vehicle License Plate	3 minutes
Account Maintenance - Cancel & Suspend Account	3 minutes
Account Maintenance - Update Credit Card	3 minutes
Parking Payment Transaction via IVR (Interactive Voice Response)	3 minutes
Process a Parking Credit and or Refund	3 minutes
New Account signup on IVR (Interactive Voice Response)	5 minutes
Account Troubleshooting - Call Tracing and Transaction Query	10 minutes
Emergency Support Call Back	30 minutes
Incident	**Acceptable Resolution**
System Outage	3 hours
New or changed meter locations	1 day
Meter configuration changes (rates, time limits, etc)	1 day
General Technical Support or Assistance	3 days
Software bug fix (non critical)	5 days
Adding New Customer Service Agent Account	5 days
Simple Reporting Request	5 days
Software Escrow Deposit	5 days
IVR (Interactive Voice Response) Script Change	5 days
Web Site Update	5 days
Transfer Funds to City Account	refer to 3.12

City of Vancouver - FOI 2021-062 - Page 36 of 191

SCHEDULE C - CONTRACTOR'S PROPOSAL

This Schedule C - Proposal (submitted on March 26, at 3:00 pm) to RFP PS20120106 - THE SUPPLY OF PARKING METER PAYMENT BY PHONE SYSTEM becomes part of the Contract Documents, not attached but incorporated by reference.

City of Vancouver - FOI 2021-062 - Page 37 of 191

SCHEDULE D - REQUEST FOR PROPOSAL

This Schedule D - Request for Proposal RFP PS20120106 - THE SUPPLY OF PARKING METER PAYMENT BY PHONE SYSTEM exclusive PART D - FORM OF AGREEMENT becomes part of the Contract Documents, not attached but incorporated by reference.

City of Vancouver - FOI 2021-062 - Page 38 of 191

CITY OF VANCOUVER

GENERAL CERTIFICATE OF INSURANCE

Appendix A

Section 8 b) – City staff to select the required # of days Written Notice before sending the certificate out for completion
Section 2 through 8 – to be completed and executed by the Insurer or its Authorized Representative

1. **THIS CERTIFICATE IS ISSUED TO:** City of Vancouver, 453 W 12th Avenue, Vancouver, BC, V5Y 1V4
and certifies that the insurance policies as listed herein have been issued to the Named Insured(s) and are in full force and effect as of the effective date of the agreement described below.

2. **NAMED INSURED:** ***[must be the same name as the Permittee/Licensee or Party(ies) to Contract and is/are either an individual(s) or a legally incorporated company(ies)]***
PAY BY PHONE TECHNOLOGIES INC.
MAILING ADDRESS:
#201 - 1028 HAMILTON ST., VANCOUVER, BC V6B 2R9
LOCATION ADDRESS:

DESCRIPTION OF OPERATION, CONTRACT, AGREEMENT, LEASE, PERMIT OR LICENSE:

3. **PROPERTY INSURANCE** naming the City of Vancouver as a Named Insured and/or Loss Payee with respect to its interests and shall contain a waiver clause in favour of the City of Vancouver.

(All Risks Coverage including Earthquake and Flood)
INSURER:
TYPE OF COVERAGE:
POLICY NUMBER:
POLICY PERIOD: From ____ to ____

INSURED VALUES: (Replacement Cost)
Building and Tenants' Improvements: $
Contents and Equipment: $
Deductible Per Loss: $

4. **COMMERCIAL GENERAL LIABILITY INSURANCE** (Occurrence Form)
Including the following extensions:
√ **Personal Injury**
√ **Products and Completed Operations**
√ **Cross Liability or Severability of Interest**
√ **Employees as Additional Insureds**
√ **Blanket Contractual Liability**
√ ~~**Non-Owned Auto Liability**~~
INSURER: LLOYD'S THRU QBE CANADA SYNDICATES
POLICY NUMBER: B0801136990 12
POLICY PERIOD: From FEB 28, 12 to FEB 28, 13

LIMITS OF LIABILITY: (Bodily Injury and Property Damage Inclusive)
Per Occurrence: $ 10,000,000
Aggregate: $ 10,000,000 Pollution; Products
All Risk Tenants' Legal Liability: $ 10,000,000
Deductible Per Occurrence: $ 3,000

5. **AUTOMOBILE LIABILITY INSURANCE** for operation of ~~**owned and/or leased vehicles**~~ NON-OWNED
INSURER: ICBC
POLICY NUMBER: 5083108
POLICY PERIOD: From OCT 24, 12 to Sep 30, 13

LIMITS OF LIABILITY:
Combined Single Limit: $ 10,000,000
If vehicles are insured by ICBC, complete and provide Form APV-47.

6. ☐ **UMBRELLA OR** ☐ **EXCESS LIABILITY INSURANCE**
INSURER:
POLICY NUMBER:
POLICY PERIOD: From ____ to ____

LIMITS OF LIABILITY: (Bodily Injury and Property Damage Inclusive)
Per Occurrence: $
Aggregate: $
Self-Insured Retention: $

7. **OTHER INSURANCE** (e.g. Boiler & Machinery, Business Interruption, Crime, etc.) – **Please specify Name of Insurer(s), Policy Number, Policy Period, and Limit**

8. **POLICY PROVISIONS:**
Where required by the governing contract, agreement, lease, permit or license, it is understood and agreed that:
a) ***The City of Vancouver, its officials, officers, employees, servants and agents have been added as Additional Insureds with respect to liability arising out of the operation of the Named Insured pursuant to the governing contract, agreement, lease, permit or license;***
b) ***SIXTY (60) days written notice of cancellation or material change resulting in reduction of coverage with respect to any of the policies listed herein, either in part or in whole, will be given by the Insurer(s) to the Holder of this Certificate; the exception is cancellation for non-payment of premiums in which case the applicable statutory conditions will apply;***
c) ***The insurance policy (policies) listed herein shall be primary with respect to all claims arising out of the operation of the Named Insured. Any insurance or self-insurance maintained by the City of Vancouver shall be in excess of this insurance and shall not contribute to it.***

SIGNED BY THE INSURER OR ITS AUTHORIZED REPRESENTATIVE

Dated: OCT 25, 12

PRINT NAME OF INSURER OR ITS AUTHORIZED REPRESENTATIVE, ADDRESS AND PHONE NUMBER
Willis CANADA INC. 1500-609 W. Pender St. Vancouver, B.C. V6E 2M6

CITY OF VANCOUVER

PROFESSIONAL LIABILITY INSURANCE CERTIFICATE

Section 4 – City staff to select the required # of days Written Notice before sending out for completion
Section 2, 3 & 4– to be completed and executed by the Insurer or its Authorized Representative

1. **THIS CERTIFICATE IS ISSUED TO:** City of Vancouver, 453 W 12th Avenue, Vancouver, BC, V5Y 1V4
and certifies that the insurance policy as listed herein has been issued to the Named Insured(s) and is in full force and effect as of the effective date of the agreement described below.

2. **NAMED INSURED:** ***[must be the same name as the Permittee/Licensee or Party(ies) to Contract and is/are either an individual(s) or a legally incorporated company(ies)]***

Pay By Phone Technologies Inc.

MAILING ADDRESS:

#201- 1028 Hamilton St, Vancouver B.C. V6B 2R9

LOCATION ADDRESS:

DESCRIPTION OF OPERATION/CONTRACT:

3. **PROFESSIONAL LIABILITY INSURANCE**

INSURER: QBE (Europe) Ltd.
POLICY NUMBER: 30801112 75 P12
POLICY PERIOD: From FEB 28, 12 to FEB 27, 13

LIMITS OF LIABILITY:

Per occurrence/claim: $ 5,000,000
Aggregate: $ 5,000,000
Deductible per occurrence/claim: $ 100,000

If the policy is in a "CLAIMS MADE" form, please specify the applicable Retroactive Date: March 4, 2010

4. **POLICY PROVISIONS:**

Where required by the governing contract, agreement, permit or license, it is understood and agreed that SIXTY (60) days written notice of cancellation or material change resulting in reduction of coverage with respect to the policy listed herein, either in part or in whole, will be given by the Insurer to the Holder of this Certificate. The exception is cancellation for non-payment of premiums in which case the applicable statutory conditions will apply.

SIGNED BY THE INSURER OR ITS AUTHORIZED REPRESENTATIVE

Dated: OCT 25, 2012

PRINT NAME OF INSURER OR ITS AUTHORIZED REPRESENTATIVE, ADDRESS AND PHONE NUMBER

Willis Canada Inc. #1500- 1095 W. Pender St., Vancouver, BC (604)683-6831

CONFIRMATION OF VEHICLE INSURANCE COVERAGE

ICBC Insurance Corporation of British Columbia

(Hereinafter called the Corporation)

APV47

NAME OF INSURED (surname followed by given name(s))		
VERRUS MOBILE TECHNOLOGIES INC.		
ADDRESS OF INSURED 201-1028 HAMILTON ST		
CITY VANCOUVER	PROVINCE BC	POSTAL CODE V6B 2R9

This is to confirm to:

The City of Vancouver
453 W 12th Avenue
Vancouver, BC V5Y1V4

that coverage in accordance with the Insurance (Vehicle) Act (the Act), the Insurance (Vehicle) Regulation (the Regulation), and the ICBC Autoplan Optional Policy is provided as herein described to the insured named above and is in force at this date.

This confirmation is issued as a matter of information only and confers no rights on the confirmee and imposes no obligations on the Corporation, or the undersigned representative.

COVERAGE		VEHICLE PLATE NO.	LIMIT OF LIABILITY	DESCRIPTION OF VEHICLE			
				YEAR	MAKE	MODEL	SERIAL NUMBER
THIRD PARTY LIABILITY (REGULATION, PART 6) (OPTIONAL POLICY, DIVISION 4)	1.	210PA1	$ 3,000,000.00	NON. OWNED. AUTO LIABILITY. POLICY			
	2.		$				
	3.		$				
	4.		$				
	5.		$				
	6.		$				
	7.		$				
	8.		$				
	9.		$				
	10.		$				
	11.		$				
	12.		$				
	13.		$				

AGENT'S COMMENTS	AGENT'S NO.
CURRENT POLICY HAS HAD COVERAGE ENDORSED TO 3 MILLION. - AK	40306

The Motor Vehicle Liability Insurance Card Canada Inter-Province on the back of this Confirmation of Vehicle Insurance Coverage is not valid.

Coverage effective from:	Coverage to expire on:
DATE (ddmmyyyy)	DATE (ddmmyyyy)
22032012	28022013

NOT VALID UNLESS STAMPED BY AUTHORIZED ISSUING OFFICE

40306

DULY AUTHORIZED REPRESENTATIVE

March 23, 2012
DATE

AM 3 PM
TIME OF VALIDATION

MAR 23 2012

COPY 1 – CONFIRMEE | COPY 2 – ICBC-CORPORATE DISBURSEMENTS (no signatures required on Copies 2, 3 and 4) | COPY 3 – CUSTOMER | COPY 4 – AGENT

APV47 (062007)

MOBILE PARKING PAYMENT SERVICES AGREEMENT

THIS AGREEMENT (the "**Agreement**") made as of the 6th day of September, 2017 (the "**Effective Date**").

BETWEEN:

PAYBYPHONE TECHNOLOGIES INC.
#403 - 1168 Hamilton Street
Vancouver, British Columbia
V6B 2S2

(the "**Service Provider**")

AND:

CITY OF VANCOUVER
453 West 12th Avenue
Vancouver, British Columbia
V5Y 1V4

(the "**City**")

BACKGROUND:

A. Pursuant to Request for Proposals No. PS20160599 Provision of Mobile Parking Payment System: Mobile Application and Interactive Voice Response (the "**RFP**"), the City invited proposals from qualified proponents for the supply of a mobile parking payments system;

B. The City's preferred proponent is the Service Provider and the City wishes to engage the Service Provider to deliver the Services; and

C. The Service Provider has agreed to perform the Services in accordance with the terms and conditions of this Agreement.

NOW THEREFORE, in consideration of the mutual covenants and promises made by the parties and other good and valuable consideration, the receipt and sufficiency of which the parties hereby acknowledge, the parties agree as follows:

1.0 DEFINITIONS AND SCHEDULES

1.1 In this Agreement, including the Background section and all schedules, the following words and terms, unless the context otherwise requires, shall have the following meanings:

(a) "**Applicable Laws**" means all laws applicable to the parties under this Agreement and includes, without limitation, FOIPPA and PIPA;

(b) "**City**" means the City of Vancouver;

(c) "**Contract Price**" means the amounts set out in Schedule D to be paid by the City to the Service Provider for the Services;

(d) "**Consumers**" means the people who use the Service Provider's Solution to pay to park a specific vehicle in a parking space or zone administered by the City in the City of Vancouver;

(e) "**Derivative Works**" has the meaning given in Section 4.4;

(f) "**Documentation**" means user documentation provided electronically or in paper form by the Service Provider for use with the Software, as may be periodically updated and provided by the Service Provider;

(g) "**Effective Date**" means the date of this Agreement, which is stated on the first page of this Agreement;

(h) "**FOIPPA**" means the *Freedom of Information and Protection of Privacy Act* (British Columbia), as such Act may be amended or superseded;

(i) "**Mobile Application**" means the smartphone mobile application owned and operated by the Service Provider through which Consumers pay to park a specific vehicle in a parking space or zone administered by the City in the City of Vancouver during the Term;

(j) "**Parking Session**" means the total time a Consumer continuously pays for a specific vehicle to park in a specific metered parking space or zone. A Parking Session can consist of one or more of the following Consumer interactions:

- the initial payment at a metered parking space/zone;
- any extensions that a Consumer makes prior to the expiration of time purchased by the initial payment or a prior extension;
- if applicable, using a stop functionality to end a Parking Session; or
- any other functionality in the Solution that could modify an active Parking Session;

(k) "**personal information**" has the meaning given to it in FOIPPA and PIPA, as applicable;

(l) "**PIPA**" means the *Personal Information Protection Act* (British Columbia), as such Act may be amended or superseded;

(m) "**Requirements**" means all of the specifications, requirements, and services set out in Schedule A and the RFP (as modified or expanded by the Service Provider's Proposal or as further modified or expanded in this Agreement) that the Services provided by the Service Provider must meet;

(n) "**RFP**" has the meaning given to it in Recital A of this Agreement and is attached to this Agreement as Schedule E;

(o) "**Service Level Commitments**" means the service level commitments set out in Schedule I;

(p) "**Services**" means all of the obligations set out in this Agreement that are to be satisfied by the Service Provider including, without limitation, supplying and maintaining throughout the Term the Solution, the granting of a licence for the City to access and use the Software, ensuring the Services are performed in accordance with the Requirements (including, without limitation, Schedule A), complying with the Service Level Commitments, and all services and other requirements set out in Schedule E (RFP) and Schedule F (Service Provider's Proposal);

(q) "**Software**" means the software that the Service Provider uses to offer the Solution and perform the Services, which is developed, owned, and hosted by the Service Provider and that complies with the Requirements of this Agreement;

(r) "**Solution**" means the Service Provider's mobile parking payment services that are used by the Service Provider to perform the Services;

(s) "**Service Provider's Proposal**" means the Service Provider's proposal submitted in response to the RFP, a copy of which is attached to this Agreement as Schedule F;

(t) "**Term**" has the meaning given in section 6; and

(u) "**Transmitted Data**" means all data or information transmitted to and from the Service Provider as a result of this Agreement, or any other current or expired agreement between the Service Provider and the City, including all parking, monetary transaction, and other data emanating from Consumers' Parking Sessions in the City of Vancouver and all data obtained through the Software, which data includes, without limitation, personal information.

1.2 The following schedules are incorporated into and form an integral part of this Agreement:

(a) Schedule A - Scope of Work

(b) Schedule B - Additional Security and Privacy Requirements

(c) Schedule C - Certificates of Insurance

(d) Schedule D - Contract Price

(e) Schedule E - RFP

(f) Schedule F - Service Provider's Proposal

(g) Schedule G - PCI DSS 3.2 Management Responsibility Matrix Between the Service Provider and the City of Vancouver, and Letter of Attestation

(h) Schedule H - Change Order Request Forms

(i) Schedule I - Service Level Agreement

In the event of any conflict or inconsistency between any of the terms of this Agreement and any terms of a schedule, the terms of the body of the Agreement will govern and prevail. In the event of any conflict or inconsistency between any of the schedules, the schedules set out in the above order of priority will govern and prevail.

2.0 PERFORMANCE OF SERVICES, GRANT OF SOFTWARE LICENCE, AND AUTHORIZED USES

2.1 The Service Provider will perform the Services and its other obligations in accordance with the terms of this Agreement, the Requirements, and all Applicable Laws (including, without limitation, FOIPPA, PIPA, and all other applicable privacy and personal information laws).

2.2 The Service Provider hereby grants to the City and to those City employees designated by the City, subject to all of the terms and conditions of this Agreement, a non-exclusive, non-transferable licence to access the Software and any related documentation for the duration of the Term in accordance with the terms set out in this Agreement for use in accordance with the purposes set out in this Agreement. The City may access the Software in accordance with

the operating instructions provided to the City by the Service Provider. The parties acknowledge and agree that the Service Provider will not supply the City with any object code or source code underlying the Software.

2.3 Any instruction given by the City that constitutes or gives rise to a variation from the scope of the Services will constitute a "Variation" and will be governed by and subject to this Section 2.3. During the Term, the City may at any time effect a Variation by notice in writing to the Service Provider, and the Service Provider will not be entitled to refuse to implement any Variation unless doing so would contravene a law, in which case the Service Provider will give written notice to the City. If the Service Provider is of the view that the Variation justifies an increase to the Contract Price, the Service Provider must, as a condition to being entitled to any such increase to the Contract Price, no later than ten (10) business days after the City gives notice of the Variation, submit a written notice to the City setting out the Service Provider's proposed change to the Contract Price. The City may then accept the Service Provider's proposed change to the Contract Price and deliver written notice instructing the Service Provider to proceed with the Variation or reject the Service Provider's proposed change to the Contract Price and the Variation would not be implemented by the Service Provider.

2.4 The City and the Service Provider acknowledge and agree that the City will pay the Service Provider as is set out in Section 7.1 and Schedule D to this Agreement and subject to Section 7.3 and Schedules A and D to this Agreement.

3.0 ACCESS TO THE SOFTWARE BY THE CITY

3.1 The Software used to offer the Services is located and runs on servers and other equipment that are physically located in Canada, which includes any production or secondary or disaster recovery sites that the Service Provider may use to store and run the Software. Such servers and other equipment are owned and controlled by the Service Provider or are owned by a third party who has agreed to host the Software pursuant to a contract between the Service Provider and such third party. If the Software is hosted on third party-owned servers and equipment, the Service Provider has full control over such Software pursuant to the contract between the Service Provider and such third party.

3.2 As part of the Services, the Service Provider will do everything necessary to ensure that the Software is operational and permits the Service Provider to perform the Services at all times throughout the Term pursuant to the Requirements and Service Level Commitments.

3.3 The Service Provider will regularly upgrade and update the Software. The Service Provider will provide the City with as much prior notice as possible when an upgrade or update is to be implemented. The Service Provider will meet the availability and Service Level Commitments.

3.4 The Service Provider solely owns the intellectual property in the Software (except for third party components) and the Documentation. Nothing in this Agreement shall be construed as a transfer of ownership of the intellectual property in the Software or other proprietary rights or interests in the Solution or any other technology or property of the Service Provider, except the specific licence to access and use such Software provided in Section 2.2 of this Agreement.

3.5 The City and the Service Provider acknowledge and agree that each of their responsibilities as to each other and with respect to the PCI DSS 3.2 management aspects of the Services are set out in Schedule G to this Agreement.

3.6 Throughout the Term, the Service Provider will consult the City and receive the City's comments prior to implementing any changes to the Mobile Application that are not contemplated in Schedule A to the Agreement. If the City has not provided the Service Provider with its comments in respect of contemplated changes to the Mobile Application that are not contemplated in Schedule A to the Agreement within fourteen (14) days of the Service Provider

consulting the City, the Service Provider and the City acknowledge and agree that the Service Provider will have fulfilled its obligation under this Section 3.6 to consult the City and the Service Provider will not be required to consider and incorporate any comments from the City prior to implementing changes to the Mobile Application that are not contemplated in Schedule A to the Agreement. For clarity, the intent of this Section 3.6 is to ensure that the Consumer experience of using the Mobile Application is not negatively affected by changes made to the Mobile Application by the Service Provider that the City did not get a chance to provide feedback on. Therefore, the Service Provider and the City acknowledge and agree that this Section 3.6 does not apply to the routine updates, fixes, and patches that the Service Provider will undertake upon the Mobile Application throughout the Term. In the event that the Service Provider makes a change to the Mobile Application that is not contemplated in Schedule A to the Agreement and that it considers to be a routine change without consulting the City, but that the City considers that it should have been consulted on, the Service Provider agrees to subsequently consult and collaborate with the City to ensure that the City is comfortable with the change.

4.0 DATA, DATA SECURITY, AND PRIVACY

4.1 As between the City and the Service Provider, the Transmitted Data is owned by the City, and the Service Provider makes no claim to any right of ownership in the Transmitted Data. Subject to the terms and conditions of this Agreement, including Schedule B to this Agreement, the City hereby grants the Service Provider a perpetual, non-exclusive, non-transferable licence to use the Transmitted Data for the Service Provider's internal business purposes and as necessary to carry out its obligations under this Agreement, including service support, analytical review, general analysis, and to comply with the Service Provider's obligations under financial and payment card industry regulations. The Service Provider acknowledges and agrees that the Service Provider will not without the City's prior written consent share or transmit or send any Transmitted Data to any third party, including any related parties or parent or subsidiary companies, except as required to provide the Services, as long as the Service Provider complies with all Applicable Laws. The Service Provider will not use the Transmitted Data for any purpose other than for its internal business purposes or to carry out the Service Provider's obligations under this Agreement.

4.2 The Service Provider shall comply with all of the confidentiality, security, and privacy requirements set out in this Agreement (including, without limitation, the requirements of this section 4.0, the requirements set out in Schedule A (Scope of Work) and the requirements set out in Schedule B (Additional Security and Privacy Requirements)) with respect to the Transmitted Data. To the extent the Service Provider possesses any Transmitted Data in any form, medium, or device during or after the Term, the foregoing obligations shall survive and continue to be in legal effect.

4.3 Once the Transmitted Data is transferred through the Software to the Service Provider, the Transmitted Data will be stored on servers and other equipment that are physically located in Canada and that are controlled by the Service Provider. Physical access to the Service Provider's primary server is locked and restricted to only the Service Provider's employees. All data that flows in and out of the Service Provider's primary server is encrypted and otherwise protected against access by, or disclosure to, any third party. A regularly updated and backed-up copy of the Transmitted Data will be stored on servers and other equipment situated at facilities operated by the Service Provider. If the location of the Service Provider's primary and back-up servers and other equipment changes during the Term, the Service Provider shall immediately notify the City in writing. The Service Provider will not store the Software or Transmitted Data on any other server or equipment without the prior written approval of the City.

4.4 Except with the prior written approval of or instructions from the City, the Service Provider shall not modify, add, delete, destroy, share, match, mine, combine, manipulate, or otherwise

tamper with the Transmitted Data in any way. For clarity, the City acknowledges and agrees that the Service Provider may modify, mine, combine, manipulate, and tamper with copies of the Transmitted Data to create derivative works that contain no personal information (the "**Derivative Works**"), so long as in doing so the Service Provider complies with all Applicable Laws and all of the provisions of this Agreement.

4.5 The Service Provider shall send the Transmitted Data or provide access to the Transmitted Data to the City at all times throughout the Term. The Service Provider shall not withhold any of the Transmitted Data to enforce payment by the City or to enforce the Service Provider's rights in a dispute over this Agreement.

4.6 If the Service Provider is responsible for any loss or corruption of any Transmitted Data, the Service Provider will immediately restore or recreate such Transmitted Data and, if it is in default of such obligation, the Service Provider will be responsible for the City's reasonable costs and expenses to restore or recreate such lost or corrupt data.

4.7 The Service Provider will ensure that the data centre or data centres and servers containing the Transmitted Data meets the following physical and electronic security requirements:

(a) single point of entry;

(b) main access monitored with additional access for emergency purposes only;

(c) surveillance cameras in physical data centre facility/room;

(d) access validation with identity check;

(e) access only to persons on the Service Provider's approved access list;

(f) log-in validation;

(g) creation of accounts only as verified by the Service Provider;

(h) access to servers via encrypted means; and

(i) servers running behind secure firewall.

4.8 The Service Provider shall ensure that its employees are aware of their obligations regarding data security and privacy under this Section 4.0, Schedule A, and Schedule B of this Agreement.

4.9 The Service Provider shall comply with all of the confidentiality, security, and privacy requirements set out in the agreements the Service Provider enters into with each Consumer. Without limiting the generality of the foregoing, the Service Provider shall protect each Consumer's payment or credit card information and not share such information with any third parties.

4.10 The City will not sell or share the Transmitted Data with any third parties, except as described in Section 7B. For clarity, the Service Provider acknowledges and agrees that the City may share with third parties Derivative Works created by the City or standard Derivative Works created by the Service Provider and provided to the City as part of the Services.

5.0 WARRANTIES

5.1 **Software Warranties:** The Service Provider warrants that:

(a) the Software will satisfy the Requirements;

(b) the Software will be designed and built in accordance with good, generally accepted engineering and design practices and maintained in good working order in accordance with the Requirements;

(c) the Service Provider will ensure the Requirements are satisfied with the degree of care, skill, and diligence normally applied in the performance of services similar in nature and in accordance with sound current professional practices;

(d) the Service Provider owns or otherwise has the right to license the Software to the City and to perform all of the Service Provider's other obligations under this Agreement.

5.2 **Corporate and Other Warranties:** The Service Provider and the City each warrant that, as of the Effective Date, each of the Service Provider and the City:

(a) has full right, power, and authority to enter into this Agreement and to perform its obligations under it;

(b) is not under any obligation, contractual or otherwise, to request or obtain the consent of any person in order to enter into this Agreement and to perform the Service Provider's obligations under it;

(c) is a duly organized and legally existing corporation in good standing and has not been dissolved under the laws of the Province of British Columbia and is lawfully registered and licenced to do business in the Province of British Columbia;

(d) has the necessary corporate power to own its properties and assets and to carry on its business as it is now being conducted and to enter into this Agreement;

(e) is not a party to or bound by any indenture, agreement (written or oral), instrument, licence, permit, understanding, or other obligation or restriction under the terms of which the execution, delivery, or performance of this Agreement will constitute or result in a violation or breach or default; and

(f) all other representations and warranties made by it in this Agreement are true and accurate.

5.3 If a part of the Services does not satisfy the Requirements, the Service Provider will within the time periods specified in the Service Level Commitment, at its option, either:

(a) modify the deficient part of the Services to conform to the Requirements; or

(b) provide a workaround solution to the City's satisfaction that will meet the Requirements.

If the Service Provider does not satisfy its obligations under either Section 5.3(a) or 5.3(b) within seven (7) days or the time period agreed upon by the City and the Service Provider, the City may terminate this Agreement, in which case the Service Provider shall refund to the City all amounts owed by the City to the Service Provider or paid by the City to the Service Provider under this Agreement for the time period in which a part of the Services did not satisfy the Requirements, and the City will have no further obligation or liability to the Service Provider. The City may waive its right to terminate this Agreement under this Section 5.3.

5.4 If the normal operation, possession, access, or use of the Software by the City is found to infringe any third party intellectual property right or the Service Provider believes that this is likely, the Service Provider must immediately, at its option, either:

(a) obtain a licence from such third party for the benefit of the City to allow the City to access and use the Software in accordance with the terms of this Agreement; or

(b) modify the Software so that it no longer infringes.

If neither of these options is reasonably satisfactory to the City, the City may terminate this Agreement, in which case the parties shall pay the other party all amounts owed until the date of termination of this Agreement and upon such payment neither party will have further obligation or liability to the other, provided, however that the Parties acknowledge and agree that all indemnification obligations of the Parties and all other sections of this Agreement that survive expiry or termination of the Agreement shall survive the termination of this Agreement to the extent of any claim or cause of action based on an event occurring prior to the date of termination of this Agreement.

6.0 TERM OF AGREEMENT

Subject to earlier termination in accordance with the terms of this Agreement, the term of this Agreement will commence on the Effective Date and expire on the fifth anniversary of the Effective Date (the "**Initial Term**"). Notwithstanding the foregoing, the City may, but is not required to, renew this Agreement on the same terms and conditions for five additional one (1) year periods (each a "**Renewal Term**", and, collectively, the Initial Term and each Renewal Term shall be called the "**Term**") by giving the Service Provider written notice of renewal no later than ninety (90) days prior to the expiry of the then-current Term. If, upon the conclusion of the fifth additional Renewal Term, the Service Provider and the City continue to deal with each other as though this Agreement has not expired, this Agreement will continue to be in force on a month-to-month basis terminable on thirty (30) days' prior written notice by either party.

7.0 CONTRACT PRICE

7.1 Subject to Schedule A, Schedule D, and Section 7.3, in consideration for the Services and other obligations to be performed by the Service Provider under this Agreement, the City will pay the Service Provider the Contract Price.

7.2 The Service Provider's obligations under this Agreement have been set out following consultations between the parties. If the Service Provider's obligations under this Agreement fail to expressly state anything that would reasonably be implied or inferred in order for the City to achieve the benefits intended to be obtained under this Agreement, the Service Provider now agrees that such thing will be deemed to be implied and included in the Agreement and the Contract Price.

7.3 The City's obligations to pay the Contract Price are subject to the Solution being operational and functional as per Schedule I - Service Level Agreement as measured on a 24 hour 7 day a week basis over each calendar month of the Term, but not including downtime (as agreed upon between the City and the Service Provider, acting reasonably, in advance of and limited to the time allocated for and agreed to for same) for the Service Provider to install updates for making mutually agreed corrections.

7.4 As part of the Services, the Service Provider will act as the "Merchant of Record" for all transactions in which Consumers use the Mobile Application to pay to park a specific vehicle in a parking space or zone administered by the City in the City of Vancouver during the Term. The Service Provider and the City acknowledge and agree that the Service Provider will own the "Merchant Account" with Global Payments or any other payment processing services providers that the Service Provider uses to perform the Services during the Term. The Service Provider

will be responsible for all risks associated with being the "Merchant of Record". At all times during the Term, the Service Provider will charge the City the lowest "Acquirer Processing Fee" available to the Service Provider for all financial transactions that take place as a result of this Agreement and will not in any way mark up the "Acquirer Processing Fee" that the Service Provider charges to the City. If the Service Provider negotiates a lower "Acquirer Processing Fee" during the Term, the Service Provider will concomitantly decrease the "Acquirer Processing Fee" the Service Provider charges to the City. If requested by the City, the Service Provider will immediately deliver to the City a copy of the Service Provider's Merchant Account agreement and related amendments governing its "Acquirer Processing Fee".

7.5 The Service Provider will use a sub-account coding system to separate all cash inflows, including applicable taxes, for Consumer payments from all non-Consumer payments and will immediately upon receiving Consumer payments deposit those Consumer payments directly into a City-owned bank account. Pursuant to the obligations set out in the "Detailed Functional Requirements" in Part 2 of Schedule A of this Agreement, the Service Provider is responsible for the regular monitoring and reconciliation relating to the sub-account coding system to ensure the accuracy and timeliness of cash inflows from Global Payments, or any other payment processing services providers, during the Term. In the event of any variance in the amounts flowing into and out of the sub-account coding system, the Service Provider will notify the City within 24 hours of the discovery of such occurrence and will investigate and resolve any variance as per the restoration times stipulated for "General Support" issues in Schedule I - Service Level Commitments. The Service Provider will ensure that its bank will not be able to change the bank account to which the aforementioned payments are to be made without the City's written consent and the Service Provider will not change the bank account to which the aforementioned payments are to be made without the City's written consent. On the first business day of each month during the Term and pursuant to Schedule D, the Service Provider will invoice the City for the fees that the City owes to the Service Provider and for the gateway fees and credit card processing fees applicable to the Consumers' parking transactions for the previous month. The City will pay the Service Provider within thirty (30) calendar days of receiving each such invoice. Along with each invoice that the Service Providers delivers to the City, the Service Provider will deliver detailed fee reports and supporting documents to the City. Within seven (7) days of the Effective Date, the Service Provider will provide the City with online access to the Service Provider's bank account remittance reports, gateway provider's reports, and credit card processor's reports. The City will be responsible for remitting all applicable taxes imposed on the Consumers' parking transactions to the relevant authorities. Within fifteen (15) days of the Effective Date, the City will deliver a deposit of $50,000 to the Service Provider as an advance against the fees that the City will be paying the Service Provider during the Term. Within seven (7) days of the expiry or termination of this Agreement, the Service Provider will return the $50,000 deposit to the City.

7.6 The Service Provider will pay for and deliver to the City on or prior to the Effective Date a performance bond in favour of the City in the amount of $1,000,000 that will include provision for the coverage of the performance of all terms and conditions of this Agreement. The Service Provider acknowledges and agrees that the performance bond will be issued by a duly licenced surety company authorized to transact the business of suretyship in British Columbia and the Service Provider will ensure that the performance bond will be maintained in good standing throughout the Term. The Service Provider acknowledges and agrees that the City may make a formal, written claim under the performance bond with the aforementioned surety company declaring that the Service Provider is in default of this Agreement's terms and conditions if the Service Provider has not performed the Services and its other obligations in accordance with the terms of this Agreement, the Requirements, and all Applicable Laws at any time during each of three successive days during the Term without curing said default within the time specified by the Service Level Commitments. If the City engages an Additional Proponent (defined below) to deliver the Services or any part of the Services concurrently with the Service Provider during the Initial Term, then the City will return the aforementioned

performance bond to the Service Provider within thirty (30) days of engaging the Additional Proponent.

7B Multi-Vendor Considerations

7B.1 Limit on Number of Additional Proponents. The City will engage no more than one (1) entity other than the Service Provider (the "**Additional Proponent**") to deliver the Services or any part of the Services concurrently with the Service Provider during the Initial Term but not any renewal periods of the Term, such that the total number of proponents delivering the Services to the City at any one time during the initial five (5) years of the Term shall be limited to two (2), which includes the Service Provider. The City and the Service Provider acknowledge and agree that the City is free to contract with an entity that provides any additional services that are not included in the Services, including but not limited to services that assist with internal City fleet management. The City acknowledges and agrees that if any of the additional services are parking related services, and/or adjacent solutions (for example: fine payment, permits, and/or other services related to *smart parking)*, the Service Provider will have the opportunity to propose a bid to the City to add the additional service to the Services provided by the Service Provider, as an addendum to this Agreement.

7B.2 Notice. If the Service Provider has not breached the Agreement and the City enters into a services agreement with an Additional Proponent at any point during the first year of the Term for the Additional Proponent to perform the Services or any part of the Services, the City will provide notice to the Service Provider no less than one (1) year prior to allowing that Additional Proponent to perform the Services or any part of the Services. If the Service Provider has not breached the Agreement and the City enters into a services agreement with an Additional Proponent at any point during the Term after the first anniversary of the Effective Date for the Additional Proponent to perform the Services or any part of the Services, the City will provide notice to the Service Provider no less than six (6) months prior to allowing that Additional Proponent to perform the Services or any part of the Services.

7B.3 Feature Parity. If the City enters into an agreement with an Additional Proponent to perform the Services or any part of the Services concurrently with the Service Provider during the Term and the City requests feature parity between the Service Provider's and the Additional Proponent's Services offerings but the requested features are not features provided by the Service Provider as part of the Services, the Service Provider will only be required to provide the City with the requested features if the Service Provider and the City agree on a price for the creation, deployment, and maintenance of such features. If the City enters into an agreement with an Additional Proponent to perform the Services or any part of the Services concurrently with the Service Provider during the Term, the City requests feature parity between the Service Provider's and the Additional Proponent's Services offerings, and the requested features are offered by the Service Provider but not by the Additional Proponent, the City acknowledges and agrees that the Service Provider will have no obligation to assist the Additional Proponent with developing such features.

7B.4 Signage Cost. The City and the Service Provider acknowledge and agree that the mobile parking payments signage in Vancouver will need to be updated if the City contracts with an Additional Proponent to perform the Services or some part of the Services concurrently with the Service Provider. The City will have sole discretion as to the content of the updated mobile parking payments signage, including sole discretion as to the allocation of space for content that is provided to the Service Provider and the Additional Proponent on the updated mobile parking payments signage. Notwithstanding the foregoing, the City agrees to allocate the space on the signage in such a way that is fairly and evenly representative of both the Service Provider and the Additional Proponent. The City and the Service Provider acknowledge and agree that costs associated with any updates to the mobile parking payments signage will be borne as follows:

a. *Parking Meter Decals.*

i. If the Additional Proponent is added in line with the schedule of signage updating established in Schedule A - Requirement 1.15, all material and labour costs related to the updating of the meters will be split 50-50 between the Service Provider and the Additional Proponent and Schedule A - Requirement 1.15 shall continue as outlined; and

ii. If the Additional Proponent commences its services on a date that is between the scheduled signage update intervals established in Schedule A - Requirement 1.15, the City acknowledges and agrees that the Service Provider will not be responsible for any material or labour costs related to the initial updating of the meters and Schedule A - Requirement 1.15 shall be amended by the City, with the total number of signage updates no greater than that which was originally agreed to in Schedule A - Requirement 1.15. After the initial update of the signage at the Additional Proponent's expense, all costs related to further updating of signage in accordance with Schedule A - Requirement 1.15, will be split 50-50 between the Service Provider and the Additional Proponent.

b. *Stand-Alone Signage.*

i. If the City and Additional Proponent wish to include the Additional Proponent on stand-alone signage that had already been erected and paid for by the Service Provider, the City will ensure that the Service Provider is reimbursed no less than 50% of the cost borne by the Service Provider to erect the sign; and

ii. If the City and Additional Proponent wish to add additional stand-alone signage, any such costs shall be split 50-50 between the Service Provider and the Additional Proponent.

c. *In-Fill Signage for New Inventory.*

If the City decides to add additional parking spaces in the city that require new signage and the City has engaged the Additional Proponent, any such costs shall be split 50-50 between the Service Provider and the Additional Proponent.

7B.5 User Base. If the City enters into an agreement with an Additional Proponent to perform the Services or any part of the Services concurrently with the Service Provider during the Term, to the extent possible to provide the Services under this Agreement, the City will cause the Additional Proponent to maintain and manage a database of its users transmitted data separate from the Service Provider's database of users of the Transmitted Data. In circumstances where the City requires the Service Provider and the Additional Proponent to share information about Service Provider's users' transactions in order for both parties to offer the Services or some part of the Services, including but not limited to integration for re-metering prevention, financial reconciliation process, and enforcement integration, the Service Provider will grant a non-exclusive, revocable, royalty-free, non-transferable licence to the Additional Proponent to use the specific data required to fulfill specific Services and the City will require the Additional Proponent to grant a non-exclusive, revocable, royalty-free, non-transferable, licence to the Service Provider to use the specific data required to fulfill specific Services.

7B.6 Access to Inventory of Parking Spaces. If the City enters into an agreement with an Additional Proponent to perform the Services or any part of the Services concurrently with the Service

Provider during the Term, the City will ensure that each of the Service Provider and the Additional Proponent has access to the inventory of parking spaces that exist in Vancouver as of the Effective Date that offer the mobile payment option, such that a customer may pay for parking at any of those spaces using the services of either the Service Provider or the Additional Proponent. If after the Effective Date and during the Term the City creates additional inventory of parking spaces that offer the mobile payment option (the "**New Spaces**"), the City agrees to allocate the same access to New Spaces to both the Service Provider and the Additional Proponent subject to the following: If access to all or a portion of the inventory of New Spaces is dependent on specific mobile parking payment features or functionality, then access to those parking spaces may be made available, at the City's sole discretion, only to the entity with whom the City has contracted to provide those features or functionality. In order for the City to ensure that each of the Service Provider and the Additional Proponent has access to the inventory of parking spaces including the New Spaces, the City acknowledges and agrees that the Service Provider will have the opportunity to propose to add the specific mobile parking payment feature or functionality related to the New Spaces to the Services provided by the Service Provider. The City is under no obligation to contract with any entity for mobile parking payment features or functionality.

8.0 TERMINATION

8.1 The City may terminate this Agreement by providing written notice to the Service Provider (a) if the Service Provider is in breach of any term of this Agreement and the breach is not cured within five (5) days of written notice of that breach by the City, and (b) immediately if the Service Provider becomes insolvent, bankrupt, or is otherwise unable to carry on business. The City may waive its right to terminate this Agreement as provided under this Section 8.1. For clarity, the main purpose of this Section 8.1 is that the Service Provider will in the event of a breach by the Service Provider be allowed to continue to try to remedy said breach without risk of termination of the Agreement by the City so long as the breach does not impact the Consumer's ability to use the Solution to pay to park a specific vehicle in a parking space or zone administered by the City in the City of Vancouver or the ability of the City to collect the fees associated with those Transactions.

8.2 At any time during the Term after the third (3^{rd}) anniversary of the Effective Date, the City may terminate this Agreement for convenience by providing the Service Provider with ninety (90) days' written notice pursuant to section 15.

9.0 THE SERVICE PROVIDER'S OBLIGATIONS AFTER AGREEMENT TERM EXPIRES

9.1 **City's Request to Delete and Destroy Transmitted Data:** At the City's request, the Service Provider will immediately, permanently, and securely delete and destroy all Transmitted Data in its possession or under its control and all records thereof (in all media and devices in or on which such Transmitted Data is stored) in a manner that is appropriate for the media or device so that the Transmitted Data or any portion of it cannot be subsequently retrieved, accessed, or used by the Service Provider or any other person, unless the Service Provider is required to keep the Transmitted Data to comply with Applicable Laws. Without limiting the scope of Transmitted Data to be deleted and destroyed by the Service Provider, the Service Provider will delete and destroy the following:

(a) all Transmitted Data in the Service Provider's possession or under its control including, without limitation, Transmitted Data stored on any media or device;

(b) all work files and copies of the Transmitted Data; and

(c) all hard copies and electronic copies of reports in the Service Provider's possession or under its control.

Notwithstanding the foregoing, the City may ask the Service Provider to not delete or destroy certain Transmitted Data and the Service Provider shall comply with such request provided it does not conflict with the Service Provider's obligations under Applicable Laws.

9.2 **Obligation to Provide City a Copy of Transmitted Data before Destruction:** Prior to the deletion and destruction of the Transmitted Data in accordance with section 9.1, the Service Provider will provide the City with one or more copies of all of the Transmitted Data (in a format, medium, and/or device instructed by the City) in the Service Provider's possession or under its control at such time.

9.3 **Declaration in Writing:** After complying with sections 9.1 and 9.2, the Service Provider shall deliver a declaration in writing (in form and substance satisfactory to the City) to the City evidencing its compliance with those sections.

9.4 **Continued Safe and Secure Storage:** Until the City makes the request in section 9.1 to delete and destroy the Transmitted Data, the Service Provider will continue to safely and securely store the Transmitted Data in accordance with the terms of this Agreement.

10.0 INSURANCE

10.1 **Required Insurance/Amounts.** Prior to commencing the Services, the Service Provider will obtain:

(a) a Professional (Error and Omissions) Liability insurance policy with limits of not less than $2,000,000 per claim and an aggregate of not less than $2,000,000, protecting the Service Provider against all claims for loss or damage arising out of any error or omission of the Service Provider or the Service Provider's directors, officers, employees, and agents (the "**Service Provider's Personnel**") in the performance of the Services; and

(b) a Commercial General Liability insurance policy with limits of not less than $5,000,000 per occurrence, aggregate of not less than $5,000,000, and a deductible of not more than $25,000, protecting the Service Provider and the Service Provider's Personnel against all claims for personal injury, including death and bodily injury, and property damage or loss arising out of the operations of the Service Provider or the actions of the Service Provider or the Service Provider's Personnel. The policy will contain a cross liability clause in favour of the City and will name the City and the City's officers, officials, employees, and agents (the "**City Personnel**") as additional insureds.

10.2 **Required Policy Terms.** All required insurance policies listed in section 10.1 will remain in full force and effect at all times until completion of the Services or earlier cancellation of this Agreement, and will:

(a) be obtained from and issued by insurers authorized to carry on business within British Columbia, on terms satisfactory to the City's Director of Risk Management, acting reasonably;

(b) be primary insurance in respect to the City and any insurance or self-insurance maintained by the City will be in excess of this insurance and will not contribute to such policies; and

(c) contain a provision that such insurance will not be cancelled without the insurer giving the City at least thirty (30) days' prior written notice.

10.3 **Insurance Certificate.** Prior to or on the Effective Date, the Service Provider will provide the City's Project Manager with evidence of all required insurance to be taken out in the form of

one or more Certificates of Insurance in form and substance satisfactory to the City. The Certificates of Insurance will identify the Agreement title, number, policyholder, and scope of work and must not contain any qualifications or disclaimers. Proof of insurance, in the form of such Certificates of Insurance (or copies of the policies themselves, if requested), will be made available to the City's contract administrator at any time during the performance of the Services immediately upon request. The Certificates of Insurance will be attached as Schedule C to this Agreement.

10.4 **Additional Requirements.** The Service Provider will provide, at its own cost, any additional insurance which is required by law to provide or which it considers necessary.

10.5 **Insurance Requirements Independent of Additional Obligations.** Neither the providing of insurance by the Service Provider in accordance with this Agreement nor the insolvency, bankruptcy, or the failure of any insurance company to pay any claim accruing will be held to relieve the Service Provider from any other provisions of this Agreement with respect to liability of the Service Provider or otherwise.

11.0 RELEASE AND INDEMNIFICATION

11.1 The Service Provider now releases the City, the City Personnel and their respective successors, assigns, heirs, and authorized representatives from all costs, losses, damages, and expenses, including those caused by personal injury, death, property damage, loss, and economic loss arising out of, suffered, or experienced by the Service Provider and the Service Provider's Personnel in connection with the Service Provider's performance of the Services under this Agreement. Notwithstanding the foregoing, the Service Provider does not release the City from the City's obligation to pay the Contract Price pursuant to section 7 of this Agreement.

11.2 The Service Provider hereby agrees to indemnify and save harmless the City and the City Personnel and their respective successors, assigns, heirs, and authorized representatives and each of them (in each case an "**Indemnified Party**") from and against all costs, losses, claims, damages, actions, and causes of actions (collectively referred to as "**Claims**") that an Indemnified Party may sustain, incur, suffer, or be put to at any time either before or after the expiration or termination of this Agreement that arise out of the negligent performance by the Service Provider of this Agreement, a breach by the Service Provider of this Agreement (including, but not limited to, a breach of any of the confidentiality, security, and privacy provisions of this Agreement), an infringement claim against the City, or errors, omissions, or negligent acts of the Service Provider or its officers, employees, or agents under this Agreement, excepting always that this indemnity does not apply to the extent, if any, to which the Claims are caused by errors, omissions, or negligent acts of an Indemnified Party.

11.3 The indemnity outlined in clause 11.2 will not affect or prejudice the City from exercising any other rights that may be available to it at law or in equity.

11.4 The release and indemnity set out above will survive the expiry or early termination of this Agreement.

11.5 The City and the Service Provider acknowledge and agree that the Service Provider's failure to properly perform the Services will cause the City to incur economic damages and losses of types and in amounts that are impossible to compute and ascertain with certainty as a basis for recovery by the City of actual damages and that liquidated damages represent a genuine estimate thereof. Accordingly, the Service Provider will pay the City liquidated damages pursuant to Schedule I to this Agreement in the circumstances stated in Schedule I to this Agreement.

12.0 CONFIDENTIALITY

12.1 The confidentiality obligations set out in this Section 12.0 are in addition to the parties' obligations to comply with FOIPPA, PIPA, all other applicable privacy and personal information laws, and the other security and privacy obligations set out in this Agreement.

12.2 In the course of or for the purpose of performing the services contemplated in this Agreement, both parties will obtain or have access to information, including but not limited to the Transmitted Data, other personal information, and possibly financial and business information that is confidential to the other party (collectively "**Confidential Information**"). Confidential Information includes all information, in whatever form, other than:

(a) information that is in, or becomes part of, the public domain, not due to either party's breach of this Agreement or actions;

(b) information that was previously in a party's possession and did not originate from the other party; and

(a) information that lawfully becomes available to a party from a third party not under an obligation of confidence to the other party regarding such information.

12.3 A party receiving the other party's Confidential Information will not use or reproduce the Confidential Information other than as reasonably required for the performance of obligations under this Agreement. Neither party will, without the prior written consent of the other party given on such terms and conditions as it prescribes in its sole discretion, disclose or allow access to the Confidential Information to any person, except to only those of its own employees, or in the case of the City officials or agents, who have a need to know the Confidential Information solely for the fulfillment of obligations under this Agreement, and who have been advised of its confidential nature and have agreed to be bound by the confidentiality and restricted use provisions in this section. Both parties will take all reasonable precautions against the Confidential Information being used by or disclosed to any unauthorized person.

12.4 If a party is required by any law, legal proceeding, or court or government order, to disclose any of the other party's Confidential Information, that party shall limit its disclosure of such Confidential Information to the extent and purpose legally required, provided that prior to any such disclosure the party will promptly notify the other party in writing of the existence and the terms, and conditions of the required disclosure and, at the Confidential Information party's request and expense, co-operate in obtaining a protective order or other assurance that confidential treatment and restricted use will be accorded such Confidential Information.

12.5 The parties acknowledge that a breach by either party or any of its employees of their respective confidentiality obligations pursuant to this Section 12.0 may cause irreparable harm and significant injury to the other party that may be difficult to ascertain. The parties therefore agree that they shall be liable for all damages caused to the other party by such a breach and further agrees that the party whose Confidential Information is breached shall have the right to seek equitable relief including, without limitation, injunction and specific performance, in the event of any breach or threatened breach of the provisions of this Section 12.0 in addition to all other remedies available to that party at law, in equity or otherwise. The breaching party shall pay all of the costs and legal expenses incurred by the other party in pursuing one or more remedies as a result of the breach or threatened breach by the Service Provider of this Section 12.0.

12.6 Either party shall return all copies of the Confidential Information to the other party, in all tangible forms and media, and delete all Confidential Information resident in any databases or systems, upon the earliest of the following dates:

(c) expiration or earlier termination of this Agreement; and

(d) written request of the a party for return of the Confidential Information.

12.7 The Service Provider will comply with its obligations stated in Schedule B to this Agreement.

12.8 Both parties shall ensure that its employees are aware of their obligations of confidentiality under this Section 12.0.

12.9 This Section 12 shall survive the expiration or earlier termination of this Agreement

13.0 NO PROMOTION OF RELATIONSHIP

13.1 Except as set out in section 13.3, the Service Provider will not disclose or promote its relationship with the City, including by means of any verbal declarations, announcements, sales, marketing or other literature, letters, client lists, websites, internet domain names, press releases, brochures or other written materials (the "**Communications**") without the express prior written consent of the City (except as may be necessary for the Service Provider to perform its obligations under this Agreement or to continue the Service Provider's ordinary course of business).

13.2 Furthermore, the Service Provider undertakes not to disclose or promote its relationship with the City in any Communications in a manner that could suggest or create an association, express or implied, between the Service Provider and the City. Without limiting the generality of the foregoing, the Service Provider will not refer to or use any website, domain name, official emblem, logo, or mascot of the City of Vancouver in any Communications without the express prior written consent of the City.

13.3 The Service Provider and the City will develop a join press strategy acceptable to both parties to promote the Solution. The Service Provider will pay for the design, manufacture, and installation of signage to promote the Solution pursuant to the Requirements.

13.4 The Service Provider will ensure that no advertisements appear in the Mobile Application unless the City provides its express prior written consent. In the event that the Service Provider wishes to have advertising appear in the Mobile Application, the Service Provider and the City agree to work collaboratively and in a timely manner to discuss the proposed advertising. The Service Provider will send the City a detailed, written and photographic description of the proposed advertising for the City to consider. If the City does not respond to the Service Provider with comments to such proposed advertising within fourteen (14) days of receiving the description from the Service Provider, the Service Provider may implement the specific advertising described to the City in the Mobile Application. In the event that the Service Provider goes forward with an advertising campaign after the City has not responded to the Service Provider pursuant to this Section 13.4 and the City then wishes to see some changes to the advertising campaign, the Service Provider agrees to consult and collaborate with the City to ensure that the City is comfortable with the advertising.

14.0 UNAVOIDABLE DELAY

14.1 Except for the performance of obligations to pay money, the Service Provider will be relieved from having to perform any obligation under this Agreement that is delayed or prevented due to an Unavoidable Delay. For the purposes of this section, an "Unavoidable Delay" means any circumstances beyond the reasonable control of the party trying to perform (such as, for example, strikes/lockouts, acts of God, war or other strife or governmental action) but expressly excludes any and all delays caused by the Service Provider's lack of financial resources, insolvency or strikes, lockouts or other withdrawals of services arising out of a labour dispute or labour affiliations of the Service Provider's employees or permitted sub-

contractor's employees, or governmental action taken in the enforcement of law specifically against the Service Provider or its permitted sub-contractors. If an Unavoidable Delay occurs, the Service Provider will: (a) as soon as possible after the occurrence of the Unavoidable Delay, give written notice to the City describing the circumstances preventing continued performance and the efforts being made to resume performance of its obligations under this Agreement, and (b) use its best efforts to resume performance and mitigate the adverse impact of the Unavoidable Delay on the City.

15.0 NOTICES

15.1 Any notice required or permitted to be given to the Service Provider will be sufficiently given if delivered in writing by the City to the Service Provider by e-mail or fax to the following:

PayByPhone Technologies Inc.
Suite 1700, Park Place, 666 Burrard Street
Vancouver, British Columbia
V6C 2X8
Attention: **Director, Product Marketing & Strategic Partnerships**
E-Mail: **Aslam@paybyphone.com**

15.2 Any notice required or permitted to be given to the City will be sufficiently given if delivered in writing by the Service Provider to the attention of the City by e-mail or fax to the following:

CITY OF VANCOUVER
453 West 12th Avenue
Vancouver, British Columbia
Attention: **Chief Procurement Officer**
E-Mail: **Nick.Kassam@vancouver.ca**
Fax: **604-873-7057**

with a copy to:

City of Vancouver - Legal Services
453 West 12th Avenue
Vancouver, British Columbia V5Y 1V4

Attention: *Francie Connell and Duncan Finley*
E-Mail: *francie.connell@vancouver.ca; duncan.finley@vancouver.ca*
Fax: *604-873-7445*

16.0 INJUNCTIVE RELIEF AND SPECIFIC PERFORMANCE

16.1 The Service Provider acknowledges that a breach by the Service Provider of any of its obligations under this Agreement (including, without limitation, any of the confidentiality, security, or privacy obligations) may cause irreparable harm and significant injury to the City that may be difficult to ascertain. The Service Provider agrees that it shall be liable for all damages caused to the City by such a breach and further agrees that the City shall have the right to seek equitable relief including, without limitation, injunction and specific performance, in the event of any breach or threatened breach of any of the Service Provider's obligations under this Agreement in addition to all other remedies available to the City at law, in equity or otherwise. The Service Provider shall pay all of the costs and legal expenses incurred by the City in pursuing one or more remedies as a result of the breach or threatened breach by the Service Provider of its obligations.

17.0 NO SUB-CONTRACTING OR ASSIGNMENT

17.1 The Service Provider shall not sub-contract or assign any of its rights or obligations under this Agreement to any other party without the prior written approval of the City. For greater certainty, the foregoing does not prevent the Service Provider from hiring independent contractors to work for it to assist in the performance of the Services. For the purposes of this Agreement, an "assignment" includes a Transfer, as defined in section 17.2. If the City allows the Service Provider to assign certain rights or obligations to another party, the Service Provider shall be responsible for ensuring that such other party complies with all of the confidentiality, security, and privacy provisions set out in this Agreement and any other provision of the Agreement required by the City.

17.2 For the purposes of this Section 17, the following events constitute a Transfer:

(a) an amalgamation of the Service Provider with any other party; or

(b) a change of control of the Service Provider, which includes any transfer, voluntary or involuntary, director or indirect, that results in a change in the person or persons exercising effective control or management of the Service Provider or the business required to be carried on by the Service Provider. For clarity, change of control of the Service Provider does not include a sole change of non-shareholder or non-director management staff or other employees.

18.0 TAXES

18.1 The Service Provider will be responsible for and will collect and remit any and all GST or PST levied on the Contract Price the Service Provider receives for the Services and the City will be responsible for and will collect and remit any and all GST or PST levied on the payments the City receives for the transactions by which a member of the public uses the Solution to pay for parking fees. Subject to the foregoing, the Service Provider will pay all GST or PST and any other sales or excise taxes in force during the Term, as modified by any repeal, enactment, increase, or decrease in such taxes. The Service Provider's invoices to the City will show the appropriate amounts for GST and PST, as applicable.

19.0 MISCELLANEOUS

19.1 **Time of the Essence.** Time shall be of the essence in this Agreement.

19.2 **No Waiver.** No action or failure to act by either party shall constitute a waiver of any right or duty under this Agreement, or constitute an approval or acquiescence in any breach thereunder, except as may be specifically agreed in writing by a party.

19.3 **Severability.** The invalidity, illegality or unenforceability of any portion or provision of this Agreement or the occurrence of any event rendering any portion or provision of this Agreement void shall in no way affect the validity or enforceability of any other portion or provision of this Agreement. Any void portion or provision shall be deemed severed from this Agreement and the balance of this Agreement shall be construed and enforced as if this Agreement did not contain the particular portion or provision held to be void. The parties further agree to amend this Agreement to replace any stricken provision with a valid provision that comes as close as possible to the intent of the stricken position.

19.4 **Workers' Compensation.** Prior to commencing any Services, the Service Provider must provide evidence that it is in good standing with the Workers' Compensation Board of British Columbia ("**WCB**"). The Service Provider is responsible for having all sites where it is performing the Services secured in accordance with WCB safety regulations and ensuring that no danger befalls the public at any time during the performance of the Services. The Service Provider will advise

the City of any accidents or incidents at the workplace that must be reported to the WCB and inform all persons working under this Agreement of all health and safety requirements.

19.5 **Prime Contractor.** The Service Provider is now appointed and accepts appointment as the "prime contractor", as defined in the *Workers Compensation Act* (British Columbia), for the purposes of this Agreement and, as such, accepts responsibility for:

(a) ensuring the Services are performed in a safe manner that complies will all regulatory requirements;

(b) directing and coordinating the work activities related to health and safety of all the sub-contractors engaged by the Service Provider and any other workers involved in the performance of the Services; and

(c) where performing the Services on the City's premises or on public premises, obtaining from the City written information on hazards and conditions and the methods necessary to address those hazards and conditions, before ultimately circulating this information to the necessary parties.

19.6 **Audit Rights.** Subject to the Service Provider's obligations with respect to Payment Card Industry compliance or with respect to other obligations the Service Provider has to not disclose confidential information of third parties, the City may examine, audit, and take away copies of the books, records, documents, and other data of the Service Provider that relate to the Transmitted Data, Services, the Software, or the Solution at any time during the Term. For greater certainty, the parties acknowledge and agree that the City may examine a maximum of twice per year, unless a claim has been identified, without limitation, books, records, bank account records, credit card records, documents, and other data for the purpose of verifying the accuracy and completeness of parking meter revenue payments and transaction fees received from Consumers.

19.7 **Right to Remedy.** Should the Service Provider not perform the Services properly or fail to perform any provision of this Agreement and Service Provider fails to remedy such failure or defect within the delay specified in the Service Level Commitments, the City may, without prejudice to any other right or remedy it may have, make good such deficiencies and deduct the cost thereof from the amounts otherwise due to the Service Provider.

19.8 **Remedies Cumulative.** The remedies of the parties provided for in this Agreement are cumulative and are in addition to any remedies available to the Parties at law or in equity. No remedy will be deemed to exclude or restrict the right of a party to any other remedies against the other party and a party may from time to time have recourse to one or more of the remedies specified in this Agreement or at law notwithstanding the termination of this Agreement.

19.9 **Further Assurances.** Each party shall execute such further and other documents and instruments and do such further and other acts as may be necessary to implement and carry out the provisions and intent of this Agreement.

19.10 **Entire Agreement.** This Agreement and the schedules constitute the entire agreement between the parties with respect to the subject matter hereof, and supersede all previous communications, representations, and agreements, whether oral or written, with respect to the subject matter hereof. The schedules attached hereto are incorporated by reference in and form an integral part of this Agreement.

19.11 **Amendment.** This Agreement shall not be amended except as specifically agreed in writing by both the City and the Service Provider.

19.12 **Sale of Goods.** All provisions of the *International Sale of Goods Act* are specifically excluded from application to this Agreement.

19.13 **Set-Off.** The City may at its option, withhold and set-off against any amount owing to the Service Provider (whether under this Agreement or otherwise) any amounts payable by the Service Provider to the City (whether under this Agreement or otherwise) and the amount of any damages suffered or claims made or to be made by the City as a result of any other claim it may have against the Service Provider, whether such claim is at law or in equity or tort or on any other basis.

19.14 **Enurement.** This Agreement shall enure to the benefit of and be binding upon the City and the Service Provider and their respective successors and permitted assigns.

19.15 **Independent Contractor.** This Agreement is a contract for services and the Service Provider, its officers, directors, shareholders, partners, personnel, affiliates and agents of the Service Provider are not, nor are they to be deemed to be, partners, appointees, employees or agents of the City. The Service Provider will not represent to anyone that the Service Provider has any authority to bind the City in any way or that the Service Provider is an agent of the City.

19.16 **Governing Law and Resolution of Disputes.** This Agreement will be governed by the laws of the Province of British Columbia and, unless the City and the Service Provider agree to mediation or arbitration, the courts of British Columbia will have exclusive jurisdiction to determine all disputes arising under this Agreement and, unless the parties agree otherwise, the parties now agree to submit all disputes to the courts of British Columbia for resolution.

19.17 **Counterparts.** This Agreement may be executed in one or more counterparts, each of which will be deemed an original, but all of which together constitute one and the same document.

As evidence of their Agreement to be bound by the above contract terms, the Service Provider and the City each have executed this Agreement as of the Effective Date.

PAYBYPHONE TECHNOLOGIES INC.

By: _____ Francis Dupuis, President & CEO
Signature Print Name and Title

By: _____ Maggie Clay, CFO
Signature Print Name and Title

CITY OF VANCOUVER

By: _____ N. Kassam
Signature Nick Kassam, Chief Procurement Officer

By: _____ J. Dobrovolny
Signature Jerry Dobrovolny, General Manager of Engineering

By: _____ F. Connell
Signature Frances J. Connell, Director of Legal Services

List of Schedules

Schedule A - Scope of Work

Schedule B - Additional Security and Privacy Requirements

Schedule C - Certificates of Insurance

Schedule D - Contract Price

Schedule E - RFP

Schedule F - Service Provider's Proposal

Schedule G - PCI DSS 3.2 Management Responsibility Matrix Between the Service Provider and the City of Vancouver, and Letter of Attestation

Schedule H - Change Order Request Forms

Schedule I - Service Level Agreement

List of Appendices

Appendix A - Parking Regulations and Rates

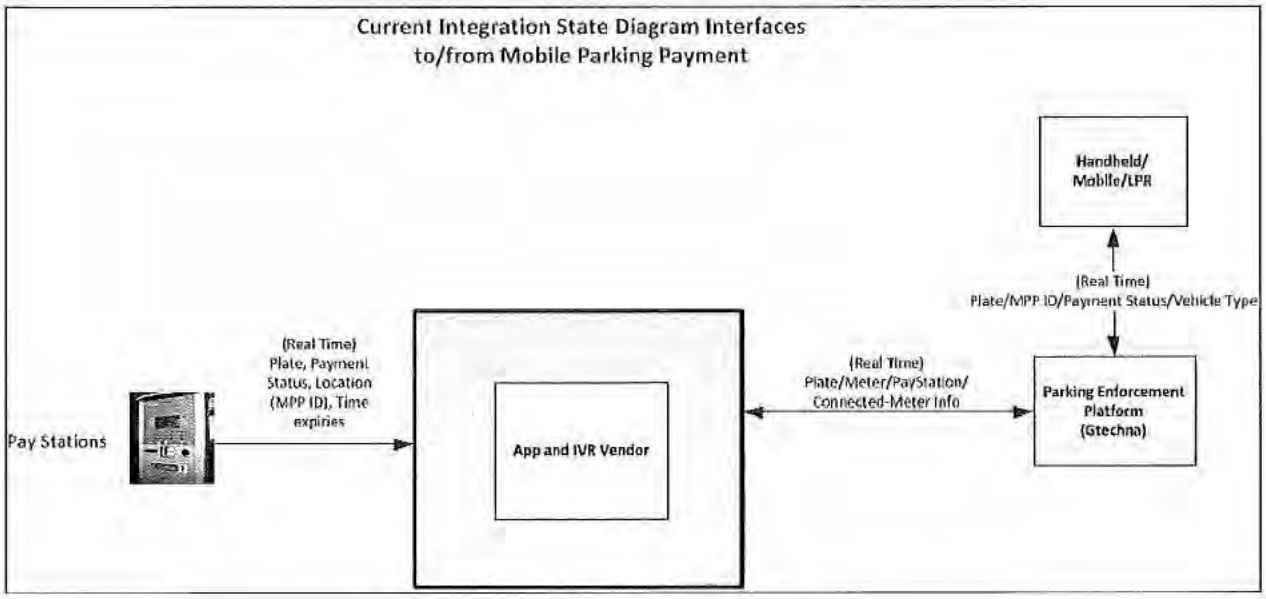
Appendix B - Integration - Current and Future State Diagram

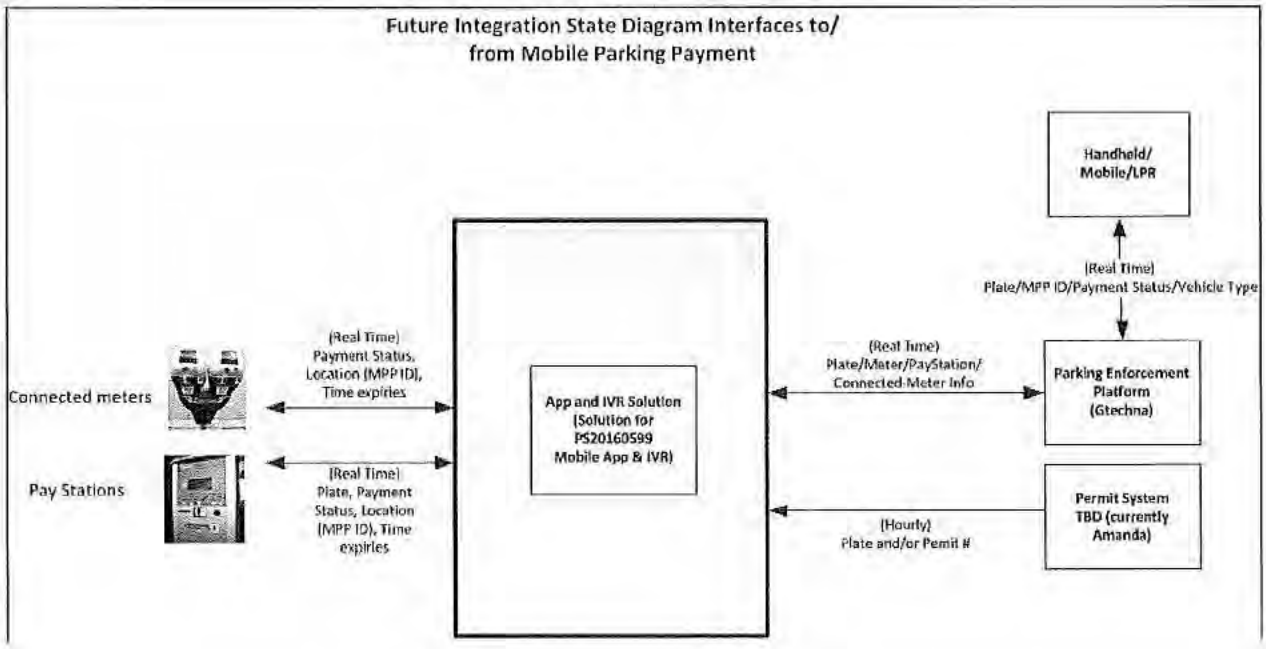
Appendix C - Integration Details

APPENDIX A – Parking Regulations and Rates

Current	Current Maximum Stay rules	Each metered parking space/zone has limits on the maximum amount of time for a parking session (e.g. 2 hours Maximum Stay)
		The Maximum Stay currently varies by time of day but could vary by day of week in the future
		After a parking session is started for a particular license plate at a particular metered parking space/zone, the maximum stay at that location is calculated based on the initial start time of the session until a set period of unpaid time elapses (currently 30 mins)
	Current No Stopping Restrictions	Many metered parking space/zones within the City of Vancouver have part time No Stopping Restrictions to allow the space to be used to accommodate traffic flow (i.e. rush period regulations) or to accommodate other uses such as commercial loading or taxi zones.
		No Stopping Restrictions vary by parking metered parking space/zone, time of day, and day of week
	Current hours in effect	Each metered parking space/zone in Vancouver has pay parking in effect between 9 AM - 10 PM
		Hours in effect could vary by day of week and or location in the future
	Current parking rates	Most metered parking spaces/zones have a flat hourly rate
		There are some metered parking spaces/zones that offer a flat hourly rate in combination with a daily (9 hour) rate
Future	Future changes to Maximum Stay rules	Maximum Stay regulations for the general public may be overridden by Account-Based Parking Rules (ABPR)
	Future changes to Maximum Stay rules	No Stopping Restrictions for the general public may be overridden by Account-Based Parking Rules (ABPR)
	Future changes to hours in effect	Hours in effect could vary by day of week and/or location
	Future changes to parking rates	Hourly rate may vary by time of day and day of week
		Escalating/de-escalating rate steps (e.g. first hour different price than second hour)
		Required purchase of discrete time periods to be purchased (e.g. 4 hours, 6 hours, 24 hours)
		Any combination of the current parking rates
		Parking rates for the general public may be overridden by Account-Based Parking Rules (ABPR)

APPENDIX B – Integration – Current and Future State Diagram





APPENDIX C – Integration Details

Process	From System	To System	Data	Frequency	Direction	Type
On-Street Meter Payment Verification	Mobile Parking Payment (currently PaybyPhone)	Parking Enforcement Platform (Gtechna) Mobile Parking Payment	Meter/PayStation/ConnectedMeter Information (Meter/MPP ID), Plate, date/time, vehicle type	Real time	Bi	API
Account-Based Parking Rules (ABPR) Eligibility	Permit System TBD (currently Amanda)		Plate and/or Permit #, ABPR eligibility features (Maximum Stay, Parking Rate, etc...)	Hourly or better	1 Way	API
Connected Meters Payment	Connected Vendor (currently IPS)	Mobile Parking Payment	Payment Status, Meter/MPP ID, start/end times	Real time	2 Way	API
Pay Stations Payment	Pay Stations (currently Cale and Mackay)	Mobile Parking Payment	Payment Status, Meter/MPP ID, start/end times	Real time	2 Way	API

SCHEDULE A - SCOPE OF WORK

Schedule A - Scope of Work consists of:

Part 1 - General Requirements

Part 2 - Detailed Functional Requirements

Part 3 - Detailed Technical Requirements

Part 4 - Implementation Schedule

Part 1 – General Requirements

1. REQUIREMENTS

1.1. Introduction

1.1.1. The Solution is functional for both a Mobile App and IVR platform; and

- The Solution has the capability to have a robust security methodology; and
- The Solution will be compliant with current and future Payment Card Industry Data Security Standards.

1.1.2. All Solution requirements are documented in this Schedule A – Scope of Work, consisting of: Part 1 – General Requirements; Part 2 – Detailed Functional Requirements; Part 3 – Detailed Technical Requirements; and Part 4 – Service Level Agreement.

1.1.3. Freedom of Information and Protection of Privacy

The Service Provider will comply with all Canadian and British Columbian security and privacy policies, including:

i. BC's Personal Information Protection Act, SBC 2003 c. 36

ii. Federal Personal Information Protection and Electronic Documents Act, SC 2000 c 5

iii. Freedom of Information and Protection of Privacy Act, RSBC 1996, c 165 (FIPPA)

In order to adhere to the privacy legislation, all Transmitted Data, including and especially personal information, will be kept in data centres located in Canada.

2. Project Management and Solution Delivery Services

2.1. Overview

2.1.1. Project Approach

Within fifteen (15) business days of the City's written notification of contract award to the Service Provider, the Service Provider will provide a detailed Project Implementation Plan & Schedule (PIPS).

2.1.2. Project Planning Phase

The project kick-off meeting will begin the Planning Phase of the project. During the kick-off meeting, the Service Provider and the City will jointly discuss timing and staffing issues that will impact the timeline. The result of the sessions shall be an updated work plan and schedule. The City will approve the sequence of implementation, following the completion of the Project Planning Phase.

2.1.3. Project Communication Platform

The Service Provider and the City Project team will be required to share information, messages, and documents. The Service Provider will be responsible for the creation and maintenance of a collaborative environment which is available to both the City project team members and the Service Provider project team members. Both the City and Service Provider Project Managers will have access within the project communication platform to add, edit, and remove members of their teams. All project deliverables and documents will be stored in a location accessible to both teams.

2.1.4. Project Deliverable List

The following table identifies the expected artefacts of the project deliverables to be provided by the Service Provider to the City for all feature releases. The Service Provider's ability to invoice will be measured against the completion of written and accepted deliverables.

Table 4 – Deliverable Timetable

Deliverable #	Deliverable Title	Due Date
1	Written Notification of Contract Award ("NOA") - issued by the City	
2	Project Implementation Plan and Schedule (PIPS) – Initial • To be maintained by the Service Provider	NOA+15
3	Gap Analysis Document	*
4	Solution Design Document (SDD) Assuming that there are gaps in functionality and customization will be required	*
5	Solution Testing Plan (STP) – includes functional testing & user acceptance testing	*
6	Solution Acceptance Criteria - Initial	*
7	Solution Administration Guide and Solution User Guide	*
8	Integration and API Procedure Details	*
9	Marketing and Transition Plan	*
10	Solution User Training Plan	*
11	Solution Issues and Defect Report	*
12	Solution Test Results Report	*
13	Deliverable Delivery Confirmation Log • Solution Receipt • Acceptance Report	*

Note: The asterisk (*) denotes the dates will be determined and included in the Service Provider's Project Implementation Plan Schedule (PIPS). At a minimum, the Service Provider's PIPS shall have each of the above deliverables specified above in its submitted document.

Note: any number added to the Due Date column will represent business days.

2.2. Project Implementation Plan and Schedule - details

2.2.1. The Service Provider is responsible for the development and maintenance of the Project Implementation Plan and Schedule (PIPS), which, at a minimum, must include:

a) Scope and goals of the Implementation Plan;
b) Advantages and challenges, assumptions, and prerequisites of proposed approach;
c) Expectations from City;
d) Detailed timeline;
e) Sequence of deployment tasks;
f) RACI Matrix (Responsible, Accountable, Consulted, Informed); and
g) Sequence and schedule of implementation.

2.2.2. The PIPS will also take into consideration, and include all aspects of business unit & project team readiness such as:

a) Schedule & Availability;
b) Change management;
c) Communication activities;
d) Providing user support post Go-Live;
e) Identifying and resolving impacts;
f) Testing;
g) Training;
h) Interfaces;
i) Hardware; and
j) Reports & Analytics.

2.2.3. The Service Provider will execute the final marketing, transition and production go-live plans, as approved by the City for each new feature that is developed and deployed.

2.3. City Responsibilities

The City shall provide the following:

2.3.1. **Project Business and Technical Support Group.** The project working group is made up of the key stakeholders from the City's business and technology groups.

2.3.2. **Project Management.** The City will assign a dedicated Project Manager to serve as a single point of contact to the Service Provider. The City's Project Manager's duties include, at a minimum:

a) Coordination of project plan development;
b) Schedule coordination;
c) Management of City's project team;

d) Monitoring and facilitating approval of deliverables;
e) Authorizing payment of invoices, pending approval of deliverables;
f) Assuring Service Provider is provided with sufficient access to both technical and business knowledge experts to maintain the project schedule;

2.3.3. **City Project Resources.** The City shall provide relevant resources to support the implementation of City's components within the Solution. **Note:** The Service Provider is responsible for describing the resources required to be provided by the City, by developing a RACI matrix within the project plan deliverable and specifying any other required resources. The City will make reasonable efforts to provide the requested resources.

2.3.4. Coordination of all project meetings between the Service Provider and applicable City functional and IT technical team members.

2.3.5. Work space, electrical power, and associated physical device connectivity within City's facilities for Service Provider personnel, where required.

2.3.6. Network-related troubleshooting as it relates to the implementation of the Solution, with assistance from the Service Provider as necessary and as requested by the City.

2.3.7. **Solution Integration with City Applications.** The City shall provide an Integration Team and Services responsible for:

- Assisting the Service Provider in validating the Solution integration capabilities

2.3.8. **Solution Testing.** The City will participate in the testing process by providing input into the development of testing success criteria.

2.3.9. **Change Management Approval.** The City Project Manager will have the sole approval authority for any Prime Contractor- or subcontractor- requested changes which impact the scope, cost, or timeline of the implementation and general roll-out. The City Project Manager shall validate and obtain required City approvals before any requested changes, as described above, can be made.

2.4. Service Provider's Responsibilities

2.4.1. **Prime Contractor.** The Service Provider (Prime Contractor) will be responsible for contract performance, and any subcontractors used. Any subcontractors and their alternates must be clearly and visibly identified by name, and must abide by all terms and conditions of the contract between the City and the Prime Contractor. If subcontractors are to be used, the Prime Contractor must clearly explain the subcontractors' roles and responsibilities.

2.4.2. **Subcontracting.** Any contract or services (e.g. cloud-hosting) under the Agreement, either in whole or in part, will not be subcontracted, assigned, or otherwise transferred to any other supplier or contract without prior written approval by the City. The Prime Contractor shall be directly responsible for any subcontractor's performance and work quality when used by the Prime

Contractor to carry out any of the scope of work. The Service Provider will ensure that subcontractors do not breach any terms and conditions of the contract between the City and the Prime Contractor.

2.4.3. **Solution Installation and Integration.** From an integration perspective, the Service Provider will be responsible for:

a) Providing, configuring and installing (if necessary) all aspects of the Solution, and any additions deemed necessary, to enable the system to operate according to the performance specifications presented in Schedule A – Scope of Work;
b) Where the Service Provider's Solution has a proven integration with existing City applications, the Service Provider will be responsible for providing the framework and technology to enable integration between the Solution and City applications;
c) Configuring the Solution to City's requirements;

2.4.4. **Service Provider Solution Testing.** The Service Provider is required to plan, execute and verify testing of the Solution, including, but not limited to:

a) Creating an end-to-end test plan for review and approval by City;
b) Coordinating with the City to document the Solution acceptance criteria for each project implementation phase;
c) Unit-testing of all hardware, customizations and user interface(s);
d) Demonstrating functionality of all Solution components;
e) Demonstrating accomplishment of functional and non-functional requirements;
f) Demonstrating reporting and analytic capabilities which address the quantifiable business benefit tracking;
g) Validating integration between the proposed Solution and City applications/equipment;
h) Load- and performance-testing;
i) Demonstrating high availability and failure recovery mechanisms, including:
    - Fail-over and fall-back of data centre systems;
    - Restoration of services to a cold-standby site;
    - Device recovery in the event of power and/or signal loss; and
    - Stress testing.
j) Security and penetration testing; and
k) Demonstrating service-desk and troubleshooting procedures.

2.4.5. **Project Management.** The Service Provider will designate a Project Manager who will be responsible for the management, oversight, delivery, and coordinating resolutions to the project and any associated issues. The Service Provider's Project Manager will also be the primary/single point of contact for Service Provider communications related to the project. For the period from contract initiation, through to the end of the Service Provider's Solution's

acceptance period, the Service Provider's Project Manager shall provide weekly project status reports, which, at a minimum, shall include:

a) Significant work plan tasks performed during the reporting period, and a review of the completed tasks and comparing to plan;
b) Identifying project risks and documenting recommendations to mitigate such risks;
c) Deliverables completed during the reporting period. Identifying milestones reached and comparing to plan;
d) Significant work plan tasks planned for the next reporting period;
e) Deliverables expected to be completed in the next reporting period;
f) Identifying problems or issues and tracking status of problems/issues;
g) Documenting what mitigation effort and plan is being done to achieve resolution of problems/issues; and
h) Project notes and comments.

2.4.6. **The** Service Provider will provide well-trained technical, support, and consulting staff that keep current with the latest technologies, and are fully knowledgeable in the features, configurations, and integrations of the Solution.

2.4.7. At the City's option, the Service Provider will be required to be on-site for the duration of the system cutover to the live production system, and the Service Provider will identify any requirements for Service Provider onsite presence during post-implementation.

2.4.8. The Service Provider will use existing documentation provided by the City (such as functional business and technical requirements). The Service Provider will ensure that the Solution is in compliance with the City's bylaws, and that the Solution meets the Solution requirements.

2.4.9. Compliance with the following at all times, when conducting activities within any City facility:

a) Provisions of all applicable directives of the City and its agencies;
b) Regulations of City Security Standards; and
c) All applicable Federal, Provincial, and Municipal statutes, ordinances, laws, regulations, codes, directives, and/or orders.

2.4.10. Participate in meetings with City's Project Business and Technical Working Group and/or Project Team, as directed by the City's Project Manager.

2.4.11. Communicate the delivery schedules of all Solution delivery implementations to allow the City the ability to track installation and to coordinate testing and acceptance. The delivery shall correspond to the Project Implementation Plan Schedule (PIPS) as required by the City.

2.4.12. Implement all aspects of the Solution, to support the City's implementation and general roll-out of the Solution.

2.4.13. Comply with the City's Change and Configuration Management procedures, including any configuration or customization requirements not specified within

this document. The Service Provider will be responsible for notifying the City's Project Manager to coordinate approval of any proposed Change Requests, or Configuration Management updates prior to installation.

2.4.14. Coordinate all project-related activities through the City's Project Manager.

2.4.15. Ensure timely and accurate identification and notification of issues, problems, and defects in the Solution, work plan, or any other effort related to the project's scope of work, or the Solution.

2.5. Service Provider's Key Personnel

2.5.1. The Service Provider shall provide the key personnel identified below. Key personnel must be available when necessary to meet the requirements of the Solution. The Service Provider may not assign key personnel to other Service Provider projects in any way that results in a conflict in their ability to meet the Requirements of the Agreement. Nor will the Service Provider propose any key personnel in a dual role (such as the Project Manager also being the Senior Systems Engineer). The Service Provider shall provide those individuals accepted by the City, as key personnel throughout the Term, except as provided in Section 2.5.2 - Substitution of Key Personnel, below.

Key Personnel Qualifications

a) The Service Provider certifies that key personnel meet the qualifications identified in, Section 2.5 (refer to Section 2.5.3 - Qualifications for Key Personnel, for further details); and

b) On a case-by-case basis, Service Provider key personnel may be interviewed and approved by the City for performance in multiple skill categories for which they are qualified.

2.5.2. **Substitution of Key Personnel**

a) Stability of key personnel is critical to project success. For this reason, the Service Provider shall retain key personnel interviewed and accepted by the City for a minimum period beginning from the receipt of a written NOA, and ending upon successful implementation. All proposed substitutes for key personnel, for reasons other than emergency situations (illness, death, emergency resignation, or emergency disciplinary termination), shall be submitted in writing by the Service Provider to the City at least ten (10) business days in advance of the substitution, and the nominated individuals must be approved by the City's Project Manager prior to the proposed substitute's commencement of work on the Project;

b) The Service Provider shall permit the City to interview and accept any proposed substitute for a key employee. The résumé of any proposed substitute shall be signed by the substitute and by the Service Provider's Project Manager and the résumé of the previous key employee shall be provided for comparison purposes;

c) City Project Manager must agree to the substitution in writing before the substitution becomes effective;

d) Any proposed substitute for a key employee shall have qualifications at least equal to those submitted in the Service Provider Personnel Résumé. The responsibility for providing evidence of meeting this requirement belongs to the Service Provider; and

e) If one or more key personnel are unavailable for work under the Agreement for a continuous period exceeding ten (10) business days, the Service Provider will be required to immediately provide written notification to the City's Project Manager, and at the city's discretion, to replace the personnel with approved substitutes of equal or better qualifications within ten (10) business days after providing the City's Project Manager with the written notification.

2.5.3. **Qualifications for Key Personnel**

a) **Project Manager (PM)** - The PM is assigned the management of the Service Provider's Solution, and project for the work performed under the Agreement. S/he performs day-to-day management of the project, identifies issues and risks, and recommends possible issue and risk mitigation strategies associated with the project. The PM acts as a facilitator between the City and the Service Provider. The PM is responsible for ensuring that work performed under the Agreement is within scope, consistent with requirements, and delivered on time and on budget. Identifies critical paths, tasks, dates, testing, and acceptance criteria. The PM provides solutions to improve efficiency (e.g., reduce costs while maintaining or improving performance levels), monitors issues and provides resolutions for up-to-date status reports, and demonstrates excellent writing and oral communications skills;

b) **Senior Application Systems Specialist** - Must be able to analyze information requirements. Must be able to evaluate problems in workflow, organization, and planning. Develops appropriate corrective action. Ensures the proposed Solution interface, reporting, analysis tools, integration parameters and processes address the requirements for the system.

c) **Integration Architect** - The Integration Architect is responsible for ensuring that the Service Provider's Solution effectively communicates via published API's using industry standard programming languages. In particular, this role will need to assure integration capabilities to City environment.

d) **Mobile Specialist** - The Mobile Specialist is responsible for ensuring that the supplier's Solution is configured for the expected business function; specifically the components that affect speed, user experience, compatibility with operating system. The Mobile Specialist also will ensure that the mobile application is customized and tested to follow the requirements of the Scope of Work.

3. Testing, Training, Implementation, Acceptance, and Marketing

3.1. Testing

Within the Solution Test Plan deliverable, the Service Provider will **describe the procedures for such testing, as well as** how the Service Provider will support the following testing methodology and timeline to incorporate the following test types and scenarios.

3.1.1. Develop Solution Test Scripts and Expected Outcomes

The Service Provider must develop detailed system test scripts and expected outcomes from the detailed design documents and the Solution Test Plan, which will include the following:

a) Test scripts and expected outcomes encompassing all modules and business functionalities for each project phase;
b) Submit a comprehensive test data set, aligned to the test scripts and expected outcomes.

3.1.2. Conduct Solution Testing

a) The City and Service Provider are responsible and accountable for conducting system testing of the proposed Solution (detailed and stress tests);

b) For the duration of the lifespan of the Solution, the Service Provider will support a development and/or testing environment, in which new hardware, functionality, reports and workflows will be tested by the business prior to implementation in a Production environment.

c) Depending on the origin of any issues arising from the test events, the Service Provider must resolve all issues (defects), under their control, that are discovered during system testing. Any issues (defects) discovered that are under the City's direct control, the Service Provider must assist and provide direction to ensure the defect resolution.

d) All test scripts and scenarios, which do not pass the system testing, must be addressed to the City's satisfaction prior to implementation.

e) The Service Provider must log and track all defects until resolved in a defect-tracking tool, which will be available to the City project team for update and comments.

f) Based on the tests performed, the Service Provider must develop a Solution Test Execution Report, which includes Testing Defects and Issues Log; and

g) The City will verify that the system testing process and testing results are in accordance with the Solution Test Plan and report any deviations. The Service Provider must support the City during the assessment. The Service Provider

must implement a mutually agreed upon Statement of Work based on the project phase testing results.

3.1.3. **Solution Test Execution Report.** At the conclusion of Solution Testing phases, the Service Provider will provide a test report and delivered to the City within five (5) business days of the testing phase conclusion that includes:

a) Completed and signed checklists documenting the successful performance of each inspection or test;

b) A detailed schedule for discrepancy correction and retesting;

c) A lessons learned document indicating what went well, and what did not, in the performance of the particular testing phase; and

d) A list of updates/revisions needed to the testing plans for any subsequent testing/retesting phases.

3.1.4. **Verify/Validate Stress Testing Process and Results.** The City will verify that the testing process and testing results are in accordance with the Test Plan and will report any deviations.

3.1.5. **Testing Data and Software.** The Service Provider will specify any requirements necessary for testing. The Service Provider will be responsible for creating test data for all testing phases. The Service Provider will provide a method that can be used for logging test cases and for defect tracking and resolution process (logs all test cases, results, and issue resolution). Sufficient time must be allocated to train City personnel on the testing expectations and procedures.

3.1.6. **Develop/Provide User Acceptance Test plan.** A User Acceptance Test ("UAT") Plan shall be created by the Service Provider, with the assistance of the City acting as the primary guide for the execution of the User Acceptance Testing activity for all interfaces that the business or drivers will interact with. The user test scripts and scenarios will cover the complete Solution, all City modules, and interfaces.

3.1.7. **Execute User Acceptance Test.** A coordinated UAT where City project team and the Service Provider will conduct user acceptance testing on the Solution, based on test scripts provided by the Service Provider.

If defects are identified during user acceptance testing, the Service Provider will address the defect and the Service Provider will be responsible for implementing a mutually agreed scope of work based on the project phase testing results.

The Service Provider is responsible for updating all application and user documentation to be consistent with code that has been accepted and that will be promoted to the production environment.

3.1.8. **Testing Support**

The Service Provider will:

a) Conduct functional testing to ensure the data produced from the proposed Solution addresses the scope of work of the project phase;

b) Provide on-site assistance to the City during Functional, Integration, and User Acceptance Testing of the Solution for each project phase;

c) Provide error handling and disaster recovery procedures, which ensure the components of the application work in accordance with City requirements; and

d) Update the testing plans and procedures based on feedback from the City, and provide the revised/updated plan(s) to the City at least five (5) business days prior to performance of the testing processes described above.

3.2. Training

See details in Schedule A, Scope of Work, Part 2 Detailed Functional Requirements, Training Requirements.

3.2.1. **Develop Training Plan**. The Service Provider will develop a comprehensive User Training Plan Deliverable which must include/describe, at a minimum:

a) the prerequisite user knowledge required prior to beginning training, as well as expected learning objectives, areas of focus and outcomes for each component of the training;

b) details regarding the required materials, amount of time and expected learning objectives of each training course;

c) differences based on the area of focus of the training; and

d) Recommendations as to training details (how many per session, how long for each session, required materials & technology).

3.2.2. **Conduct Training**

The supplier will provide cost details in Schedule D for further training sessions (please include details for on-site and remote training opportunities).

3.3. Implementation

3.3.1. During the Solution implementation, the Service Provider will provide the following:

a) Complete and timely installation, and coordination of all Installation processes with the City's Project Manager;

b) Confirm all Project Scope of Work and functional and technical requirements for the Solution have been met or addressed;

c) Prior to the Solution implementation, the Service Provider shall ensure that all the deliverables described in the proposal documents have been approved and accepted by the City's Project Manager;

d) Training and Issues support is in place to aid the business in the implementation process;

e) Implementation support;

f) Conduct a walkthrough of the Solution User Guide and all Training Materials with the City Project Team; and

g) Update the City Project team in a timely manner.

3.4. Implementation Support

3.4.1. The Service Provider shall provide services for "implementation support" activities.

3.4.2. The Service Provider will provide support staffing during installation through production go-live,

3.4.3. The Service Provider will complete a milestone status report for each significant implementation milestone, stating what was completed and what actions are necessary as a result of the milestone. The City will review and formally accept each milestone report if the milestone deliverable demonstrates fulfillment of the requirements.

3.5. Solution Acceptance

3.5.1. Solution Acceptance will occur in four (4) phases:

a) **Functional Certification:** For each project phase the Service Provider will certify that the Service Provider's Solution implementation is complete in accordance with project phase scope of work.

b) **Proof of Integration:** The Service Provider is responsible for ensuring that the Solution is capable of integrating with the City's current suite of application integrations (including the capability to integrate via web services platform). To confirm that this has been successful, the Service Provider will work with City teams to ensure that bi-directional communication between the Service Provider's Solution and designated City's applications are fully operational.

c) **Production System Documentation**: The Service Provider will deliver "as built" online or otherwise electronic and hard copy documentation, clearly describing actual implementation configurations, settings, customizations, and complete installed Solution documentation.

d) **60-Day Reliability Test:** The duration for the Performance Period for Acceptance shall be sixty (60) calendar days and shall begin after:

i. Configuration and Implementation of the Solution user interface has been deployed in a Production Environment for a period of sixty (60) calendar days;

ii. No major bugs or defects have been reported to the Service Provider in the implemented Solution for a period of sixty (60) days;

iii. Successful completion of User Acceptance Testing; and

iv. City users and Consumers have been utilizing the application for a minimum of sixty (60) days.

Criteria for Success:

- No major defects or bugs within the Solution has been reported;
- Solution uptime is consistent with SLA parameters set out in Schedule I SLA
- Support response is consistent with SLA parameters set out in Schedule I SLA
- All functions implemented within the project phase scope of work continue to be functional.

Outcome:

City's Project Manager will issue a written notice to the Service Provider of either completion or failure of the 60-Day Reliability Test.

In the event that the 60-Day Reliability Test has been unsuccessful, the City Project Manager will identify the areas which were unsuccessful and collaborate with the Service Provider on an acceptable Solution - upon which the application will then re-enter the Performance Period for Acceptance, and repeat if necessary until successful.

3.5.2. Solution Acceptance Completion

After all System Acceptance benchmarks have been achieved - the Service Provider will provide City staff with a Solution Acceptance Report, which documents benchmarks, significant achievements, deliverables and signoffs, for the phase of project implementation.

Upon City receipt and acceptance of the Solution Acceptance Report from the Service Provider, the project will enter a sustainment phase, in which all components have been installed and the Solution deemed to be stable.

3.6. Marketing and Transition Plan

3.6.1. Marketing and Transition Plan

If the City responds with comments to the Service Provider's consultation pursuant to Section 3.6 of the Agreement regarding changes to the Mobile Application that are not contemplated in this Schedule A to the Agreement, the Service Provider will be responsible for creating and executing a comprehensive Marketing Plan. Such Marketing Plans will include:

- An overall strategy to ensure minimal disruption to the Consumer at initial roll-out, (may include direct contact with account information for existing Consumers);
- An overall strategy to improve awareness of the Solution for the term of the Agreement;
- A comprehensive marketing and communications plan outlining how the Service Provider will promote the base and enhanced MPP features to encourage usage;
- Identification of tasks that are to be performed by the Service Provider, the City and other parties; and
- Design and installation of parking meter and pay station decals and/or other materials (e.g. NFC chips, signage, if required)

Prior to the execution of the Marketing Plan, the Service Provider must receive approval from the City.

4. Maintenance Services and Level of Support

4.1. Technical, Maintenance, Operations and Level of Support

4.1.1. **Technical Support**

The Service Provider will provide support for the proposed Solution (including technical, hardware, and data, reporting and billing inquiries). See Schedule I SLA for details.

4.1.2. **System Support Services**

a) The Service Provider will provide system maintenance (e.g. upgrades, enhancements, new releases, etc.) and technical support for all products/services provided under the Agreement, including ongoing unlimited technical support problem determination and resolution;

b) The Service Provider will provide recurring application maintenance for the Solution;

c) The Service Provider will provide for any upgrades to the system components to accommodate and maintain the Solution customizations developed within the scope of the project phases (or contracted with the Service Provider in a change request form - in the form of Schedule H). Concurrent with the installation of any upgrade or revision to the Solution, the Service Provider must provide the City with updated Solution documentation;

d) The Service Provider must fully test and resolve any Solution deficiency on upgrades prior to installing/implementing the upgrades into production;

e) The Service Provider must ensure that upgrades may be rolled-back. There must be a back-out strategy if an upgrade fails. In performing the regression testing on a new version/upgrade of the Solution, the Service Provider must certify in writing to the City that all the previous (i.e. prior) Solution capabilities will continue to work in accordance with the requirements described in this Schedule A - Scope of Work;

f) Maintenance services shall include, at a minimum, the detection and correction of Solution errors discovered by the City, or otherwise made known to the Service Provider. The Service Provider agrees to respond to the City's inquiries regarding the use and functionality of the Solution as issues are encountered by system users;

g) For a cloud-based Solution, System Maintenance will also include all services necessary to maintain uptime redundancy, and recovery as described in Schedule I SLA for all products provided by the Service Provider, as well as the resolution of system errors, malfunctions, and system restoration. Scheduled downtime for maintenance or upgrades shall not be included in the calculation of system production uptime;

h) The Service Provider will update the Solution and configuration settings; and

i) If investigation and research is required by the Service Provider's technical staff, and the problem cannot be resolved (or the question cannot be answered immediately), the Service Provider's help desk/technical support staff will notify City representatives and provide City personnel with a progress report (in electronic format) on the problem's resolution per Schedule I SLA. The Service Provider will continue to update City staff on the ongoing progress related to resolving the problem.

4.1.3. Maintenance Log

The Service Provider will keep a log of all maintenance/technical support calls made to the Service Provider's Help Desk/technical support personnel, and

document the complaints and problems reported to the help desk system, whether reported by a City resource or by the Service Provider. The log shall be made available to the City as part of monthly or quarterly reporting, and at any other time as requested by the City. Maintenance logs will be delivered to, or made available to the City no later than by the close of business (at 5:00 p.m. Pacific Time) on the fifth calendar day of every month. The log will, at a minimum, contain the following information:

a) Time of incident notification;

b) Name of City resource;

c) Ticket Number;

d) Description of Reported Problem/Complaint;

e) Indication of whether the problem/compliant was resolved at time of call;

f) Description of any follow-up investigation/resolution plans;

g) Date of and Description of Final Resolution;

4.1.4. Level of Support:

a) The Service Provider will provide support services for the proposed Solution. The services proposed by the Service Provider will include, but not be limited to, the following issues:

- **Escalation Procedures:** The Service Provider will provide the City with a copy of the Service Provider's trouble escalation procedures, and provide a written description of the processes and procedures that would be followed by City personnel when issues require escalation. The Service Provider will maintain the above-mentioned procedures with correct and current data during the course of the maintenance period;

- **Installation, Verification and Validation:** The Service Provider will provide support during testing phases of new releases of the application;

- **Application Defects:** The Service Provider will provide resolution to all confirmed application defects

- **Upgrade Support:** The Service Provider must offer, for the full term of the maintenance agreement, support for the proposed Solution to

ensure continued operation during and after upgrades and implementation of new releases of all user interface applications covered under the Service Provider's standard maintenance agreement;

- **Enhancements:** The Service Provider must provide enhancement updates to the user interface applications as they become available, or as requested by the City. The Service Provider will provide a description of the method of distributing information on the available updates and software modifications, with clearly-defined responsibilities of the Service Provider and the City.

b) Through Solution support, the Service Provider will ensure that the Solution remains compatible with the current and future City operating system software (Windows 7+), web browser (IE 11+ and Chrome), or any third-party software used by the Service Provider that is associated with the developed Solution;

c) Solution support includes updates and modifications as required, as a matter of federal, provincial or municipal law, and/or regulation in connection with the City's compliance standards; and

d) The Service Provider shall comply with the City's Change Management Process for testing and implementing Solution-related changes in the production environment. This process consists of thorough Solution-testing in the Development/Testing Environment. Following testing and acceptance, the system may be loaded into the Production Environment.

5. Security Requirements

5.1. Service Provider Security Requirements

5.1.1. The integrity and security of the data communications are fundamental components of all applications procured by the City; accordingly, the City has implemented security processes and procedures that foster and safeguard the data integrity within all City applications.

5.1.2. The Service Provider will comply with City Information Technology security policies and procedures regarding access to the City's networks and physical facilities;

5.1.3. Authorized Service Provider staff may require secured remote access privileges into the configuration. City IT staff reserve the right to monitor all remote access activities;

5.1.4. The Service Provider shall comply with, and adhere to, all relevant City Policies and Standards. These policies may be revised from time to time, and the Service Provider shall comply with all such revisions. Current and revised versions of the security policy will be made available to the Service Provider;

5.1.5. The Service Provider shall complete all required paperwork for security access if access is needed to the City's Information Technology LAN/WAN, as directed and coordinated with the City's Project Manager;

5.1.6. Any Service Provider employee providing services under the Agreement, who will be in and out of City facilities on a daily basis, must participate in a City security awareness, occupational health & safety orientation and training session; and

5.1.7. At all times, at any City facility, the Service Provider's personnel shall ensure cooperation with City site requirements, inclusive of being escorted at all times (if required), providing information in order to obtain a badge, and wearing the badge in a visible manner at all times.

5.1.8. The integrity and security of the data storage (when being collected, in transit and within the application) is of paramount importance to the City; therefore, the Service Provider and the Solution must adhere to industry best practices in terms of data encryption, data transmission and key management.

Part 2 – Detailed Functional Requirements

1.0 Global Requirements

Requirement 1.1

Requirement	The Solution will be functional for both a Mobile App and IVR platform
Required Implementation Date	Effective Date
References	Annex 2: ID 1.1, Service Provider Proposal Reference: 2.1.2

Requirement 1.2

Requirement	The Solution will accommodate an MPP ID location numbering system similar to what is detailed in Appendix B of the RFP (Schedule E - RFP Appendix B) - Parking Meter Management Table. - Parking Meter Management Table.
Required Implementation Date	Effective Date
References	Annex 2: ID 1.2, Service Provider Proposal Reference: 2.1.3

Requirement 1.3

Requirement	The Solution will have the ability to support 10,000-20,000 metered parking spaces/zones which have parking regulations and rates that can vary individually and/or by block according to the current parking regulations and rates are described in Appendix A - Parking Regulations and Rates - Parking Regulations and Rates. Current parking regulations and rates for all City metered parking spaces/zones are detailed in Appendix B of the RFP (Schedule E - RFP Appendix B) - Parking Meter Management Table. - Parking Meter Management Table.
Required Implementation Date	Effective Date
References	Annex 2: ID 1.3, Service Provider Proposal Reference: 2.1.4

Requirement 1.4

Requirement	Ability to support 10,000-20,000 metered parking spaces/zones which have parking regulations and rates that can vary individually and/or by block according to the future parking regulations and

	described in Appendix A - Parking Regulations and Rates - Parking Regulations and Rates.
Required Implementation Date	Effective Date
References	Annex 2: ID 1.4, Service Provider Proposal Reference: 2.1.5

Requirement 1.5A

Requirement	The Solution will accept the addition of new metered parking spaces/zones as well as changes to the parking regulations and rates of existing metered parking spaces/zones manually, via an user-friendly website or software The Solution will be able to verify that data supplied by City has been entered/loaded correctly. The Solution should also allow the User to set effective time and date when the new metered space/zone attributes go into effect
Required Implementation Date	Effective Date
References	Annex 2: ID 1.4, Service Provider Proposal Reference 2.1.6
Specific Training Required	Yes, Include in Training Plan (Refresher training)

Requirement 1.5B

Requirement	The Solution will accept the addition of new metered parking spaces/zones as well as changes to the parking regulations and rates of existing metered parking spaces/zones automatically via XML or CSV file deposited to the Proponent's SFTP site or similar. The Solution will be able to verify that data supplied by City has been entered/loaded correctly. The Solution should also allow the User to set effective time and date when the new metered space/zone attributes go into effect
Required Implementation Date	Required by November 2017
References	Annex 2: ID 1.4, Service Provider Proposal Reference 2.1.6
Specific Training Required	Yes, Include in Training Plan (New features)
Specific Testing Required	Yes - Successful testing and sign-off by City required prior to implementation.

Requirement 1.6A

Requirement	To accommodate Special Event Scheduling, for every MPP ID, temporary parking regulations and rates should have the ability to be programmed in advance
Required Implementation Date	Effective Date
References	Annex 2: ID 1.6, Service Provider Proposal Reference 2.1.7
Specific Training Required	Yes, Include in Training Plan (Refresher training)

Requirement 1.6B

Requirement	At a future date, the City may wish to integrate a 3rd party system to put temporary parking regulations and rates into effect. The Solution must be capable of this integration.
Required Implementation Date	Six months from when requested by City
References	Annex 2: ID 1.6, Service Provider Proposal Reference 2.1.7
Specific Training Required	Yes, Include in Training Plan (New features)
Specific Testing Required	Yes - Successful testing and sign-off by City required prior to implementation.

Requirement 1.7

Requirement	To accommodate Special Event Scheduling, for every MPP ID, temporary parking regulations and rates will have the ability to be programmed in real-time.
Required Implementation Date	Effective Date
References	Annex 2: ID 1.7, Service Provider Proposal Reference 2.1.8
Specific Training Required	Yes, Include in Training Plan (Refresher training)

Requirement 1.8

Requirement	Date formatting will follow MM/DD/YYYY and Time formatting will follow 24hr clock (HH:MM:SS)
Required Implementation	Effective Date

Date	
References	Annex 2: ID 1.8, Service Provider Proposal Reference 2.1.9

Requirement 1.9

Requirement	The date/time will be reported in local time and be capable of automatically adjusting for daylight savings time For details, refer to Schedule I Service Level Agreement
Required Implementation Date	Effective Date
References	Annex 2: ID 1.9, Service Provider Proposal Reference 2.1.10

Requirement 1.10

Requirement	All Solution functionality will be available to all users 24 hrs per day 365 days per year (with exception(s) to be made for scheduled updates and system maintenance - subject to agreement SLA). The operating hours of the business units are 6am-12am PST.
Required Implementation Date	Effective Date
References	Schedule A, Part 4 - Service Level Agreement; Annex 2: ID 1.9, Service Provider Proposal Reference 2.1.11

Requirement 1.11

Requirement	The Solution will have a reliable and proven audit trail process, including minimum specifications to keep an audit of when data is created, modified, and by whom
Required Implementation Date	Effective Date
References	Annex 2: ID 1.11, Service Provider Proposal Reference 2.1.12

Requirement 1.12

The requirement listed in Annex 2: ID 1.12 in the RFP is not required as part of the Agreement.

Requirement 1.13

Requirement	The Solution is able to change fee calculation and billing schedule without software modification
Required Implementation	Effective Date

Date	
References	Annex 2: ID 1.13, Service Provider Proposal Reference 2.1.14

Requirement 1.14

Requirement	All information displayed to and requiring data entry will be optimized for display depending on the resolution of the device being used
Required Implementation Date	Effective Date
References	Annex 2: ID 1.14, Service Provider Proposal Reference 2.1.15

Requirement 1.15

Requirement	The Solution will only require the following infrastructure on street: • Stickers and / or signage communicating information regarding how to access the service including telephone numbers, web site URL and application name for app stores • Stickers providing location numbers to be used within the apps or IVR when initiating payment The Service Provider will be responsible for the material and labour costs for installation and reinstallation of MPP-related stickers and/or signage on all parking meter equipment as follows: 1. Year 1: Pilot new signage 2. End of Year 2: signage refresh 3. End of Year 6: signage refresh 4. End of Year 9: signage refresh 5. When the decals are to be changed as the result of a Service Provider initiated request
Required Implementation Date	Effective Date
References	Annex 2: ID 1.15, Service Provider Proposal Reference 2.1.16, Section 7B.4

Requirement 1.16

Requirement	The City has pay-by-plate pay stations. It may be possible for a Consumer to exceed the Maximum Stay if they purchase time using the Solution then "re-meter" using the pay-by-plate pay station (or vice versa).

	The Solution will be able to prevent this re-metering from occurring.
Required Implementation Date	6 months from when requested by the City
References	Annex 2: ID 1.16, Service Provider Proposal Reference 2.1.17
Specific Training Required	If this feature is requested by the City, include in Training Plan (New features)
Specific Testing Required	If this feature is requested by the City, Successful Testing and sign-off by City required prior to implementation

Requirement 1.17A

Requirement	Solution will be capable of integrating with Connected Meters to send payment information to PayByPhone Integrations to Cale and Mackay Pay-by-licence pay stations currently exist and are not subject to additional integration fees (monthly or lump sum)
Required Implementation Date	• For Cale and Mackay Pay-by-licence pay stations: Effective Date • For other connected meter integrations: 3 months from when requested by City
References	Annex 2: ID 1.17, Service Provider Proposal Reference 2.1.18

Requirement 1.17B

Requirement	Solution will be capable of integrating with Connected Meters to allow of communication/display of MPP payments at Connected Meters in real-time Integrations to Cale and Mackay Pay-by-licence pay stations are not subject to additional integration fees (monthly or lump sum)
Required Implementation Date	3 months from when requested by City
References	Annex 2: ID 1.17, Service Provider Proposal Reference 2.1.18
Specific Training Required	If this feature is requested by the City, include in Training Plan (New features)
Specific Testing Required	If this feature is requested by the City, Successful Testing and sign-off by City required prior to implementation

Requirement 1.18

Requirement	The Solution will be able to support Account-Based Parking Rules (ABPR) that would will allow City-registered Consumers to:

	- Be eligible to park in a space/zone that the general public cannot; - Have access to different metered parking rates (including free); and; - Allow for a longer/shorter Maximum Stay; or, - Any combination of the above The initial roll-out of ABPR will be with a small group (<200) of internal City employees and will not include an integration to POSSE. An iterative design process with the supplier is required. The feature will be activated after design sign-off by the City. A detailed implementation schedule will be created by the Service Provider and signed-off by the City.
Required Implementation Date	3 months from when requested by the City
References	Annex 2: ID 1.18, Service Provider Proposal Reference 2.1.19,
Specific Training Required	Yes - Include in Training Plan (New features)
Specific Testing Required	Yes - Successful testing and sign-off by City required prior to implementation

Requirement 1.19

Requirement	The Solution will be able to support multiple types of ABPR user groups. Examples of these user groups include: - On-duty City staff - Able to park for free at metered parking spaces/zones for a maximum of three hours; able to park in any time limited zone (e.g. 1 hour parking) for a maximum of three hours - On-duty City inspectors - Able to park for free at metered parking spaces/zones for a maximum of three hours; able to park in City of Vancouver lanes for a maximum of three hours; able to park in all Residential Permit Zones (except for near City Hall) for a maximum of three hours - Tradespeople - Able to park at metered parking spaces/zones at a public rate for a maximum of 12 hours and in select Residential Permit zones at set rate for a maximum of 5 hours between 7 AM and 5 PM - Commercial vehicles - Able to park at commercial loading zones for up to 30 minutes (general public cannot do this) - Resident authorized visitors - able to park in select Residential Parking Permit zones for up to 24 hours using a daily rate OR able to park for a discount rate for up to 8 hours in a neighbourhood - Consumers may be part of more than one user group. The initial roll-out of ABPR will be with a small group (<200) of

	internal City employees and will not include an integration to POSSE. An iterative design process with the supplier is required. The feature will be activated after design sign-off by the City. A detailed implementation schedule will be created by the Service Provider and signed-off by the City.
Required Implementation Date	3 months from when requested by the City
References	Annex 2: ID 1.19; Service Provider Proposal Reference 2.1.19; Schedule A Part 1 2.2.4.1;
Specific Training Required	Yes - Include in Training Plan (New features)
Specific Testing Required	Yes - Successful testing and sign-off by City required prior to implementation

Requirement 1.20

Refer to Section 7B.

Requirement 1.21

Requirement	The Solution will be able to prevent re-metering from Parking Sessions initiated on another MPP service.
Required Implementation Date	6 months from when requested by the City
References	Annex 2: ID 1.21, Service Provider Proposal Reference 2.1.22
Specific Training Required	Yes - Include in Training Plan (New features)
Specific Testing Required	Yes - Successful Testing and sign-off by City required prior to implementation

2.0 Mobile App Requirements

Requirement 2.1

Requirement	Mobile App will be available on iOS and Android Platforms
Required Implementation Date	Effective Date
References	Annex 2: ID 2.1, Service Provider Proposal Reference 2.2.2, 2.2.3

Requirement 2.2

Requirement	Mobile App will be available via an internet browser optimized for mobile
Required Implementation Date	Effective Date
References	Annex 2: ID 2.2, Service Provider Proposal Reference 2.2.2, 2.2.3

Requirement 2.3

Requirement	Mobile App will be available on other platforms
Required Implementation Date	Effective Date
References	Annex 2: ID 2.3, Service Provider Proposal Reference 2.2.2, 2.2.3

Requirement 2.4

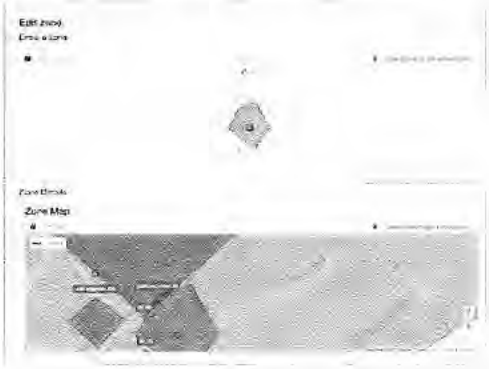
Requirement	Mobile App will be integrated with and/or exposed to wearables such as smart watches (e.g. Apple Watch, Samsung Gear,etc)
Required Implementation Date	Effective Date
References	Annex 2: ID 2.4, Service Provider Proposal Reference 2.2.2, 2.2.3

Requirement 2.5

Requirement	Mobile App will be offered in English, Simplified Chinese, Traditional Chinese, and Punjabi. An iterative design process with the Service Provider is required. The feature will be activated after design sign-off by the City. A detailed implementation schedule will be created by the Service Provider and signed-off by the City.

	Simplified Chinese and Traditional Chinese to be rolled out concurrently and for development, release, and payment purposes are to be considered a single language.
Required Implementation Date	English: Effective Date Simplified Chinese and Traditional Chinese and Punjabi: Effective Date + 6 months for the first non-Latin language and an additional 3 months for the additional language.
References	Annex 2, ID 2.5, Service Provider Proposal Reference 2.2.2.1
Specific Training Required	Yes - Include in Training Plan (New features)
Specific Testing Required	Yes - Successful testing and sign-off by City required prior to implementation

Requirement 2.6

Requirement	The Solution will allow for customization of the brand identity (e.g make changes to the design and/or look of the app to reflect or compliment the City of Vancouver brand) in the Mobile App. The City requires that this feature will operate similarly to the initial mock-ups provided in the Proposal as well as the additional screenshots provided here which highlight zone-based Dynamic labelling. City based DL Zone Based DL  A detailed implementation schedule will be created by the Service Provider and signed-off by the City.
Required Implementation Date	As requested by the City + 3 months
References	Annex 2: ID 2.6, Service Provider Proposal Reference: 2.2.2.2
Specific Training Required	Yes - Include in Training Plan (New features)

Specific Testing Required	Yes - Successful Testing and sign-off by City required prior to implementation

Requirement 2.7

Requirement	Consumers can create a secure MPP account for their exclusive use
Required Implementation Date	Effective Date
References	Annex 2: ID 2.7, Service Provider Proposal Reference 2.2.4

Requirement 2.8

Requirement	Consumers can create a secure MPP account using social media login (e.g. Facebook) (Note: a Solution meeting this requirement must be compliant with all applicable privacy laws) It is expected that this functionality be presented to Consumers similar to the following screenshots:
Required Implementation Date	Effective Date + 3 months
References	Annex 2: ID 2.8, Service Provider Proposal Reference 2.2.4.5

Requirement 2.9

Requirement	Consumers can add one or more licence plates (from all North American jurisdictions)
Required Implementation Date	Effective Date
References	Annex 2: ID 2.9, Service Provider Proposal Reference 2.2.5, 2.2.5.1

Requirement 2.10

Requirement	Consumers can specify vehicle type (e.g. regular vehicle or motorcycle) to each plate on MPP account
Required Implementation Date	Effective Date
References	Annex 2: ID 2.10, Service Provider Proposal Reference 2.2.5.1

Requirement 2.11

Requirement	Consumers can add/modify/remove credit card information to their MPP account
Required Implementation Date	Effective Date
References	Annex 2: ID 2.11, Service Provider Proposal Reference 2.2.5.1

Requirement 2.12

Requirement	Consumers can add/modify/remove credit card information to their MPP account
Required Implementation Date	Effective Date
References	Annex 2: ID 2.12, Service Provider Proposal Reference 2.2.5.2

Requirement 2.13

Requirement	Consumers can add/modify/remove a non-credit card payment option to their account in lieu of a credit card (e.g. debit cards, Apple Pay, Android Pay, Samsung Pay, PayPal, digital wallets, ability to carry balance, among others.)
Required Implementation Date	Apple Pay and Android Pay: Effective Date Additional Forms of Payment: When available
References	Annex 2: ID 2.13, Service Provider Proposal Reference 2.2.5.2

Requirement 2.14

Requirement	Consumers can add/modify/remove additional payments methods to MPP account (Credit Card or non-Credit Card). This will result in multiple payment options stored on one MPP account.
Required Implementation	Effective Date

Date	
References	Annex 2: ID 2.14, Service Provider Proposal Reference 2.2.5.2

Requirement 2.15

Requirement	Consumers can add/modify/remove email address to MPP account for reporting and other messaging related to the MPP system.
Required Implementation Date	Effective Date
References	Annex 2: ID 2.15, Service Provider Proposal Reference 2.2.5.3

Requirement 2.16A

Requirement	-Using their MPP account, Consumers can purchase a Parking Session using license plate, MPP ID, and valid payment information according to the metered space/zone's parking rate -The time period to be purchased should be in accordance with any parking rules and regulations for the metered parking space/zone -Prior to finalizing a purchase, the details (location, MPP ID, time, cost, warning messages) of the Parking Session should be clear to the Consumer
Required Implementation Date	Effective Date
References	Service Provider Proposal Reference 2.2.6

Requirement 2.16B

Requirement	On the vehicle confirmation screen, Consumers will be able click on at least the "Vehicle" and "Location" field to adjust the field. Sample confirmation screen:

Required Implementation Date	To be determined.
References	Service Provider Proposal Reference 2.2.6
Specific Training Required	Yes - Include in Training Plan (New features)
Specific Testing Required	Yes - Successful Testing and sign-off by City required prior to implementation

Requirement 2.17

Requirement	-The Mobile App will not allow Consumers to purchase more time than indicated by the Maximum Stay regulations -If a Consumer attempts to purchase more time than the Maximum Stay, the Mobile App will provide guidance to the Consumer on what the issue is and how to proceed It is expected that this functionality be presented to Consumers similar to the following screenshots:

Required Implementation Date	Effective Date
References	Annex 2: ID 2.17, Service Provider Proposal Reference 2.2.6

Requirement 2.18

Requirement	-The Mobile App will not allow Consumers to purchase a time period that overlaps with the time period that the No Stopping regulations are in effect -In instances where Consumers attempt to purchase a time period that overlaps with the time period that the No Stopping regulations are in effect, the Mobile App will provide guidance to the Consumer on what the issue is and how to proceedIt is expected that this functionality be presented to Consumers similar to the following screenshots: An iterative design process with the supplier is required. The feature will be activated after design sign-off by the City. A detailed implementation schedule will be created by the Service Provider and signed-off by the City. Ensure that the experience using IVR is reviewed to ensure alignment of functionality and experience.
Required Implementation Date	Effective Date
References	Annex 2: ID 2.18, Service Provider Proposal Reference 2.2.6

Requirement 2.19

Requirement	-The Mobile App will not allow Consumers to park a plate specified as a regular vehicle in a designated motorcycle space -If a Consumer attempts to complete a Parking Session with a plate specified as a regular vehicle in a designated motorcycle space, the Mobile App will provide guidance to the Consumer on what the issue is and how to proceed It is expected that this functionality be presented to Consumers similar to the following screenshots An iterative design process with the supplier is required. The feature will be activated after design sign-off by the City. A detailed implementation schedule will be created by the Service Provider and signed-off by the City. Ensure that the experience using IVR is reviewed to ensure alignment of functionality and experience.
Required Implementation Date	Effective Date
References	Annex 2: ID 2.19, Service Provider Proposal Reference 2.2.6

Requirement 2.20

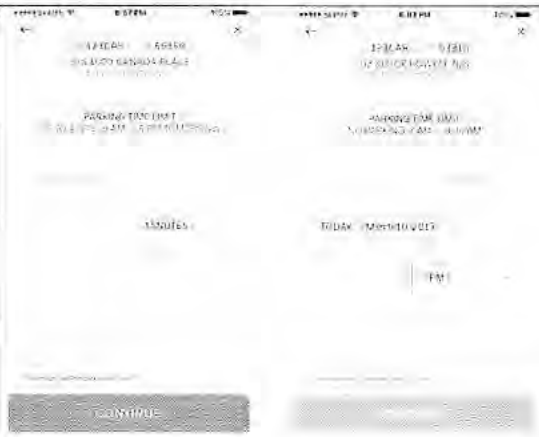
The requirement listed Annex 2: ID 2.20 in the RFP is not required as part of the Agreement.

Requirement 2.21

Requirement	The Solution should enable the City to control messaging (e.g. No Stopping Messaging) in the Mobile App It is expected that this functionality will be similar to the following screenshots: An iterative design process with the supplier is required. The feature will be activated after design sign-off by the City. A detailed implementation schedule will be created by the Service Provider and signed-off by the City. Ensure that the experience using IVR is reviewed to ensure alignment of functionality and experience. The response provided by the Service Provider for this requirement is now included in the requirement called City Messaging in the Value Add section.
Required Implementation Date	Effective Date+ 3 months
References	Annex 2: ID 2.21, Service Provider Proposal Reference 2.2.6

Requirement 2.22

Requirement	Pre-Pay: There are two scenarios that require Consumers to pay for parking in advance: 1. Consumers that park in the morning prior to pay parking coming into effect (e.g. a customer that arrives at 8 AM and wishes to pay for parking between 9 AM - 10:15 AM) 2. Consumers that park at a space in the evening should be able to pre-pay for parking for the next morning This feature will be implemented using "Park Until" functionality, similar to what is shown in the following screenshots:

	 An iterative design process with the supplier is required. The feature will be activated after design sign-off by the City. A detailed implementation schedule will be created by the Service Provider and signed-off by the City. Ensure that the experience using IVR is reviewed to ensure alignment of functionality and experience.
Required Implementation Date	Effective Date + 3 months
References	Service Provider Proposal Reference 2.2.6.4
Specific Training Required	Yes, include in Training Plan (New Features)
Specific Testing Required	Yes - Successful testing and sign-off by City required prior to implementation

Requirement 2.23

Requirement	-Without using an account, Consumers can purchase a Parking Session using license plate, MPP ID, and valid payment information according to the metered space/zone's parking rate -The time period to be purchased should be in accordance with any parking rules and regulations for the metered parking space/zone -Prior to finalizing a purchase, the details (location, MPP ID, time, cost, warning messages) of the Parking Session should be clear to the Consumer -The Mobile app may offer to create account post-Parking Session using information provided

	The City expects that this feature will operate similarly to the initial mock-ups provided in the Proposal as well as the additional screenshots provided here: Note that the geolocation services features shown in these screenshots are not part of this requirement. An iterative design process with the supplier is required. The feature will be activated after design sign-off by the City. A detailed implementation schedule will be created by the Service Provider and signed-off by the City.
Required Implementation Date	Effective Date + 3 months
References	Annex 2: ID 2.23, Service Provider Proposal Reference 2.2.6.5
Specific Training Required	Yes, include in Training Plan (New Features)
Specific Testing Required	Yes - Successful testing and sign-off by City required prior to implementation

Requirement 2.24

Requirement	The Mobile App will be able to direct the Consumer to a configurable URL (e.g. http://vancouver.ca/streets-transportation/pay-your-ticket.aspx) to allow paying for City issued parking tickets An iterative design process with the supplier is required. The feature will be activated after design sign-off by the City. A detailed implementation schedule will be created by the Service Provider and signed-off by the City.
Required Implementation Date	6 months after requested by the City
References	Annex 2: ID 2.24, Service Provider Proposal Reference 2.2.6.6

Requirement 2.25

Requirement	Using a device's GPS features, the Mobile App will automatically suggest the exact metered parking space/zone or a short list of metered parking spaces/zones to help the Consumer to complete a Parking Session faster and more accurately An iterative design process with the supplier is required. The feature will be activated after design sign-off by the City. A detailed implementation schedule will be created by the Service Provider and signed-off by the City.
Required Implementation Date	As requested by the City + 3 months
References	Annex 2: ID 2.26, Service Provider Proposal Reference 2.2.6.7
Specific Training Required	Yes, include in Training Plan (New Features)
Specific Testing Required	Yes - Successful testing and sign-off by City required prior to implementation

Requirement 2.26A

Requirement	- Vancouver is home to four distinct car sharing organizations (Modo, car2go, Evo, ZipCar) - For Consumers to pay for parking with a car share vehicle, the Mobile App will provide a user-friendly way to pay for a car sharing vehicle without having to manually enter the car sharing vehicle's plate This feature will be implemented by allowing by Consumers to select Car Share as a vehicle type similar to what is shown in the following screenshots: An iterative design process with the Service Provider is required. The feature will be activated after design sign-off by the City.

	A detailed implementation schedule will be created by the Service Provider and signed-off by the City.
Required Implementation Date	Effective Date
References	Annex 2: ID 2.26, Service Provider Proposal Reference 2.2.6.8
Specific Training Required	Yes, include in Training Plan (New Features)
Specific Testing Required	Yes - Successful testing and sign-off by City required prior to implementation

Requirement 2.26B

Requirement	The Mobile App will have the ability to add new vehicle types (e.g. EV Car) An iterative design process with the Service Provider is required. The feature will be activated after design sign-off by the City. A detailed implementation schedule will be created by the Service Provider and signed-off by the City.
Required Implementation Date	Effective Date
Specific Training Required	Yes, include in Training Plan (New Features)
Specific Testing Required	Yes - Successful testing and sign-off by City required prior to implementation

Requirement 2.27

Requirement	- Consumer will receive a reminder notification a set time period prior to the end of the their Parking Session - Mobile App push notifications are more desirable than text messages for this purpose - If more than one option available, the Consumer will be able to select their preference (or none)
Required Implementation Date	Effective Date
References	Annex 2: ID 2.27, Service Provider Proposal Reference 2.2.7.1

Requirement 2.28

Requirement	In instances when the end of a Consumer's Parking Session is close to a No Stopping regulation coming into effect, the Consumer will receive a reminder with messaging that informs them of this This feature will similar to what is shown in the following screenshots: An iterative design process with the Service Provider is required. The feature will be activated after design sign-off by the City. A detailed implementation schedule will be created by the Service Provider and signed-off by the City.
Required Implementation Date	Effective Date + 8 months
References	Annex 2: ID 2.28, Service Provider Proposal Reference 2.2.7.2
Specific Training Required	Yes, include in Training Plan (New Features)
Specific Testing Required	Yes - Successful testing and sign-off by City required prior to implementation

Requirement 2.29

Requirement	- Consumer will be able to extend the time purchased on an individual Parking Session - If conflicts with the Maximum Stay or No Stopping restrictions regulations are encountered, appropriate messages and guidance will be provided to the Consumer
Required Implementation Date	Effective Date
References	Annex 2: ID 2.29, Service Provider Proposal Reference 2.2.7.3

Requirement 2.30

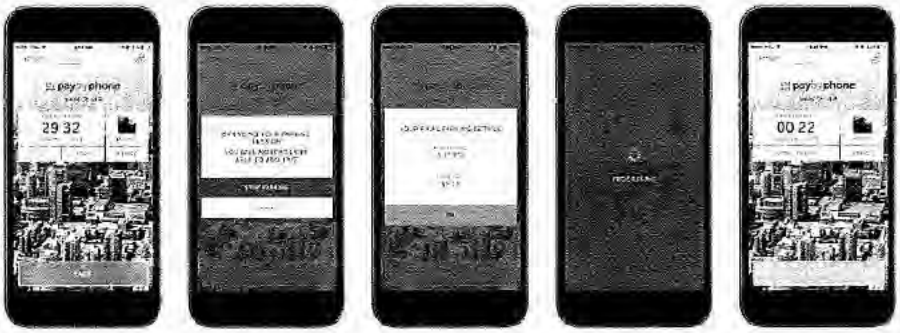
Requirement	Consumer will be able to extend Parking Sessions created using the IVR system

Required Implementation Date	Effective Date
References	Annex 2: ID 2.30, Service Provider Proposal Reference 2.2.7.3

Requirement 2.31

Requirement	Consumer will be able to see on the Mobile App how much time is remaining on their current Parking Session
Required Implementation Date	Effective Date
References	Annex 2: ID 2.31, Service Provider Proposal Reference 2.2.7.4

Requirement 2.32

Requirement	- Consumer will be able to end a Parking Session with time remaining and only pay for time that has elapsed. This would not be available for areas that require minimum amounts of time to be purchased. - Consumer will be able to end a Parking Session created using the IVR system This feature will similar to what is shown in the following screenshots:  This feature should be included in the Marketing Plan. An iterative design process with the Service Provider is required. The feature will be activated after design sign-off by the City. A detailed implementation schedule will be created by the Service Provider and signed-off by the City.
Required Implementation Date	1 month from when requested by the City
References	Annex 2: ID 2.32, Service Provider Proposal Reference 2.2.7.5
Specific	Yes, include in Training Plan (New Features)

Training Required	
Specific Testing Required	Yes - Successful testing and sign-off by City required prior to implementation

Requirement 2.33

Requirement	- If selected as an option for their account, the Consumer will receive a confirmation of the cost and duration of their Parking Session via one or more of the following options: 1. An email 2. A text message 3. A Mobile App notification - If more than one option available, the Consumer will be able to select their preference (or none)
Required Implementation Date	Effective Date
References	Annex 2: ID 2.33, Service Provider Proposal References 2.2.5.3 and 2.2.7.6

Requirement 2.34

Requirement	- Using the Mobile App, Consumers will be able to access history of all of their Parking Sessions that includes information such as location of a Parking Session, license plate used, amount paid, time purchased, start time (including Parking Session extensions) - Reporting will include some basic filtering capability (plate, date range, location) - Report will be exportable to other file formats (e.g. pdf, csv) - From the Service Provider's website, Consumer will be able to send a history of Parking Sessions to an email address
Required Implementation Date	Effective Date + 3 months
References	Annex 2: ID 2.34, Service Provider Proposal Reference 2.2.7.7

Requirement 2.35

Requirement	- The City's most common customer call to the 311 call centre is related to the use of the MPP System (such as resolving a ticket as a result of using a wrong license plate) - The Mobile App will provide some self-service help features to help

	mitigate these calls.
Required Implementation Date	Effective Date
References	Annex 2: ID 2.35, Service Provider Proposal Reference 2.2.7.8

Requirement 2.36

Requirement	Consumer will be able to report broken meter equipment to the City using the Mobile App
Required Implementation Date	6 months from when requested by the City
References	Annex 2: ID 2.36, Service Provider Proposal Reference 2.2.8.1
Specific Training Required	Yes, include in Training Plan (New Features)
Specific Testing Required	Yes - Successful testing and sign-off by City required prior to implementation

Requirement 2.37

Requirement	- All parking meters within the City are mapped with GIS coordinates - The Mobile App will present Consumers with an interface map showing the locations of metered parking spaces/zones and associated parking regulations and rates An iterative design process with the Service Provider is required. The feature will be activated after design sign-off by the City. A detailed implementation schedule will be created by the Service Provider and signed-off by the City.
Required Implementation Date	5 months after requested by the City
References	Annex 2: ID 2.37, Service Provider Proposal Reference 2.2.8.2
Specific Training Required	Yes, include in Training Plan (New Features)
Specific Testing Required	Yes - Successful testing and sign-off by City required prior to implementation

Requirement 2.38

Requirement	- For the functionality described in 2.37, the Mobile App will offer the ability to show historical parking availability by time of day

	- Although information is not currently available, the Mobile App will offer the ability to show real time parking availability - The City does not currently have sensors, but there may be the capability to infer parking availability based solely on MPP use in the future An iterative design process with the Service Provider is required. The feature will be activated after design sign-off by the City. A detailed implementation schedule will be created by the Service Provider and signed-off by the City.
Required Implementation Date	5 months after requested by the City
References	Annex 2: ID 2.38, Service Provider Proposal Reference 2.2.8.3

Requirement 2.39

Requirement	If a Consumer has a plate registered on their account that has been flagged for ticketing or towing by City PEOs (likely via the Parking Enforcement Platform), the Solution will notify the Consumer that this has occurred. An iterative design process with the Service Provider is required. The feature will be activated after design sign-off by the City. A detailed implementation schedule will be created by the Service Provider and signed-off by the City.
Required Implementation Date	7 months after requested by the City
References	Annex 2: ID 2.39, Service Provider Proposal Reference 2.2.8.4

Requirement 2.40

Requirement	Prior to paying for parking, the Mobile App will give Consumers the option of using their ABPR privileges (if applicable) or using what is available publically (e.g. a City worker entitled to free parking at meters while working but would not want to use this feature on a day off). The initial roll-out of ABPR will be with a small group (<200) of internal City employees and will not include an integration to POSSE. An iterative design process with the supplier is required. The feature will be activated after design sign-off by the City.

	A detailed implementation schedule will be created by the Service Provider and signed-off by the City.
Required Implementation Date	3 months from when requested by the City
References	Annex 2: ID 2.40; Service Provider Proposal Reference 2.1.19; Schedule A Part 1 2.2.4.1;
Specific Training Required	Yes - Include in Training Plan (New features)
Specific Testing Required	Yes - Successful testing and sign-off by City required prior to implementation

Requirement 2.41

Requirement	If the Consumer chooses to use their ABPR on their account, this functionality will meet the same requirements as listed in Requirement 2.16 but take into account the APBR overrides where applicable - For example, if the metered space/zone has a max stay of 2 hours, but the Consumer's ABPR allows for a Max Stay of 3 hours at this space, then the Consumer could stay for a maximum of 3 hours The initial roll-out of ABPR will be with a small group (<200) of internal City employees and will not include an integration to POSSE. An iterative design process with the supplier is required. The feature will be activated after design sign-off by the City. A detailed implementation schedule will be created by the Service Provider and signed-off by the City
Required Implementation Date	3 months from when requested by the City
References	Annex 2: ID 2.41; Service Provider Proposal Reference 2.1.19; Schedule A Part 1 2.2.4.1;
Specific Training Required	Yes - Include in Training Plan (New features)
Specific Testing Required	Yes - Successful testing and sign-off by City required prior to implementation

Requirement 2.42

Requirement	- If applicable, the Mobile App will not allow Consumers to purchase more time than indicated by the Maximum Stay regulations permitted by ABPR - If a Consumer attempts to purchase more time than the Maximum Stay permitted by ABPR privileges, the Mobile App will provide guidance to the Consumer on what the issue is and how to proceed The initial roll-out of ABPR will be with a small group (<200) of internal City employees and will not include an integration to POSSE. An iterative design process with the supplier is required. The feature will be activated after design sign-off by the City. A detailed implementation schedule will be created by the Service Provider and signed-off by the City.
Required Implementation Date	3 months from when requested by the City
References	Annex 2: ID 2.42; Service Provider Proposal Reference 2.1.19; Schedule A Part 1 2.2.4.1;
Specific Training Required	Yes - Include in Training Plan (New features)
Specific Testing Required	Yes - Successful testing and sign-off by City required prior to implementation

Requirement 2.43

Requirement	- Consumer's ABPR will allow some vehicles to park in No Stopping regulations (e.g. Registered Commercial vehicles could pay to park in marked Commercial Loading Zones) The initial roll-out of ABPR will be with a small group (<200) of internal City employees and will not include an integration to POSSE. An iterative design process with the supplier is required. The feature will be activated after design sign-off by the City. A detailed implementation schedule will be created by the Service Provider and signed-off by the City.
Required Implementation Date	3 months from when requested by the City
References	Annex 2: ID 2.43; Service Provider Proposal Reference 2.1.19;

	Schedule A Part 1 2.2.4.1;
Specific Training Required	Yes - Include in Training Plan (New features)
Specific Testing Required	Yes - Successful testing and sign-off by City required prior to implementation

Requirement 2.44

Requirement	-Consumers will have the option to link specific payment information to use of their ABPR features (e.g. a corporate credit card(or account that can be invoiced) is used for ABPR privileges, a private credit card is used for non-ABPR Parking Sessions) The initial roll-out of ABPR will be with a small group (<200) of internal City employees and will not include an integration to POSSE. An iterative design process with the supplier is required. The feature will be activated after design sign-off by the City. A detailed implementation schedule will be created by the Service Provider and signed-off by the City.
Required Implementation Date	3 months from when requested by the City
References	Annex 2: ID 2.44; Service Provider Proposal Reference 2.1.19; Schedule A Part 1 2.2.4.1;
Specific Training Required	Yes - Include in Training Plan (New features)
Specific Testing Required	Yes - Successful testing and sign-off by City required prior to implementation

Requirement 2.45

Requirement	- Using the Mobile App, Consumers with ABPR privileges will be able to access a history of all their Parking Sessions as listed in Requirement 2.34 including information on ABPR features utilized The initial roll-out of ABPR will be with a small group (<200) of internal City employees and will not include an integration to POSSE. An iterative design process with the supplier is required. The feature will be activated after design sign-off by the City. A detailed implementation schedule will be created by the Service Provider and signed-off by the City

Required Implementation Date	3 months from when requested by the City
References	Annex 2: ID 2.45; Service Provider Proposal Reference 2.1.19; Schedule A Part 1 2.2.4.1;
Specific Training Required	Yes - Include in Training Plan (New features)
Specific Testing Required	Yes - Successful testing and sign-off by City required prior to implementation

3.0 IVR

Requirement 3.1

Requirement	Consumers can create a secure MPP account for their exclusive use
Required Implementation Date	Effective Date
Proposal References	Service Provider Proposal Reference 2.3.2

Requirement 3.2, 3.3, 3.4, 3.5, 3.6

Requirement	-Consumers can add one or more licence plates (from all North American jurisdictions) -Consumers can specify vehicle type (e.g. regular vehicle or motorcycle) to each plate on MPP account -Consumers can add/modify/remove credit card information to their MPP account -Consumers can add/modify/remove additional payments methods to MPP account (Credit Card or non-Credit Card). This will result in multiple payment options stored on one MPP account.
Required Implementation Date	Effective Date
Proposal References	Service Provider Proposal Reference 2.3.2, 2.3.4, 2.3.5

Requirement 3.7, 3.8, 3.9, 3.10

Requirement	-Using their MPP account, Consumers can purchase a Parking Session using license plate, MPP ID, and valid payment information according to the metered space/zone's parking rate • The time period to be purchased should be in accordance with any parking rules and regulations for the metered parking space/zone • Prior to finalizing a purchase, the details (location, MPP ID, time, cost, warning messages) of the transaction should be clear to the Consumer -The IVR system will not allow Consumers to purchase more time than indicated by the Maximum Stay regulations • If a Consumer attempts to purchase more time than the

	Maximum Stay, the Mobile App will provide guidance to the Consumer on what the issue is and how to proceed -The Mobile App will not allow Consumers to purchase a time period that overlaps with the time period that the No Stopping regulations are in effect • In instances where Consumers attempt to purchase a time period that overlaps with the time period that the No Stopping regulations are in effect, the Mobile App will provide guidance to the Consumer on what the issue is and how to proceed -The IVR system will not allow Consumers to park a plate specified as a regular vehicle in a designated motorcycle space -If a Consumer attempts to complete a Parking Session with a plate specified as a regular vehicle in a designated motorcycle space, the Mobile App will provide guidance to the Consumer on what the issue is and how to proceed Note: If the City implements ABPR to the general public, then as per Service Provider Proposal Reference 2.3.9, the City will define how the requirement for designated motorcycle space will be implemented. The Service Provider has proposed a possible solution, and the City will work with the supplier to finalize what the best solution is at that time.
Required Implementation Date	Effective Date
Proposal References	Service Provider Proposal Reference 2.3.6, 2.3.7, 2.3.8, 2.3.9

Requirement 3.11

Requirement	For a Consumer's first Parking Session on a City street, they should be presented with a message that indicates: 1. The purpose for which the information is being collected 2. The legal authority for collecting it, and 3. The title, business address and business telephone number of an officer or employee who can answer questions about the collection
Required Implementation Date	Effective Date
Proposal References	Service Provider Proposal Reference 2.3.10

Requirement 3.12

Requirement	The Solution should enable the City to control messaging (e.g. No

	Stopping Messaging) for IVR system.
Required Implementation Date	Effective Date
Proposal References	Service Provider Proposal Reference 2.3.11

Requirement 3.13

Requirement	There are two scenarios that require Consumers to pay for parking in advance: 1. Consumers that park in the morning prior to pay parking coming into effect (e.g. a customer that arrives at 8 AM and wishes to pay for parking between 9 AM - 10:15 AM) 2. Consumers that park at a space in the evening should be able to pre-pay for parking for the next morning After requirement 2.22 (pre-pay for app/park until) is implemented, the Service Provider will review the Mobile App experience with the City and discuss the potential extension of the feature to the IVR System.
Required Implementation Date	Effective Date
Proposal References	Service Provider Proposal Reference 2.3.12

Requirement 3.14

The requirement listed in Annex 2: ID 3.14 in the RFP is not required as part of the Agreement.

Requirement 3.15

Requirement	Consumer should receive a text message a set time period prior to the end of the their Parking Sessions
Required Implementation Date	Effective Date
Proposal References	Service Provider Proposal Reference 2.3.14

Requirement 3.16

Requirement	In instances when the end of a Consumer's Parking Session is close to a No Stopping regulation coming into effect, the Consumer will receive a reminder with messaging that informs them of this
Required Implementation Date	Effective Date + 9 months
Proposal References	Service Provider Proposal Reference 2.3.14
Specific Training Required	Yes, include in Training Plan
Specific Testing Required	Yes - Successful UAT and sign-off by City required prior to implementation

Requirement 3.17, 3.18

Requirement	-Consumer will be able to extend the time purchased on an individual Parking Sessions • If conflicts with the Maximum Stay or No Stopping restrictions regulations are encountered, appropriate messages and guidance will be provided to the Consumer -Consumer will be able to extend Parking Sessions created using the Mobile App
Required Implementation Date	Effective Date
Proposal References	Service Provider Proposal Reference 2.3.15

Requirement 3.19

Requirement	If selected as an option for their account, the Consumer will receive a confirmation of the cost and duration of their Parking Sessions via one or more of the following options: 1. An email 2. A text message - If more than one option available, the Consumer will be able to select their preference (or none)
Required Implementation Date	Effective Date
Proposal References	Service Provider Proposal Reference 2.3.16

4.0 Reports

Requirement 4.1

Requirement	In general, the Solution reporting requirements will provide access to the underlying raw data, ideally via a direct feed on an on-demand frequency. For example, the underlying, directly-accessed raw data can be coupled with a data visualization / reporting layer (such as Business Objects, Tableau, QlikView). The Solution should support pulling of all required data into a data infrastructure of City's choice
Required Implementation Date	3 months from when requested by the City
Proposal References	Service Provider Proposal Reference 2.4.2
Specific Training Required	Yes - Include in Training Plan (New features)
Specific Testing Required	Yes - Successful testing and sign-off by City required prior to implementation

Requirement 4.2

Requirement	Specific User roles and audience permissions will need to be specified, including support for data level permissions (depending upon design). The Solution will enable reports to be allocated to specific levels of employee e.g. PEOB Supervisor, TE CSR, etc."
Required Implementation Date	Effective Date
Proposal References	Service Provider Proposal Reference 2.4.3
Specific Training Required	Yes - Include in Training Plan (New features)
Specific Testing Required	Yes - Successful testing and sign-off by City required prior to implementation

Requirement 4.3

Requirement	City should have unimpeded access to a user-friendly website or software for financial purposes. The following reports should be available for viewing and export/download in tabular (.xlsx and .csv) format: • Consumer contact information (phone number, email address,

<table>
<tr>
<td></td>
<td>plate, vehicle type)
• Individual Parking Session reports (i.e. reports that includes complete Parking Session details e.g. MPP ID, Meter ID, type of metered parking space, Street and block, pre-defined City areas, rate, transaction amount, start/end time, license plate, payment type, charge reference number, MPP type [App or IVR], type of transaction i.e. start/extension)
• Summary transaction reports e.g. daily, weekly, monthly or annual reports (which also allow for filtering such as by parking space or zone, block, pre-defined COV areas, rate, amount paid, license plate, time of day).

-The Service Provider will create and maintain a Data Dictionary that provides a description of all available metrics.

The following reports will be made available at no charge:
<table>
<tr><th>Report Name</th></tr>
<tr><td>Active member account detail - basic</td></tr>
<tr><td>COV - Accepted Transaction By Location</td></tr>
<tr><td>COV - Accepted Transaction Summary Report</td></tr>
<tr><td>COV - Business Account Summary</td></tr>
<tr><td>COV - Deposit Report</td></tr>
<tr><td>COV - Individual Transaction Report</td></tr>
<tr><td>COV - Meter Transactions Deposit Report</td></tr>
<tr><td>COV - Promotions Detail</td></tr>
<tr><td>COV - Promotions Summary</td></tr>
<tr><td>Individual Transaction Report</td></tr>
<tr><td>Parking Credits</td></tr>
<tr><td>Refunds By Account - All Accounts</td></tr>
<tr><td>USAGE - Signups By Method, Date Range</td></tr>
<tr><td>Credits By Account In Past Year</td></tr>
<tr><td>Credits By Initiating Account</td></tr>
<tr><td>Customer Call Log (fast, last month)</td></tr>
<tr><td>Customer Call Log (with older data)</td></tr>
<tr><td>Customer Call Log Simple (Last 3 Months)</td></tr>
<tr><td>Customer Call Log Simple (Last 6 Months)</td></tr>
<tr><td>Lookup CoV Meter From Verrus Loc</td></tr>
<tr><td>Lookup Verrus Loc From CoV Meter</td></tr>
<tr><td>Mobile App User Session Log - (LIVE)</td></tr>
<tr><td>Mobile Web User Session Log - (LIVE)</td></tr>
<tr><td>Parking accounts by Vendor</td></tr>
<tr><td>Parking History By Account</td></tr>
<tr><td>Parking History By CoV Meter #</td></tr>
<tr><td>Parking History By Plate</td></tr>
<tr><td>Parking History By Verrus Location</td></tr>
<tr><td>Refunds by Account</td></tr>
</table>
</td>
</tr>
<tr>
<td>Required Implementation Date</td>
<td>Effective Date</td>
</tr>
<tr>
<td>Proposal References</td>
<td>Service Provider Proposal Reference 2.4.4</td>
</tr>
</table>

Specific Training Required	Yes - Include in Training Plan (New features)
Specific Testing Required	Yes - Successful testing and sign-off by City required prior to implementation

Requirement 4.4

Require	City should have unimpeded access to a user-friendly website or software for customer service purposes. The following reports should be available for viewing and for export/download in tabular (.xlsx or .csv) format: • Consumer Parking Session reports (i.e. Consumer's Parking Session history) e.g. history of dates, times, space location (Meter ID /MPP ID), Parking Session amount, type of transaction (initial / extension), payment type, last four digit of credit card, parking time credits & refunds. • IVR Transaction Log Report • Mobile App Transaction Log Report These reports can be generated by querying phone number, email address, license plate or last four digits of a credit card.
Required Implementation Date	Effective Date
Proposal References	Service Provider Proposal Reference 2.4.5
Specific Training Required	Yes - Include in Training Plan (New features)
Specific Testing Required	Yes - Successful testing and sign-off by City required prior to implementation

Requirement 4.5

Requirement	City should have access to a user-friendly website or software to view reports online to evaluate: • parking usage and revenue patterns • program performance • Reports would summarize results in tables and/or graphs, and if applicable, results can be visually displayed on a map interface. Example of these summary reports may include statistics on: • Parking activity (revenue and paid occupancy) by metered space/block/area • Parking duration by metered space/block/area • Time of day parking activity by metered space/block/area

	• Number of new Consumer Parking Sessions per month • Number of Parking session per Consumer per month • Value ($) and duration (min) of initial/extension Transaction per month • MPP Solution outages (MPP mobile App, IVR system) The reports should allow for selection, either from a list (space, block, pre-defined City areas, rate, amount paid, MPP type, ABPR user group) or by using an interactive map where geofences (areas of concern, analysis areas) can be defined in variety of methods (e.g. import a GIS file, manually created). These summary reports should be available for export in tabular (.xlsx and .csv) and/or PDF format." The Service Provider will create and maintain a Data Dictionary that provides a description of all available metrics. The following reports will be made available at no charge:
Required Implementation	Effective Date

Report Name
Active member account detail - basic
COV - Accepted Transaction By Location
COV - Accepted Transaction Summary Report
COV - Business Account Summary
COV - Deposit Report
COV - Individual Transaction Report
COV - Meter Transactions Deposit Report
COV - Promotions Detail
COV - Promotions Summary
Individual Transaction Report
Parking Credits
Refunds By Account - All Accounts
USAGE - Signups By Method, Date Range
Credits By Account In Past Year
Credits By Initiating Account
Customer Call Log (fast, last month)
Customer Call Log (with older data)
Customer Call Log Simple (Last 3 Months)
Customer Call Log Simple (Last 6 Months)
Lookup CoV Meter From Verrus Loc
Lookup Verrus Loc From CoV Meter
Mobile App User Session Log - (LIVE)
Mobile Web User Session Log - (LIVE)
Parking accounts by Vendor
Parking History By Account
Parking History By CoV Meter #
Parking History By Plate
Parking History By Verrus Location
Refunds by Account

Date	
Proposal References	Service Provider Proposal Reference 2.4.6
Specific Training Required	Yes - Include in Training Plan (New features)
Specific Testing Required	Yes - Successful testing and sign-off by City required prior to implementation

Requirement 4.6

Requirement	The Solution should allow organizations with multiple subordinates with ABPR to see reports on how ABPR is being used via a user-friendly website or software. Reports will automatically include appropriate ABPR details when ABPR is implemented as per requirement 1.18
Required Implementation Date	Within one (1) month of the adaptation of the start of ABPR services.
Proposal References	Service Provider Proposal Reference 2.4.7
Specific Training Required	Yes - Include in Training Plan (New features)
Specific Testing Required	Yes - Successful testing and sign-off by City required prior to implementation

Requirement 4.7

Requirement	The Solution has query logic to support ad-hoc reports. For example, create a mechanism that allows a User to create a 'Custom report' using predefined fields that are being searched for in a specific way (query). To the extent reports cannot be modified by the User, the Service Provider shall develop up to 15 additional, non-standard reports at no extra cost to the City during the term of the Agreement. Timing of the reports' development will be dependent on the complexity of the request and will be mutually agreed upon between the City and the Service Provider.
Required Implementation Date	3 months from when requested by the City
Proposal References	Service Provider Proposal Reference 2.4.8
Specific Training	Yes - Include in Training Plan (New features)

Required	
Specific Testing Required	Yes - Successful testing and sign-off by City required prior to implementation

Requirement 4.8

Requirement	Reports can be run on-demand or saved and run on a schedule (date/time or daily/weekly/monthly, etc.) with output type and destination to be specified by the City
Required Implementation Date	Effective Date.
Proposal References	Service Provider Proposal Reference 2.4.9
Specific Training Required	Yes - Include in Training Plan (New features)
Specific Testing Required	Yes - Successful testing and sign-off by City required prior to implementation

5.0 Customer Services

Requirement 5.1

Requirement	The Solution will enable the CSR to review a Consumer MPP account profile. The following attributes are required with this review: • Search / filter options • Capability to view all plates on the account • View current and historical Parking Session details (such as time, date, plate, MPP ID, payment details and duration) as listed in 4.4 Reporting - Customer Service Agent requirement • Display of last 4 digit of the current credit card info with expiry date
Required Implementation Date	Effective Date
Specific Training Required	Yes - Include in Training Plan (Refresher)
Proposal References	Service Provider Proposal Reference 2.5.2.1

Requirement 5.2

Requirement	The Solution will enable the CSR to add/update Consumer MPP account information. • Add/Edit credit card number & expiry date, plates and vehicle type • Modify PIN • Suspend account and/or delete account • View customer IVR access log, Mobile App access log and data communication • Capability to access user current Parking Session, and parking time credit report
Required Implementation Date	Effective Date
Specific Training Required	Yes - Include in Training Plan (Refresher)
Proposal References	Service Provider Proposal Reference 2.5.2.1

Requirement 5.3

Requirement	The Solution will enable the CSR (while assisting a Consumer) to search and view metered parking regulations and rates for a specific MPP ID or Meter ID
Required	Effective Date

Implementation Date	
Specific Training Required	Yes - Include in Training Plan (Refresher)
Proposal References	Service Provider Proposal Reference 2.5.2.2

Requirement 5.4

Requirement	The Solution should allow the City to customize web-site/software interface to accommodate CSRs workflow for assisting Consumers If requested by City, the Service Provider will elicit and document City requirements, then produce a scope of work that includes schedule and cost. The scope of work will require approval by the City before work commences.
Required Implementation Date	As requested by the City + 5 months
Proposal References	Service Provider Proposal Reference 2.5.3
Specific Training Required	Yes, include in Training Plan (New Features)
Specific Testing Required	Yes - Successful UAT and sign-off by City required prior to implementation

Requirement 5.5

Requirement	The Solution will allow the CSR to issue: • Parking time credit • Manually initiate a Parking Session
Required Implementation Date	Effective Date
Specific Training Required	Yes - Include in Training Plan (Refresher)
Proposal References	Service Provider Proposal Reference 2.5.4

Requirement 5.6, 5.7

Requirement	When a CSR issues a parking time credit or initiates a Parking Session on a Consumer's MPP account, the Solution will allow: • Entering an explanation comment for the parking credit/Parking Session (e.g. from a drop-down menu with

	"Broken Meter", "Incorrect MPP ID", etc. as selections) for recording purposes. • A CSR to view explanation comment (as described above) when viewing Parking Session history and/or parking time credit report When a CSR issues a parking time credit on a Consumer's MPP account, the Solution should allow the CSR to enter the time credit in either a time or dollar value If requested by City, the Service Provider will elicit and document City requirements, then produce a scope of work that includes schedule and cost. The scope of work will require approval by the City before work commences.
Required Implementation Date	As requested by the City + 5 months
Proposal References	Service Provider Proposal Reference 2.5.4
Specific Training Required	Yes, include in Training Plan (New Features)
Specific Testing Required	Yes - Successful UAT and sign-off by City required prior to implementation

Requirement 5.8

Requirement	The Solution will allow a PEOB Supervisor to perform the following: • To reverse a transaction (refund an existing transaction) • Capability to search a transaction by the last 4 digit of the credit card number
Required Implementation Date	Effective Date
Specific Training Required	Yes - Include in Training Plan (Refresher)
Proposal References	Service Provider Proposal Reference 2.5.5

Requirement 5.9

Requirement	At Effective Date, the City will use its 311 and Ticket Enquiry Centre CSR's to provide telephone and online customer service for the MPP system. However, should the City choose to change its model for providing this customer service, the Service Provider will provide it.

Required Implementation Date	As requested by the City + 1 months
Proposal References	Service Provider Proposal Reference 2.5.6
Specific Training Required	Yes, include in Training Plan (New Features)
Specific Testing Required	Yes - Successful UAT and sign-off by City required prior to implementation

6.0 Marketing and Transition Plan

Requirement	The successful Proponent will be required to create and execute a comprehensive Marketing and Transition Plan. Details of the expected content of the Plan can be found in Schedule A, Section 5.6. When the supplier releases a new feature that the City specifically requested or was one of the features listed in this Agreement, a City-approved marketing plan is required. When a new global feature that City did not specifically request or was not one of the features listed in this agreement is released, the Service Provider will develop a marketing plan. In such cases, the Service Provider will work collaboratively with the City and seek the City's comments on said marketing plan. Should the City decide to employ a multi-vendor environment during the period of this Agreement, the Service Provider is required to participate in the development of a City-led transition plan.
Required Implementation Date	Prior to the rollout of any new feature, the Service Provider will create a marketing plan for adoption of the new feature by users of the app.
References	Service Provider Proposal References: 2.6.1, 2.6.2

7.0 Training Requirements

Requirement	For New Features, Table 2 of Section 2.7.3 from original Service Provider Proposal does not apply. A new table outlining training features will be created as part of the Training Plan (Schedule A, Part 1, Section 5.2.1). For New Feature Training, the total number of hours required will be determined as part of the Training Plan. Any time a new feature is rolled-out, whether a global feature that City did not specifically request or one of the features listed in this agreement, training is required.
Required Implementation Date	Refresher Training: Within 12 months of Effective Date New Feature Training: Prior to each feature roll-out
References	Service Provider Proposal References: 2.7.1, 2.7.2, 2.7.3 , 2.7.4, 2.7.5

8.0 Reference

Requirement	The proposed Solution has been fully operational for a minimum of one year.

	The latest version of the proposed solution and functionality should currently be in production (for a period of at least 6 months); Prototypes or items in test production and not formally announced for market availability are to be flagged clearly with comments in the responses. Provide at least two (2) descriptions of where a system similar to the Solution has been implemented. For each description, provide a corresponding reference. Note: Solution is proven system
References	Service Provider Proposal Reference 2.8.2

9.0 Value Added Requirements

VA 1.0 Dashboards, Reporting, Data

Requirement VA1.1

Requirement	Provide at-a-glance metrics that show program performance, in a visualized, dashboard UI: "Standard Dashboard" at no additional cost. Service Provider will collaborate with the City, at no additional cost, to define the metrics displayed on the Standard Dashboard of their global product.
Required Implementation Date	Effective Date + 1 month
Specific Training Required	Yes, include in Training Plan (New Features)
Specific Testing Required	Yes - Successful testing and sign-off by City required prior to implementation

Requirement VA1.2

Requirement	Provide drill-down capability and data analysis with customizable visualizations in a dashboard-type UI: "Premium Dashboard"
Required	As requested by City + 3 months

Implementation Date	
Specific Training Required	Yes, include in Training Plan (New Features)
Specific Testing Required	Yes - Successful testing and sign-off by City required prior to implementation

Requirement VA1.3

Requirement	Service Provider will establish a methodology to deliver mutually-agreed upon User Journey data including sample User Journey data required App User Journey Data Sample List

USER JOURNEY	TYPES OF ANALYSIS
Apps downloaded	Over any specified time period
User Registration	• Time to complete by user • Drop-off screens/pages • Completed registrations (includes at least 1 vehicle and 1 payment method)
Add a New Vehicle	• Time to complete • Drop-off screen/page • Improperly entered license plates • Use of description field and its content • Entry screens/pages (there are a few ways to access this journey)
Parking Payment	• Time to complete a payment • Drop-off screen/page • Expired payment method (start of expiry to update)
My Account - Vehicle Management	• See 'Add a New Vehicle' journey
My Account - Payment Options	• Time to complete • Entry screens/pages • Use of camera features for details • Empty fields
My Account - Account Settings - Location Services	• Auto- or manual-setting • Value
My Account - Account Settings - Notification Services	• Email entered • Email receipts (on or off) • Special offers (on or off)

	My Account - Account Settings - Security Settings	• # of changes to password
	My Account - Help & Support - Email Support	• # of emails sent • Email subject
	My Account - Help & Support - Call the Helpline	• # calls initiated • # calls connected
	My Account - Help & Support - Submit Feedback	• # surveys started/finished • Response details
	My Account - Help & Support - Additional Info - FAQ	• # views • Time spent on screen
	My Account - Help & Support - Additional Info - T&C	• # views • Time spent on screen
Required Implementation Date	As requested by City + 3 months	
Specific Training Required	Yes, include in Training Plan (New Features)	
Specific Testing Required	Yes - Successful testing and sign-off by City required prior to implementation	

VA 2.0 City Messaging

Requirement VA2.1

Requirement	The Solution should enable the City to provide City-specific messaging to users on city-wide or specific zone-based basis. City should have ability to add message, set start and end time, add zone applied to. This requirement includes: City Driven Initiatives; Local Events; City-controlled location-based messages; Dynamic SMS (and traditional); and Local notifications and push The feature will be similar to the following screenshots:

	An iterative design process with the supplier is required. The feature will be activated after design sign-off by the City. A detailed implementation schedule will be created by the Service Provider and signed-off by the City.
Required Implementation Date	Effective Date + 6 months
References	Service Provider Proposal Reference 2.2.6
Specific Training Required	Yes, include in Training Plan (New Features)
Specific Testing Required	Yes - Successful UAT and sign-off by City required prior to implementation

Part 3 – Detailed Technical Requirements

1.0 IT Architecture

ID	Category	Associated Functionality within Proposed Solution	Mandatory/ Critical / Desirable / Optional
1.1	Scalable	The application is scalable and extensible to meet anticipated workload. The architecture will consider all scale metrics both current and future anticipated. Typical scalable and extensible solutions include: - Distributed deployment; - Powerful servers; - Fast networking components; and - Performance sensitive software design.	Critical
1.2	Open Architecture	The architecture will be open such that The City may access, augment, enhance, repurpose or extend the implemented systems for uses and applications as the City's needs evolve in the future.	Critical
1.3	Flexible	The architecture is not singularly focused on specific functionality, but will allow for growth, changing requirements, and simplicity of configuration.	Critical
1.4	Expandable	The Solution architecture supports expansion over time, both in terms of processing volume, as well as enhancements and new functionality.	Critical
1.5	Integratable	The architecture accommodates integration of new auxiliary devices, complementary systems, and management systems without causing unmanageable disruption.	Critical
1.6	Maintainable	Initial development is only a part of the system lifecycle; maintenance generally requires greater effort. To aid in this regard, the architecture needs to accommodate a simplified maintenance regime by having a clear and concise layout of components, responsibilities, and extension points.	Critical
1.7	High Performance Metrics	Performance is a constant concern for the architecture and redundancy will be built into the solution. Performance failures will cause Users to revert to paper-based procedures and systems.	Critical
1.8	Clear, Consistent, and Coherent Interfaces	The foundation of a solid implementation is rooted in the elegance of the interfaces. The overall architecture and design will lend itself to well placed, logical, intuitive interfaces.	Critical

1.9	Loose Coupling	Loose coupling allows one or more clients of the functions of the Solution to access a specific implementation of a software function without having to know the address or specifics of the implementation. Clients may include users or other software components in the Solution. Loose coupling is usually accomplished by implementing functions as software services (often a web service) and by registering the address of the current implementation of the service in a service registry. Loose coupling supports flexibility, expandability, maintainability and reuse.	Critical
1.10	Component based	The Solution will be designed as an interacting set of relatively granular software components. A component-based design facilitates software reuse and maintainability.	Critical
1.11	Convenience	Minimizing time, effort, and/or costs in the achievement of some tasks or goals.	Critical
1.12	Consistency & Ease of Use	Ease of use and consistency of application are key to ensuring productive system use by the Users.	Desirable
1.13	Trust & Security	Measures taken to protect the privacy and safety of citizens; to protect information and resources with respect to privacy, confidentiality, and integrity; to be seen and understood as doing the above. Ensures that: - Only authorized users/roles have access to view or modify documents based on their security profiles; - Sensitive information can be encrypted and be shared with appropriate controls; - Administrators can delegate access privileges to authorized users at the branch level; and - The system keeps an audit trail of all activity with reporting capabilities.	Desirable
1.14	Metadata Driven	A focus on collecting data about the business and items related to the parking business operations	Desirable

2.0 IT Standards

ID	Category	Associated Functionality within Proposed Solution	Mandatory/ Critical / Desirable / Optional
2.1	IT Standards	The Solution will provide for Database Failure/Corruption Recovery, i.e. off-site data storage and redundancy and fail over.	Critical
2.2	IT Standards	The Solution will allow for 3rd party reporting tools to pull data from the solution to satisfy unanticipated reporting requirements	Critical

2.3	IT Standards	Where applicable, the End-User Solution shall support either Google Chrome or Internet Explorer 11+ for the browser-based components of their solution.	Critical
2.4	IT Standards	The COV supports the following standards: - Java Message Service (JMS) API v1.0.2 - JavaScript Object Notation (JSON) (also - GeoJSON) - Extensible Markup Language (XML) v1.0 and related specifications (e.g., XML Namespaces, XML Signature, XML Encryption) - Representational State Transfer with a XML MIME (Multipurpose Internet Mail Extensions) type - Simple Object Access Protocol (SOAP) v1.1 and v1.2 - Web Services Description Language (WSDL) v1.1 and v2.0 - Web Services Security (WS-Security or WSS) – Username Token Profile v1.0 and X.509 Token Profile v1.0 - Hypertext Transfer Protocol (HTTP) v1.0 (IETF RFC 1945) and v1.1 (IETF RFC 2616) - Hypertext Transfer Protocol Secure (HTTPS), also known as HTTP over TLS (Transport Layer Security) (IETF RFC 2818) **The Service Provider's solution will integrate with COV applications using these standards.**	Desirable
2.5	IT Standards	Web-based interfaces will incorporate Responsive Web Design fundamentals	Desirable
2.6	Security	All information will be encrypted to acceptable security standards, both "at rest" and "in transit". The data includes personal information (such as license plate/license information) and financial information (such as payment information (credit/debit card info)).	Critical
2.7	Security	The Solution will monitor and log all security events. - The Solution will alert administrators of suspected security violations.	Critical
2.8	Security	Username/Password Management. Conforms to City security standards, preference for City AD domain authentication for internal accounts. If not using City domain authentication: a) Enforce periodic password changes (the City standard is every 60 days); b) Enforce a minimum password length (the City standard is 7 characters); c) Enforce requirement that passwords contain alpha and numeric characters and symbols; and d) Prevent assigning of a previously used password.	Critical
2.9	Security	Limit the system functionality available to the User based on their username/group association.	Critical

2.10	Security	The Service Provider will ensure that all security updates to the Solution, including, but not limited to, the application, operating solution, and databases are incorporated within 30 days of their release.	Critical
2.11	Security	All web services associated with the Solution will incorporate security, such as: - Web Services Security (WS-Security or WSS) – Username Token Profile v1.0 and X.509 Token Profile v1.0 - Hypertext Transfer Protocol Secure (HTTPS), also known as HTTP over TLS (Transport Layer Security) (IETF RFC 2818)	Desirable
2.12	User Security Profiles	The Solution will have the capability to have a robust security profile methodology.	Mandatory
2.13	Security	The Solution will restrict unauthorized viewing for financial data and financial reports.	Critical
2.14	Security	The Solution will include separate control over viewing and editing data via roles and security	Critical
2.15	Security	The Solution will lock a User account after a preset number of unsuccessful logon attempts	Critical
2.16	Security	The Solution will timeout a User after a preset time. Note: timeout will be in line with the City's security policies.	Critical
2.17	Security	Ability to restrict or prevent changes to specific data elements by role as provided by the City	Critical
2.18	Audit - City Staff	The Solution will provide audit logs of key events and when transaction logs are cleared, records when and by whom	Critical
2.19	PCI Compliance	The Solution is Payment Card Industry Data Security Standard V3.1 compliant. Please provide: 1) date of Attestation; and 2) targeted timelines associated with compliance against V3.2. **Refer to Schedule G - PCI DSS 3.2 Management Responsibility Matrix Between PayByPhone and City of Vancouver.**	Mandatory
2.20	Coordinate System	The Solution will have the capability to associate the location of an inquiry to a geographic point location which can then be displayed in an industry acceptable G.I.S format; either: 1) Universal Transvers Mercator coordinate system - zone 10 (referenced in meters X,Y) with a North American Datumn 1983 (NAD 83)* OR 2) Geographic coordinate system (Latitude, Longitude) with a North American Datumn 1983 (NAD 83)* *Not NAD 83 (CSRS) Note: All City meters have been surveyed to the nearest cm.	Desirable

2.21	System	The Solution will synchronize its server clock no less than two times per day to the NTP.org time protocol or the City's server time protocol. During any given 30 day period, the server time will deviate no more than two seconds from the source for 99.5% of the time and will not deviate more than 30 seconds from the source at any time.	Critical

3.0 Support

ID	Category	Associated Functionality within Proposed Solution	Mandatory/ Critical / Desirable / Optional
3.1	Standard SLA	The City will have expectations for a very robust SLA agreement and this will be reviewed as part of the final selection criteria. Do you have a standard SLA? See Schedule I – Service Level Agreement	Critical
3.2	Ongoing Maintenance & Support	The Service Provider will provide recurring application maintenance support for the Solution such as Mobile Apps, End-User Interface, Administration tools, Reporting and Database for the term of the Agreement.	Critical
3.3	3rd Party Service Maintenance	For any 3rd party services used by the Service Provider to deliver the Solution to the City, the Service Provider will ensure the availability of these services is maintained to meet all the availability requirements described in this Part 3 – Detailed Technical Requirements.	Critical
3.4	Maintenance Deliverables	Please refer to Part 1 – General Requirements, section 6 for the details of the required deliverable. Please outline any exceptions to the required list in the Comments column.	Critical
3.5	Payment Test & Maintenance	The Solution will provide means for the City staff to perform test transactions by using mobile application, mobile web and IVR (Interactive Voice Recognition) system. Such transactions will be recorded differently to identify test transactions. All of the test payments will be communicated but not affect any of the monthly revenue totals and transaction totals.	Desirable

4.0 Integration

ID	Category	Associated Functionality within Proposed Solution	Mandatory/ Critical / Desirable / Optional
4.1	Middleware Standards	In general, all integration from/to the Solution will be real time with the use of BizTalk middleware unless otherwise stated. The City requires that web services (API) be the general method of integration. Refer to Appendix B - Integration Current & Future State Diagram. - Integration State Diagram Refer to Appendix C - Integration Details. - Integration Details	Critical
4.2	Parking Enforcement Platform Integration	The City is currently transitioning from Ticket Manager to GTechna's Parking Enforcement Platform. The Solution will provide the capability for users to verify mobile payments based on license plate, MPP ID, and vehicle type. Refer to Appendix B - Integration Current & Future State Diagram. - Integration State Diagram The solution architecture will push both payment information and the interaction with the Parking Enforcement Platform. Integration with the existing TicketManager system is to remain as per existing rules (pull/query). Integration will be provided with the City's new Gtechna platform as per a push methodology whereby all Parking Sessions captured by PayByPhone will be pushed to the Gtechna platform.	Critical
4.4	Connected Meter and Paystation Integration	The City currently has 17 Pay Stations that transmit approximately 30,000 annual transactions to the current MPP vendor to be made available for enforcement querying. The Solution will be required to complete this task. The Service Provider will provide the following integrations at no cost: Integration with Cale and MacKay paystations Integration with Parking Enforcement systems: both TicketManager and Gtechna. The solution architecture will push both payment information and the interaction with	Critical

		the Parking Enforcement Platform. Integration with the existing TicketManager system is to remain as per existing rules (pull/query). Integration will be provided with the City's new Gtechna platform as per a push methodology whereby all Parking Sessions captured by PayByPhone will be pushed to the Gtechna platform. Refer to Appendix B - Integration Current & Future State Diagram. – Integration State Diagram	
4.5	Account Based Parking Rules Database	In order to manage access to Account based Parking Rules (ABPR), it is anticipated that a database of Consumers will be maintained by City staff. This database could be cloud-hosted by the Service Provider or part of the City's parking permit database. As the City's parking permit database is not yet configured for ABPR, in the short term the City may wish to provide ABPR Consumer information manually, and periodically by providing .csv files or equivalent. In the long-term, the Solution will either host the ABPR database in the cloud (with access available via website or software) or integrate into the City's fully developed hosted permit database.	Desirable

5.0 Data Management

ID	Category	Associated Functionality within Proposed Solution	Mandatory/ Critical / Desirable / Optional
5.1	Data Performance	Solution will support data reporting and queries without affecting the performance of the core solution (e.g. via indexing and a separate reporting warehouse).	Critical
5.2	Data Transactions	The Solution will have the ability to support the anticipated transaction volume and number of mobile app Consumers and allow for future growth. Current volume is approx. 12 million transactions a year, and growing rapidly. Refer to Appendix C in RFP (Schedule E - RFP Appendix	Critical

		C)- Gross Revenue and Transactions.	
5.3	Data Transactions	There are approximately 30,000 pay station transactions per year (in addition to mobile payment transactions). Solution will be required to host/store paystation transaction data.	Critical
5.4	Data Availability	The Solution will allow reporting on historical Consumer activity and transactions. Historical data should be available for 7 years.	Critical
5.5	Data Availability	All data collected will be readily available (for searching, display, reporting, etc.), for at least 72 months in a production system environment.	Critical
5.6	Data Availability	The Solution will support pulling of all required data into a data infrastructure of the City's choice as needed without further cost. Data Services: a. Provisioning of APIs i. Service Provider will provide documentation for City and/or City's vendors to set up endpoints for Service Provider Data Services ii. Service Provider will work with City to establish a methodology to deliver mutually agreed upon User Journey data b. Frequency of data pushes i. Transactional data pushes will be done in real-time, with no set limit to data volume ii. Enforcement data pushes will be done in real-time, as Parking Sessions are created iii. Bulk data exports will be done at regular intervals, or ad-hoc (2-4 week lead time required), as required by City c. Data transfer limits i. All transactions will be sent, without set limit, when Service Provider sends transactions to a data warehouse d. Access to data i. Service Provider will retain a minimum of 24 months of real-time data in direct access ii. Older data can be requested by City as a bulk data export (2-4 week lead time required) e. New data points i. Service Provider will ensure new transactional data points will be added automatically to the systems used by City ii. At City's request, Service Provider will add other data points (e.g. GIS data) as	Critical

		part of Service Provider's regular release cycles f. Transaction level data i. Will include a consistent 'profile id' (currently Member_uid) ii. Service Provider will support City with City's data warehouse data model, as required g. Data classified by City as personal information will be provided in an unaltered state, unless: i. Its provision would violate City's terms of service or put City in breach of existing legal and/or compliance-related regulations; or ii. City requests (through a pre-arranged and agreed upon mechanism for customized data provisioning services) an alteration to specific data as part of personal information h. Custom data provisioning services - details i. Lead time: 2-6 weeks lead time required, depending on complexity of the requirement ii. Requirements process: a. Service Provider's Product Manager collaborates with City to develop requirements b. Service Provider's team will provide sizing and sequencing c. Service Provider will review with City iii. Development and testing processes: a. Service Provider will add requirements to Service Provider's prioritized backlog for development, then executed b. Service Provider will perform internal testing prior to deploying updates (internal testing may be done in conjunction with UAT) iv. New templates: Service Provider will use a set of templates as a starting point for each type of integration, and if a new template is required for an integration, Service Provider may add it to Service Provider's inventory if it may be used by other Consumers i. Data - details i. Service Provider will supply data by individual transaction/event, in a summary, or both ii. Application usage reporting, see sample list below iii. Data provided by Service Provider to City may be used by City: standalone; or combined with other data: a. as part of City's current and future Open Data platforms and initiatives; b. in revenue-generating or cost-	

		reducing initiatives (either wholly-owned by City, or in partnerships, at the sole discretion of City) j. Data Services i. Service Provider platform will publish 'events' for every transaction performed by a Consumer ii. Each 'event' (e.g. 'parking quote created', 'Parking Session created') will have multiple data elements iii. Events and data elements can be published to City's data warehouse in real-time iv. Publishing via Service Provider's Data Delivery Service (refer to Schedule P), which will be extensively monitored and hardened v. Service Provider will work with City to determine which events and data elements are required for data warehouse	
5.7	Data Quality	The Solution will guarantee the quality, delivery, accuracy and validity of the data it captures, transmits and stores.	Critical

6.0 Cloud

ID	Category	Associated Functionality within Proposed Solution	Mandatory/ Critical / Desirable / Optional
6.1	Cloud Based	The Solution is a Canadian cloud hosted option.	Critical
6.2	Cloud based	All data centres are hosted in Canada.	Critical
6.3	Canada Security and Privacy Policy Compliance	The Service Provider will comply with all Canadian security and privacy policies. i. BC's Personal Information Protection Act, SBC 2003 c. 36 ii. Federal Personal Information Protection and Electronic Documents Act, SC 2000 c 5 iii. Freedom of Information and Protection of Privacy Act, RSBC 1996, c 165 (FIPPA)	Critical

6.4	Solution Availability	The Service Provider will provide detailed availability data for the Solution (for the entire service not individual servers): - Mean Time To Failure (MTTF): How long it takes before service delivery is interrupted - Mean Time To Recover (MTTR): How long it takes to recover from a complete service outage back to normal operations - Average Transaction processing speed (in seconds) - Average number of transactions supported (per hour) - Web page delivery times (in seconds) - Average query response times (in seconds)	Desirable
6.5	Performance and Service	The Solution will meet or exceed the criteria provided in Section 3.1 (Standard SLA) and Section 6.4 given the anticipated usage.	Critical
6.6	Solution Availability	All system functionality will be available to City Users 24 hrs per day, 365 days per year (note: exception(s) to be made for scheduled updates and system maintenance, as agreed upon under a Service Level Agreement). Note: the operating hours of Parking Operations & Enforcement Branch are 6am-12am PST.	Critical
6.7	Solution Test Environment	The Solution provides a test environment for implementation and on-going support	Critical

Part 4 – Implementation Schedule

As per Schedule A - Part 1, Section 2.11 of this agreement, a detailed Project Implementation Plan & Schedule (PIPS) will be provided "within fifteen (15) business days of the City's written notification of contract award to the Service Provider".

SCHEDULE B - ADDITIONAL SECURITY AND PRIVACY REQUIREMENTS

The Service Provider shall comply with the following terms and conditions relating to data security and compliance with applicable privacy legislation in respect of any personal information acquired or accessed by the Service Provider in connection with the Agreement.

1.0 GENERAL

1.1 **Acknowledgment:** The Service Provider acknowledges that under this Agreement, it will acquire or have access to "personal information" as such term is defined in FOIPPA. The Service Provider further acknowledges that both the City and the Service Provider have obligations under FOIPPA to protect such information and that any unauthorized disclosure or use of such information could result in irreparable and significant harm to the City.

1.2 **Privacy Legislation and Obligations**

(a) The City is subject to the provisions of FOIPPA which imposes significant obligations on the City and its contractors (including the Service Provider) to protect all personal information acquired from the City or obtained independently in the course of providing services to the City. The Service Provider confirms and acknowledges its obligations to comply with the provisions of FOIPPA. The Service Provider further confirms and acknowledges its obligations to comply with all other applicable laws relating to privacy and personal information including PIPA in relation to any personal information (as defined in such Act) to which the Service Provider has access under this Agreement.

(b) The Service Provider has implemented appropriate or will implement appropriate policies and security measures to comply with all applicable laws relating to privacy and personal information including FOIPPA and PIPA, as well as to comply with the terms of this Agreement.

(c) The Service Provider agrees that all personal information to which the Service Provider has access under this Agreement is "under the control" of the City for the purposes of FOIPPA. The City is only transferring physical custody of the personal information to the Service Provider, not control of that information, and the authority over the use, disclosure, access, destruction and integrity of the personal information remains with the City. At any time during the term of the Agreement, the City may exercise the foregoing control over the personal information by notice in writing to the Service Provider and the Service Provider shall comply with the instructions in the City's notice.

(d) If an access to information request is made to the Service Provider under applicable laws relating to privacy and personal information, the Service Provider shall (i) immediately, and in any event before responding to such information request, notify the City in writing of such request, and (ii) upon the City's request, provided the Service Provider is not prohibited by applicable laws from doing so, direct such information request to the City for the City to handle. In the case of (ii), the Service Provider shall, at the City's expense, deliver to the City copies of all relevant records within seven (7) days of notification by the City and shall comply with all other requests of the City.

(e) In the case of an access to information request made to the City, the Service Provider, at the City's expense, shall deliver to the City copies of all relevant records within seven (7) days of notification by the City and shall comply with all other requests of the City.

(f) All personal information and City information shall be treated as confidential and is supplied to the Service Provider only for the purpose of fulfilling the obligations under this Agreement. This obligation, along with all of the other provisions of this Schedule B, shall survive the expiry or termination of this Agreement. No personal information and City information shall be disclosed unless the Service Provider is legally compelled to do so and having first challenged that requirement and given the City an opportunity to challenge that requirement.

(g) The Service Provider shall not sub-contract any obligations to be performed by the Service Provider under the Agreement to any other party other than as permitted under the Agreement. If the City allows the Service Provider to engage a sub-contractor, the Service Provider shall ensure that any sub-contractor complies with all provisions of this document.

(h) Once the Service Provider possesses or has access to personal information and City information, such information will be stored and backed-up on servers and other equipment that are owned or controlled by the Service Provider and that are physically located in Canada. Physical access to the Service Provider's servers are locked and restricted to only the Service Provider employees and authorized agents. If the location of the Service Provider's primary or back-up servers change, the Service Provider will promptly notify the City in writing of the address of the new location. The Service Provider will not store any personal information or City information on any other server or equipment without the prior written approval of the City.

(i) Except with the prior written approval of or instructions from the City, the Service Provider shall not modify, add, delete, destroy, share, sell, transfer, match, mine, combine, manipulate or otherwise tamper with the personal information or City information in any way. For clarity, the foregoing restrictions do not apply to derivative works, created by the Service Provider that contain no personal information.

(j) The Service Provider shall not withhold any personal information or City information to enforce payment by the City or to enforce the Service Provider's rights in a dispute over this Agreement.

(k) As between the City and the Service Provider, the personal information and City information is owned by the City, and the Service Provider makes no claim to any right of ownership in it.

1.3 **Authorized Purposes:** The Service Provider may only use the personal information and City information to which the Service Provider has access under this Agreement to carry out the Service Provider's obligations under this Agreement and for no other purpose ("**Authorized Purposes**").

1.4 **Restricted Access**

(a) The Service Provider will permit access to personal information and City information only to those employees who need such access in order to carry out the Authorized Purposes (the "**Authorized Employees**"). The Service Provider will at all times maintain a current list of Authorized Employees. The Service Provider will, upon City's request, provide the City with the list of Authorized Employees.

(b) The Service Provider will at all times have in place a knowledgeable senior person within its organization to be responsible for, or, and to have the authority to ensure, compliance with the terms of this document (the "**Compliance Representative**"). The Compliance Representative will ensure that each Authorized Employee is aware of the terms of this Agreement, and to maintain proof, in writing, that the terms have been

explained and understood by each Authorized Employee. As of the Effective Date, the Service Provider hereby designates Barbara Hubert, the Service Provider's Privacy Officer - located at the Service Provider's office at the address given for the Service Provider on Page 1 of the Agreement, as the Compliance Representative. The Service Provider will promptly advise the City of any change to the Compliance Representative.

1.5 **Security:** The Service Provider will have appropriate physical, organizational, and technological security measures (consistent with best practices in the software industry) in place to ensure that all personal information and City information is collected, accessed, used, disclosed and destroyed only by Authorized Employees, including without limitation:

(a) restricted access to records containing paper copies of personal information and City information;

(b) restricted access to personal information and City information stored on computer systems and electronic storage devices and media, by using unique user IDs and passwords that are linked to identifiable Authorized Employees; and

(c) systems containing personal information and City information will be capable of providing an audit trail and user access logs, which logs will be retained by the Service Provider during the term of this Agreement and for at least two (2) years following its expiry, termination, or destruction of the personal information and City information.

(d) The Service Provider must ensure that the data centre and servers containing the personal information and City information meets the following physical and electronic security requirements:

(i) single point of entry;

(ii) access only to persons on the Service Provider approved access list;

(iii) log-in validation;

(iv) creation of accounts only as verified by the Service Provider;

(v) external or WIFI access to servers via encrypted means; and

(vi) servers running behind secure firewall.

1.6 **No Storage, Access or Transmission outside Canada; Limited Exception:**

(a) Subject to the exception set out in subsection 1.6(b) below, the Service Provider will not (i) store personal information and City information outside Canada, (ii) have personal information and City information accessible from outside Canada, (iii) transmit personal information and City information outside Canada, or (iv) otherwise permit any personal information and City information to leave Canada.

(b) Notwithstanding the above, the Service Provider is permitted under subsection 33.1(1)(p) of FOIPPA to disclose personal information outside of Canada strictly under the following limited circumstances:

(i) such disclosure is necessary for the Service Provider to provide the support services as contemplated under the Agreement;

(ii) such disclosure is limited to temporary access and storage by the Service Provider or its authorized contractor outside of Canada for the minimum time necessary for the purpose set out in (i);

(iii) once the purpose of disclosure is fulfilled, all applicable personal information accessed or retained by the Service Provider or its authorized contractor is irrevocably and permanently destroyed and deleted and, if requested by City, the Service Provider has certified the foregoing in writing (with the City having a right to audit or verify the foregoing, acting reasonably);

(iv) all processes and requirements requested by the City in respect of such disclosure (including, without limitation, how such disclosure will be made (e.g. through a dedicated VPN) , how such information will be accessed, whether such information may only be viewed outside Canada but not retained, etc.) have been complied with by the Service Provider;

(v) the Service Provider complies with all applicable laws outside Canada regarding the Service Provider's disclosure and handling of such information; and

(vi) upon request by the City, acting reasonably, the Service Provider cooperates in good faith in facilitating the audit or verification of the Service Provider's compliance with the foregoing by the City.

1.7 **Information Retention and Destruction:**

(a) **The Service Provider's Retention and Destruction:** The Service Provider is only permitted to retain personal information and City information or any records of personal information and City information in any form whatsoever (including without limitation hard copy or electronic formats) during the term of this Agreement and for one year after the end of the term. During this period of time, the Service Provider shall hold such personal information and City information in compliance with the security, privacy and confidentiality requirements of this Agreement. Upon the expiry of one year after the end of the term, the Service Provider will permanently and securely destroy the personal information and City information and all records thereof in a manner that is appropriate for the media so that the personal information and City information or any portion of it cannot be subsequently retrieved, accessed or used by the Service Provider or any other person. After the personal information and City information is destroyed, the Service Provider shall deliver a notice in writing (in form and substance satisfactory to the City) to the City confirming such destruction.

1.8 **Inspection and Compliance**

(a) During this Agreement and during the period of time that the Service Provider is permitted by this document to retain personal information and City information, the City's authorized representative may, on reasonable notice and during regular business hours, enter the Service Provider's premises and/or will be given access to the Service Provider's computer systems to inspect any personal information and City information in the possession of the Service Provider or any of the Service Provider's information management policies or practices relevant to its compliance with this Agreement.

(b) The City may request the Service Provider to provide a written certificate confirming the Service Provider's compliance with all obligations under this document, and if so requested, the Service Provider will within ten (10) business days either:

(i) provide such certificate; or

(ii) provide a notice of non-compliance in accordance with section 1.9.

(c) The Service Provider will promptly forward to the City any records that the City may request in order to review whether the Service Provider is complying with this Agreement.

(d) If requested by the City, acting reasonably, the Service Provider will appoint an independent, external auditor at the City's expense to review the Service Provider's information and security practices under this Agreement. the Service Provider will provide copies of the results of any such audit to the City within seven (7) days of receiving the auditor's report.

(e) The Service Provider will promptly and fully comply with any investigation, review, order or ruling of the Office of the Information and Privacy Commission (British Columbia) in connection with the personal information and City information.

1.9 **Written Notice of Non-Compliance.** The Service Provider will immediately notify the City in writing of any non-compliance or anticipated non-compliance with this document and will further inform the City of all steps the Service Provider proposes to take to address and prevent recurrence of such non-compliance or anticipated non-compliance.

1.10 **Survival:** The obligations in this Schedule B shall survive the expiration or earlier termination of this Agreement.

2.0 ADDITIONAL TERMS GOVERNING STORAGE AND ACCESS OF INFORMATION

2.1 The Service Provider shall, in respect of storage of, and access to, personal information and City information:

(a) take a physical inventory, at least annually, of all records containing personal information and City information, to identify any losses;

(b) ensure that records are not removed from storage premises without appropriate written authorization;

(c) use physically secure areas for the storage of records and restrict access to authorized personnel;

(d) ensure that access to documentation about computer systems that contain personal information and City information is restricted to authorized personnel;

(e) ensure that users of a system or network that processes personal information and City information are uniquely identified and that, before a user is given access to the system or personal information and City information, their identification is authenticated each time;

(f) implement procedures for identification and authentication, which include:

(i) controls for the issue, change, cancellation and audit-processing of user identifiers and authentication mechanisms;

(ii) ensuring that authentication codes or passwords:

(1) are generated, controlled and distributed so as to maintain the confidentiality and availability of the authentication code;

(2) are known only to the authorized user of the account;

(3) are pseudo-random in nature or vetted through a verification technique designed to counter triviality and repetition;

(4) are no fewer than 6 characters in length;

(5) are one-way encrypted;

(6) are excluded from unprotected automatic log-on processes; and

(7) are changed at irregular and frequent intervals at least semi-annually;

(g) maintain and implement formal procedures for terminated employees who have access to personal information and City information, with prompts to ensure revocation or retrieval of identity badges, keys, passwords and access rights;

(h) take reasonable security measures in respect of personal information and City information displayed on computer screens or in hardcopy form to prevent viewing or other access by unauthorized persons;

(i) implement automated or manual controls to prevent unauthorized copying, transmission or printing of personal information and City information; and

(j) implement control procedures to ensure the integrity of the personal information and City information being stored, notably its accuracy and completeness.

2.2 The Service Provider must store personal information and City information on agreed-upon media in accordance with prescribed techniques that store the personal information and City information in a form that only authorized persons may access. These techniques may include translating the personal information and City information into code (encryption) or shrinking or tightly packaging the personal information and City information into unreadable form (compression).

2.3 The Service Provider shall store backup copies of personal information and City information off-site under conditions which are the same as or better than originals.

2.4 The Service Provider shall securely segregate personal information and City information from information owned by others (including the Service Provider), including by installing access barriers to prevent information elements from being associated (including compared or linked, based on similar characteristics) with other information, including:

(a) separate storage facilities for personal information and City information;

(b) authorization before a person is granted access to computers containing such personal information and City information; and

(c) entry passwords and the employment of public key encryption/smart card technology where practicable.

2.5 The Service Provider shall ensure the integrity of personal information and City information stored, processed or transmitted through its system or network.

2.6 The Service Provider shall co-operate with, and assist in, any City investigation of a complaint that personal information and City information has been used or disclosed contrary to the terms of this Agreement, FOIPPA or any other applicable privacy or personal information laws.

2.7 As per section 1.8 of this Schedule B, the City shall be able to access the Service Provider's premises and other places where the Service Provider's servers and other equipment are located to recover any or all City records and personal information and City information and for auditing purposes to ensure compliance with the terms of this Agreement.

SCHEDULE C - INSURANCE CERTIFICATES

SCHEDULE D - CONTRACT PRICE

1.0 Parking Session Pricing (Mobile App and IVR)

Parking Session pricing is determined as follows:

(a) A rate of $0.05 per Parking Session for the Services and other obligations to be performed by the Service Provider under this Agreement at all times during the Term that the Service Provider is the only entity performing the Services or any part of the Services; or

(b) A rate of $0.06 per Parking Session for the Services and other obligations to be performed by the Service Provider under this Agreement at all times during the Term that an entity other than the Service Provider (the "Additional Proponent") is performing the Services or any part of the Services concurrently with the Service Provider.

Unless described in the proceeding Tables 2 and 3, all other capabilities described in Schedule A - Scope of Work are included in the above note Parking Session pricing.

1.1 Pricing for Optional Services

The City has identified several optional functional capabilities that are either available but not currently used by the City, or require customization to deliver. Pricing for these items is provided separately in tables 2 & 3, and is valid for the Term of the Agreement.

Table 2 - Recurring or Per Usage Pricing

Schedule A, Part 2 Requirement Reference	Feature	Price	Notes
1.16,1.21	Re-metering prevention from 3rd party systems – refer to Schedule S	$3,000/Month	Up to two integrations
1.18, 1.19	Account Based Parking Rules	$1.75/Active Eligibility/Month $500/Month minimum usage fee (if activated)	An "Active Eligibility includes the rights for a single licence plate to access a single set of account-based parking rules (called an "eligibility type")

VA2.1	City Messaging to end users	In-App Messages: $1000 setup + $0.050 per message sent SMS Messages: $1500 setup + $0.075 per message sent E-mail Messages: $1500 setup + $0.075 per message sent	During setup for each campaign, PayByPhone will work with the City to define a list of users who will receive the messages. Once the list of users is defined to the City's satisfaction, PayByPhone will provide the City with an estimate of the campaign cost for all of the City's desired communication modes and the City will have the ability to sign-off on the expected charges
2.6	Mobile app brand identity (Dynamic Labeling[1])	$2500/Image Change/Zone Zone set-up fee $500	The whole of Vancouver is considered a zone. If multiple zones use the same image, only one image change fee applies.
4.1	Direct feed - (Data Delivery Service)	$2,000/Month	Up to two integrations
4.1	Direct feed - (Data Delivery Service)	$500/ Month	Per additional integration
2.36	Broken Meter Reporting	$2,500/Month	
4.7	Ad-hoc reporting via 3rd party	$2,500/Month	Unlimited users + reports
4.7	Premium Dashboard + Ad-hoc Reports	$3,500/Month	Unlimited users + reports

[1]Dynamic labels do not include multiple language support; however, the notifications and City labels will be localized to the phone's language.

One Time Customization Fees

The following enhancements will be subject to time and materials pricing following a complete definition of functional and technical requirements in collaboration with the City.

Table 3 - One-Time Customization Fees

Ref.	Feature	CoV Rating	Est. Cost Range	Dependencies

2.5	Mobile App in other languages	Optional	$50k for the first language (i.e. one of Punjabi, Simplified Chinese, or Tradition al Chinese.) and $35k per additional language (i.e. $35k for each of the 2 remaining languages .)	Scope of language changes (i.e. apps, mobile web, consumer web, text messages, customer support)
2.38	Historical & real time parking availability in mobile app	Optional	$75-$250K+ operational costs	Cost dependent on availability prediction accuracy and granularity requirements that drive complexity of inference engine.
2.39, 2.24	Link to Citation Payments + Ticketing & Towing Notification	Optional	$50-$95K + operational fees	Dependent on desired system behavior and integration requirements.
4.7	Additional custom reports beyond 15 no cost reports.	Critical	$1-2K / report	Dependent on report complexity.
5.4	Customization of Consumer Service workflow in back office	Desirable	$10-20K	Dependent on specific scope of changes required.

1.2 Pricing for Telephone and Online Consumer Service for the General Public

The Service Provider operates a 24 hours per day, 7 days per week, 365 days per year Call Center with 54 agents providing support in English, French and Spanish. Should the City desire, the Service Provider will extend Call Center access to Drivers parking at City of Vancouver locations at pass-through cost (currently $0.50 CAD per minute).

Table 5 - Telephone Consumer Service for the General Public (Optional)

☐ Pass through cost. Currently at $0.50 CAD per minute.

1.3 Pricing for Other Services

Should the City wish to engage the Service Provider to build custom enhancements to the mobile parking payment solution, the rates in Table 6 shall apply.

Custom software development fees will apply only to those items outside the scope of Schedule A - Scope of Work, or those items identified herein as having customization fees associated with delivery.

Table 6 - Pricing for Other Items Not Identified in Schedule A - Scope of Work

Resource	Office Hours Rate (9AM – 5PM)[1]	After Hours Rate[1]
Senior Architect	$250	$315
Senior Product Manager	$250	$315
Creative Services	$200	$250
Project Manager	$200	$250
Programmer / Developer	$200	$250
Implementation Manager	$175	$225
Consumer Adoption Strategist	$150	$200
Application Trainer	$125	$150
Support Agent	$125	$150
Tester	$125	$150

[1]Rate per hour $ CAD

2.0 Credit Card Processing Fees

2.1 Credit Cards Processed by Moneris

While the solution can work with Moneris, it is not required. Should the City wish to use Moneris and have the Service Provider act as merchant of record, credit card fees will be passed through at cost, without markup.

Table 7 - Costs if Credit Cards Processed by Moneris (Optional)

☐ Provided at pass through costs for both acquirer and gateway fees.

2.2 Credit Cards and other Payment Methods Processed by the Service Provider's Preferred Service Provider, other than Moneris

The Service Provider can act as Merchant of Record for mobile payment transactions. All costs associated with credit card processing will be passed through to the City at cost, without markup.

Current rates are described in Table 8. These costs are subject to changes made by 3rd party acquiring banks and payment processing suppliers from time to time. The Service Provider will endeavor to find and use the most reliable and cost-effective options for payment processing.

Table 8 - Current Pass-Through Costs if Credit Cards Processed by the Service Provider's Preferred Service Provider, other than Moneris (Optional)

• Credit Card Acquirer Fee: the lowest rate available to the Service Provider without markup - currently averaging at 2.32% of purchase price and will decrease as soon as the Service Provider negotiates a lower rate. This will be settled on a monthly basis in Canadian dollars. • Credit Card Gateway Fee: the lowest rate available to the Service Provider without markup - currently at $0.022USD per Parking Session and will decrease as soon as the Service Provider negotiates a lower rate. This will be settled in Canadian Dollars using the Bank of Canada published month end exchange rate.

Immediately upon request from the City, the Service Provider will provide the City with documentary proof that the Service Provider has passed through to the City all costs associated with credit card processing at its cost without any mark-up.

SCHEDULE E - RFP

(incorporated by reference)

SCHEDULE F – SERVICE PROVIDER'S PROPOSAL

(incorporated by reference)

SCHEDULE G - PCI

1.0 PCI DSS 3.2 Management Responsibility Matrix Between the Service Provider and City of Vancouver

PCI DSS 3.2 Management Responsibility Matrix Between PayByPhone and City of Vancouver		
The purpose of this spreadsheet is to satisfy PCI DSS Requirement 12.8.5: Maintain information about which PCI DSS requirements are managed by each service provider, and which are managed by the entity.		This document is intended to meet the requirements for PCI DSS V3.2 Requirement 12.8.5 as it relates to the Mobile Parking Service provided by PayByPhone Technologies Inc. As such, the following list of controls and applicable responsibilities only apply to the security of cardholder data which is accepted by PayByPhone on behalf of City of Vancouver. This document does not apply to any cardholder data that City of Vancouver processes, stores, transmits, or otherwise uses for any other purpose, or on the behalf of any other entities.
Control / Requirement	**Responsibility**	**QSA Notes**
Requirement 1: Install and maintain a firewall configuration to protect cardholder data		The PayByPhone network is fully owned and operated by PayByPhone Technologies Inc. From the Mobile Applications to the backend processing and cardholder storage systems, PayByPhone is responsible for all logical controls. This includes the placement, configuration, maintenance, and security of all firewalls,

		routers, switches, IPSec tunnels, and wireless (GSM) connectivity. No cardholder data traverses the client network, taking all card numbers accepted by the SSPM system out of scope for the majority of controls.
1.1 Establish and implement firewall and router configuration standards that include the following:	*Service Provider	
1.1.1 A formal process for approving and testing all network connections and changes to the firewall and router configurations.	*Service Provider	
1.1.2 Current network diagram that identifies all connections between the cardholder data environment and other networks, including any wireless networks.	*Service Provider	
1.1.3 Current diagram that shows all cardholder data flows across systems and networks.	*Service Provider	
1.1.4 Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone.	*Service Provider	
1.1.5 Description of groups, roles, and responsibilities for management of network components.	*Service Provider	
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. *Examples of insecure services, protocols, or ports include but are not limited to FTP, Telnet, POP3, IMAP, and SNMP v1 and v2.*	*Service Provider	
1.1.7 Requirement to review firewall and router rule sets at least every six months.	*Service Provider	
1.2 Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder 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.*	*Service Provider	
1.2.1 Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic.	*Service Provider	
1.2.2 Secure and synchronize router configuration files.	*Service Provider	
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.	*Service Provider	
1.3 Prohibit direct public access between the Internet and any system component in the cardholder data environment.	*Service Provider	
1.3.1 Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.	*Service Provider	
1.3.2 Limit inbound Internet traffic to IP addresses within the DMZ.	*Service Provider	
1.3.3 Do not allow any direct connections inbound or outbound for traffic between the Internet and the cardholder data environment.	*Service Provider	
1.3.4 Implement anti-spoofing measures to detect and block forged source IP addresses from entering the network. (For example, block traffic originating from the Internet with an internal source address.)	*Service Provider	
1.3.5 Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet.	*Service Provider	

1.3.6 Implement stateful inspection, also known as dynamic packet filtering. (That is, only "established" connections are allowed into the network.)	*Service Provider	
1.3.7 Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks.	*Service Provider	
1.3.8 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.*	*Service Provider	
1.4 Install personal firewall software on any mobile and/or employee-owned devices that connect to the Internet when outside the network (for example, laptops used by employees), and which are also used to access the network. Firewall configurations include: - Specific configuration settings are defined for personal firewall software. - Personal firewall software is actively running. - Personal firewall software is not alterable by users of mobile and/or employee-owned devices.	*Service Provider	
1.5 Ensure that security policies and operational procedures for managing firewalls are documented, in use, and known to all affected parties.	*Service Provider	
Requirement 2: Do not use vendor-supplied defaults far system passwords and other security parameters		PayByPhone operates a global Software as a Service platform. The physical infrastructure which powers the platform is maintained and managed by PayByPhone technical teams. Each new Parking Operator onboarded to PayByPhone receives unique access to the system.
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.).*	*Service Provider	
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.	*Service Provider	
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).	*Service Provider	
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 will be implemented on separate servers.) *Note: Where virtualization technologies are in use, implement only one primary function per virtual system component.*	*Service Provider	

2.2.2 Enable only necessary services, protocols, daemons, etc., as required for the function of the system.	*Service Provider	
2.2.3 Implement additional security features for any required services, protocols, or daemons that are considered to be insecure—for example, use secured technologies such as SSH, S-FTP, TLS, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP,etc.	*Service Provider	
2.2.4 Configure system security parameters to prevent misuse.	*Service Provider	
2.2.5 Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.	*Service Provider	
2.3 Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or TLS for web-based management and other non-console administrative access.	*Service Provider	
2.4 Maintain an inventory of system components that are in scope for PCI DSS.	*Service Provider	
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.	*Service Provider	
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 - Parking Regulations and Rates: Additional PCI DSS Requirements for Shared Hosting Providers.*	*Service Provider	
Requirement 3: Protect stored cardholder data		PayByPhone accepts all card numbers on behalf of clients. As such, no PAN data ever traverses client-owned networks or systems.
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, 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.	*Service Provider	
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 securely.* *Sensitive authentication data includes the data as cited in the following Requirements 3.2.1 through 3.2.3:*	*Service Provider	
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 magneticstripe data *Note: In the normal course of business, the 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.*	*Service Provider	
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.	*Service Provider	

3.2.3Do not store the personal identification number (PIN) or the encrypted PIN block after authorization.	*Service Provider
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 the full 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.*	*Service Provider
3.4 Render PAN unreadable anywhere it is stored (including on portable digital media, backup 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 will be in place to ensure that the hashed and truncated versions cannot be correlated to reconstruct the original PAN.*	*Service Provider
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.	*Service Provider
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.*	*Service Provider
3.5.1 Restrict access to cryptographic keys to the fewest number of custodians necessary.	*Service Provider
3.5.2 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 - Within a secure cryptographic device (such as a 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.	*Service Provider
3.5.3 Store cryptographic keys in the fewest possible locations.	*Service Provider
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.*	*Service Provider
3.6.1 Generation of strong cryptographic keys	*Service Provider
3.6.2 Secure cryptographic key distribution	*Service Provider
3.6.3 Secure cryptographic key storage	*Service Provider

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 vendor or key owner, and based on industry best practices and guidelines (for example, NIST Special Publication 800-57).	*Service Provider	
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 will only be used for decryption/verification purposes.*	*Service Provider	
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.*	*Service Provider	
3.6.7 Prevention of unauthorized substitution of cryptographic keys.	*Service Provider	
3.6.8 Requirement for cryptographic key custodians to formally acknowledge that they understand and accept their key-custodian responsibilities.	*Service Provider	
3.7 Ensure that security policies and operational procedures for protecting stored cardholder data are documented, in use, and known to all affected parties.	*Service Provider	
Requirement 4: Encrypt transmission of cardholder data across open, public networks		The PayByPhone network is fully owned and operated by PayByPhone Technologies Inc. All card numbers in transit are protected by strong cryptography to processing systems.
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. *Exomples 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.*	*Service Provider	
4.1.1 Ensure wireless networks transmitting cardholder data or connected to the cardholder data environment, use industry best practices (for example, IEEE 802.11i) to implement strong encryption for authentication and transmission. *Note: The use of WEP as a security control is prohibited.*	*Service Provider	
4.2 Never send unprotected PANs by end-user messaging technologies (for example, e-mail, instant messaging, sms, chat, etc.).	*Service Provider	
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.	*Service Provider	
Requirement 5: Use and regularly update anti-virus software or programs		PayByPhone maintains and monitors all anti-virus software/programs and

		ensures they are up to date and running.
5.1 Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers).	*Service Provider	
5.1.1 Ensure that anti-virus programs are capable of detecting, removing, and protecting against all known types of malicious software.	*Service Provider	
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.	*Service Provider	
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.	*Service Provider	
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 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.*	*Service Provider	
5.4 Ensure that security policies and operational procedures for protecting systems against malware are documented, in use, and known to all affected parties.	*Service Provider	
Requirement 6: Develop and maintain secure systems and applications		All development, patching, security and critical updates to applications and operating systems are performed by PayByPhone Technologies Inc.
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 will 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 assigning risk ratings will vary based on an organization's environment and risk assessment strategy. Risk rankings will, 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.*	*Service Provider	
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 will be identified according to the risk ranking process defined in Requirement 6.1.*	*Service Provider	

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 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.*	*Service Provider
6.3.1 Remove development, test and/or custom application accounts, user IDs, and passwords before applications become active or are released to Consumers.	*Service Provider
6.3.2 Review custom code prior to release to production or Consumers 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. · Code-review results are reviewed and approved by management 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 threats and vulnerabilities after implementotion, as defined at PCI DSS Requirement 6.6.*	*Service Provider
6.4 Follow change control processes and procedures for all changes to system components. The processes must include the following:	*Service Provider
6.4.1 Separate development/test environments from production environments, and enforce the separation with access controls.	*Service Provider
6.4.2 Separation of duties between development/test and production environments	*Service Provider
6.4.3 Production data (live PANs) are not used for testing or development	*Service Provider
6.4.4 Removal of test data and accounts before production systems become active	*Service Provider
6.4.5 Change control procedures for the implementation of security patches and software modifications must include the following:	*Service Provider
6.4.5.1 Documentation of impact.	*Service Provider
6.4.5.2 Documented change approval by authorized parties.	*Service Provider
6.4.5.3 Functionality testing to verify that the change does not adversely impact the security of the system.	*Service Provider
6.4.5.4 Back-out procedures.	*Service Provider
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 proctices must be used far these requirements.* *Note: Requirements 6.5.1 through 6.5.6, below, apply to all applications (internal or external):*	*Service Provider

6.5.1 Injection flaws, particularly SQL injection. Also consider OS Command Injection, LDAP and XPath injection flaws as well as other injection flaws.	*Service Provider	
6.5.2 Buffer overflows	*Service Provider	
6.5.3 Insecure cryptographic storage	*Service Provider	
6.5.4 Insecure communications	*Service Provider	
6.5.5 Improper error handling	*Service Provider	
6.5.6 All "high risk" vulnerabilities identified in the vulnerability identification process (as defined in PCI DSS Requirement 6.1).	*Service Provider	
Note: Requirements 6.5.7 through 6.5.10, below, apply to web applications and application interfaces (internal or external):	*Service Provider	
6.5.7 Cross-site scripting (XSS)	*Service Provider	
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).	*Service Provider	
6.5.9 Cross-site request forgery (CSRF)	*Service Provider	
6.5.10 Broken authentication and session management *Note: Requirement 6.5.10 is a best practice until June 30, 2015, after which it becomes a requirement.*	*Service Provider	
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.	*Service Provider	
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.	*Service Provider	
Requirement 7: Restrict access to cardholder data by business need to know		The PayByPhone network is fully owned and operated by PayByPhone Technologies Inc. All access to cardholder data is restricted by business need to know. Full PAN data is not accessible to Parking Operators or PayByPhone employees.
7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access.	*Service Provider	
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.	*Service Provider	
7.1.2 Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities.	*Service Provider	
7.1.3 Assign access based on individual personnel's job classification and function.	*Service Provider	
7.1.4 Require documented approval by authorized parties specifying required privileges.	*Service Provider	

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:	*Service Provider	
7.2.1 Coverage of all system components	*Service Provider	
7.2.2 Assignment of privileges to individuals based on job classification and function.	*Service Provider	
7.2.3 Default "deny-all" setting.	*Service Provider	
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.	*Service Provider	
Requirement 8: Assign a unique ID to each person with computer access		The PayByPhone network is fully owned and operated by PayByPhone Technologies Inc. All logical access including access to the PayByPhone Back office client portal, used for accessing transactional data and modifying parking meter settings, such as schedules and rate changes, is maintained by PayByPhone.
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:	*Service Provider	
8.1.1 Assign all users a unique ID before allowing them to access system components or cardholder data.	*Service Provider	
8.1.2 Control addition, deletion, and modification of user IDs, credentials, and other identifier objects.	*Service Provider	
8.1.3 Immediately revoke access for any terminated users.	*Service Provider	
8.1.4 Remove/disable inactive user accounts at least every 90 days.	*Service Provider	
8.1.5 Manage IDs used by 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.	*Service Provider	
8.1.6 Limit repeated access attempts by locking out the user ID after not more than six attempts.	*Service Provider	
8.1.7 Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID.	*Service Provider	
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.	*Service Provider	
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.	*Service Provider	
8.2.1 Using strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components.	*Service Provider	
8.2.2 Verify user identity before modifying any authentication credential - for example, performing password resets, provisioning new tokens, or generating new keys.	*Service Provider	

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 complexity and strength at least equivalent to the parameters specified above.	*Service Provider
8.2.4 Change user passwords/passphrases at least once every 90 days.	*Service Provider
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.	*Service Provider
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.	*Service Provider
8.3 Incorporate two-factor authentication for remote network access originating from outside the network by personnel (including users and administrators) and all third parties, (including vendor access for support or maintenance). *Note: Two-factor authentication requires that 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 two-factor authentication.* Examples of two-factor technologies include remote authentication and dial-in service (RADIUS) with tokens; terminal access controller access control system (TACACS) with tokens; and other technologies that facilitate two-factor authentication.	*Service Provider
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.	*Service Provider
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.	*Service Provider
8.5.1 Additional requirement for service providers: Service providers with remote access to customer 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.* *Note: Requirement 8.5.1 is a best practice until June 30, 2015, after which it becomes a requirement.*	*Service Provider
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.	*Service Provider
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).	*Service Provider

8.8 Ensure that security policies and operational procedures for identification and authentication are documented, in use, and known to all affected parties.	*Service Provider	
Requirement 9: Restrict physical access to cardholder data		PayByPhone manages the physical security of the backend systems, including processing and database servers, firewalls, routers, wireless telecommunications devices over which they have ownership.
9.1 Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment.	*Service Provider	
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.*	*Service Provider	
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.*	*Service Provider	
9.1.3 Restrict physical access to wireless access points, gateways, handheld devices, networking/communications hardware, and telecommunication lines.	*Service Provider	
9.2 Develop procedures to easily distinguish between onsite personnel and visitors, to include: - Identifying new onsite personnel or visitors (for example, assigning badges) - Changes to access requirements - Revoking or terminating onsite personnel and expired visitor identification (such as ID badges).	*Service Provider	
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.	*Service Provider	
9.4 Implement procedures to identify and authorize visitors. Procedures will include the following:	*Service Provider	
9.4.2 Visitors are identified and given a badge or other identification that expires and that visibly distinguishes the visitors from onsite personnel.	*Service Provider	
9.4.3 Visitors are asked to surrender the badge or identification before leaving the facility or at the date of expiration.	*Service Provider	
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.	*Service Provider	
9.5 Physically secure all media.	*Service Provider	
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.	*Service Provider	
9.6 Maintain strict control over the internal or external distribution of any kind of media, including the following:	*Service Provider	

9.6.1 Classify media so the sensitivity of the data can be determined.	*Service Provider	
9.6.2 Send the media by secured courier or other delivery method that can be accurately tracked.	*Service Provider	
9.6.3 Ensure management approves any and all media that is moved from a secured area (including when media is distributed to individuals).	*Service Provider	
9.7 Maintain strict control over the storage and accessibility of media.	*Service Provider	
9.8 Destroy media when it is no longer needed for business or legal reasons as follows:	*Service Provider	
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.	*Service Provider	
9.8.2 Render cardholder data on electronic media unrecoverable so that cardholder data cannot be reconstructed.	*Service Provider	
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 ar 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.* *Note: Requirement 9.9 is a best practice until June 30, 2015, after which it becomes a requirement.*	*Service Provider	
9.9.1 Maintain an up-to-date list of devices. The list will include the following: - Make, model of device - 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.	*Service Provider	
9.9.2 Periodically inspect device surfaces to detect tampering (for example, addition of card skimmers to devices), or substitution (for 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.*	*Service Provider	
9.9.3 Provide training for personnel to be aware of attempted tampering or replacement of devices. Training will 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).	*Service Provider	
9.10 Ensure that security policies and operational procedures for restricting physical access to cardholder data are documented, in use, and known to all affected parties.	*Service Provider	
Requirement 10: Track and monitor all access to network resources and cardholder data		The PayByPhone network is fully owned and operated by PayByPhone Technologies Inc. All logical access including access to the PayByPhone Back office client portal, used for accessing transactional data and modifying parking meter settings,

		such as schedules and rate changes, is maintained by PayByPhone. All access to cardholder data is restricted by business need to know. Full PAN data is not accessible to Parking Operators or PayByPhone employees.
10.1 Implement audit trails to link all access to system components to each individual user.	*Service Provider	
10.2 Implement automated audit trails for all system components to reconstruct the following events:	*Service Provider	
10.2.1 All individual user accesses to cardholder data	*Service Provider	
10.2.2 All actions taken by any individual with root or administrative privileges	*Service Provider	
10.2.3 Access to all audit trails	*Service Provider	
10.2.4 Invalid logical access attempts	*Service Provider	
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	*Service Provider	
10.2.6 Initialization, stopping, or pausing of the audit logs	*Service Provider	
10.2.7 Creation and deletion of system-level objects	*Service Provider	
10.3 Record at least the following audit trail entries for all system components for each event:	*Service Provider	
10.3.1 User identification	*Service Provider	
10.3.2 Type of event	*Service Provider	
10.3.3 Date and time	*Service Provider	
10.3.4 Success or failure indication	*Service Provider	
10.3.5 Origination of event	*Service Provider	
10.3.6 Identity or name of affected data, system component, or resource.	*Service Provider	
10.4 Using time-synchronization technology, synchronize all critical system clocks and times 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).*	*Service Provider	
10.4.1 Critical systems have the correct and consistent time.	*Service Provider	
10.4.2 Time data is protected.	*Service Provider	
10.4.3 Time settings are received from industry-accepted time sources.	*Service Provider	
10.5 Secure audit trails so they cannot be altered.	*Service Provider	
10.5.1 Limit viewing of audit trails to those with a job-related need.	*Service Provider	
10.5.2 Protect audit trail files from unauthorized modifications.	*Service Provider	

10.5.3 Promptly back up audit trail files to a centralized log server or media that is difficult to alter.	*Service Provider	
10.5.4 Write logs for external-facing technologies onto a secure, centralized, internal log server or media device.	*Service Provider	
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 will not cause an alert).	*Service Provider	
10.6 Review logs and security events for all system components to identify anomalies or suspicious activity.	*Service Provider	
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.).	*Service Provider	
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.	*Service Provider	
10.6.3 Follow up exceptions and anomalies identified during the review process.	*Service Provider	
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).	*Service Provider	
10.8 Ensure that security policies and operational procedures for monitoring all access to network resources and cardholder data are documented, in use, and known to all affected parties.	*Service Provider	
Requirement 11: Regularly test security systems and processes		The PayByPhone network is fully owned and operated by PayByPhone Technologies Inc. All external and internal systems are scanned for vulnerabilities at least quarterly and penetration testing activities are performed against all systems at least annually.
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.*	*Service Provider	
11.1.1 Maintain an inventory of authorized wireless access points including a documented business justification.	*Service Provider	
11.1.2 Implement incident response procedures in the event unauthorized wireless access points are detected.	*Service Provider	

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 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.*	*Service Provider
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.	*Service Provider
11.2.2 Perform quarterly external vulnerability scans, via an Approved Scanning 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 be performed by an Approved Scanning Vendar (ASV), approved by the Payment Card Industry Security Standards Council (PCI SSC). Refer to the ASV Program Guide published an the PCI SSC website for scan customer responsibilities, scan preparation, etc.*	*Service Provider
11.2.3 Perform internal and external scans, and rescans as needed, after any significant change. Scans must be performed by qualified personnel.	*Service Provider
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 - 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.*	*Service Provider
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).	*Service Provider
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).	*Service Provider
11.3.3 Exploitable vulnerabilities found during penetration testing are corrected and testing is repeated to verify the corrections.	*Service Provider
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 segmentation controls/methods to verify that the segmentation methods are operational and effective, and isolate all out-of-scope systems from in-scope systems.	*Service Provider
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.	*Service Provider

11.5 Deploy a change-detection mechanism (for example, file-integrity monitoring tools) to alert personnel to unauthorized modification of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly. *Note: For change-detection purposes, critical files are usually those that do not regularly change, but the modification of which could indicate a system compromise or risk of compromise. Change-detection mechanisms such as file-integrity monitoring products usually come pre-configured with critical files for the related operating system. Other critical files, such as those for custom applications, must be evaluated and defined by the entity (that is, the merchant or service provider).*	*Service Provider	
11.5.1 Implement a process to respond to any alerts generated by the change-detection solution.	*Service Provider	
11.6 Ensure that security policies and operational procedures for security monitoring and testing are documented, in use, and known to all affected parties.	*Service Provider	
Requirement 12: Maintain a policy that addresses information security for all personnel		PayByPhone Technologies Inc. maintains their own information security policies and procedures, related to the development, configuration, and installation of the PayByPhone platform. These information security policies and procedures do not in any way supplant the policies maintained and developed by Parking Operators for their own PCI DSS compliance.
12.1 Establish, publish, maintain, and disseminate a security policy.	*Service Provider	
12.1.1 Review the security policy at least annually and update the policy when the environment changes.	*Service Provider	
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 risk assessment. *Examples of risk-assessment methodologies include but are not limited to OCTAVE, ISO 27005 and NIST SP 800-30.*	*Service Provider	
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:	*Service Provider	
12.3.1 Explicit approval by authorized parties	*Service Provider	
12.3.2 Authentication for use of the technology	*Service Provider	
12.3.3 A list of all such devices and personnel with access	*Service Provider	
12.3.4 A method to accurately and readily determine owner, contact information, and purpose (for example, labeling, coding, and/or inventorying of devices)	*Service Provider	
12.3.5 Acceptable uses of the technology	*Service Provider	
12.3.6 Acceptable network locations for the technologies	*Service	

	Provider
12.3.7 List of company-approved products	*Service Provider
12.3.8 Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity	*Service Provider
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	*Service Provider
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.	*Service Provider
12.4 Ensure that the security policy and procedures clearly define information security responsibilities for all personnel.	*Service Provider
12.5 Assign to an individual or team the following information security management responsibilities:	*Service Provider
12.5.1 Establish, document, and distribute security policies and procedures.	*Service Provider
12.5.2 Monitor and analyze security alerts and information, and distribute to appropriate personnel.	*Service Provider
12.5.3 Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations.	*Service Provider
12.5.4 Administer user accounts, including additions, deletions, and modifications.	*Service Provider
12.5.5 Monitor and control all access to data.	*Service Provider
12.6 Implement a formal security awareness program to make all personnel aware of the importance of cardholder data security.	*Service Provider
12.6.1 Educate personnel upon hire and at least annually. *Note: Methods can vary depending on the role of the personnel ond their level of access to the cardholder data.*	*Service Provider
12.6.2 Require personnel to acknowledge at least annually that they have read and understood the security policy and procedures.	*Service Provider
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.*	*Service Provider
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:	*Service Provider
12.8.1 Maintain a list of service providers.	*Service Provider
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 customer, or to the extent that they could impact the security of the customer'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.*	*Service Provider
12.8.3 Ensure there is an established process for engaging service providers including proper due diligence prior to engagement.	*Service Provider
12.8.4 Maintain a program to monitor service providers' PCI DSS compliance status at least annually.	*Service Provider

12.8.5 Maintain information about which PCI DSS requirements are managed by each service provider, and which are managed by the entity.	*Service Provider	
12.9 Additional requirement for service providers: Service providers acknowledge in writing to Consumers that they are responsible for the security of cardholder data the service provider possesses or otherwise stores, processes, or transmits on behalf of the customer, or to the extent that they could impact the security of the customer's cardholder data environment. *Note: This requirement is a best practice until June 30, 2015, after which it becomes a requirement.* *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.*	*Service Provider	
12.10 Implement an incident response plan. Be prepared to respond immediately to a system breach.	*Service Provider	
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.	*Service Provider	
12.10.2 Test the plan at least annually.	*Service Provider	
12.10.3 Designate specific personnel to be available on a 24/7 basis to respond to alerts.	*Service Provider	
12.10.4 Provide appropriate training to staff with security breach response responsibilities.	*Service Provider	
12.10.5 Include alerts from security monitoring systems, including but not limited to intrusion-detection, intrusion-prevention, firewalls, and file-integrity monitoring systems.	*Service Provider	
12.10.6 Develop a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments.	*Service Provider	

2.0 Attestation of Compliance

Prior to execution of this Agreement, the Service Provider will provide the City with a current and valid Attestation of Compliance document. Annually on an ongoing basis, the Service Provider will provide current and valid Attestation of Compliance documentation.

Current and valid Attestation of Compliance document to be inserted

SCHEDULE H - CHANGE ORDER REQUEST FORMS

City of Vancouver - Contemplated Change Notice

PROJECT:		PROJECT NO.:	
PURCHASE ORDER NO.:		FILE NO.:	
CCN NO.:		ISSUE DATE:	
CoV CONTACT:		SERVICE PROVIDER:	

CONTEMPLATED CHANGE NOTICE: The following items are Contemplated Changes to the Contract for this project. Work is not to proceed unless authorized by a Change Directive or Change Order signed by the City. All materials and workmanship are to be in accordance with the Specifications unless otherwise stated. Submit an itemized quotation for changes to the Contract Price and Contract Time within ____ days of the date above.

TITLE:			
REASON:			
DESCRIPTION: *(provide short description of additional work to be completed; reference and attach documents, specifications and/or drawings describing the contemplated change including dates)*			
Project Manager's Approval*:		Date:	

* Authorized by the Project Manager. If impact is materially significant ensure that an Internal Change Consent is authorized and on file prior to issuance. Impact is materially significant if it is estimated to be greater than 15% of project budget for projects under $500K, greater than 10% of project budget for projects under $2M, or greater than $200K in absolute value.

City of Vancouver - Change Control Form

PROJECT:		PROJECT NO.:	
PURCHASE ORDER NO.:		FILE NO.:	
ISSUE DATE:		CO NO.:	

The customer CONTACT:		SERVICE PROVIDER:	

TITLE:
REASON:
REFERENCE: *(list and attach preceding Contemplated Change Notice, Change Directive, Site Instruction or quotation)*
DESCRIPTION: *(provide short description of additional work to be completed; reference and attach documents, specifications and/or drawings describing the contemplated change including dates)*

Subject to the terms and conditions of the Agreement, the Service Provider hereby offers to perform the changes to the Work described above with the following net adjustments to the Contract Price and Contract Time:

NET ADJUSTMENT TO CONTRACT PRICE:

Previous Contract Price (including Change Orders authorized to date): $0.00 (including PST)

Note: Prices quoted do not include GST.

Contract Price is hereby: **(a) increased* by** $0.00 (including PST)

(b) decreased by $0.00 (including PST)

If total change is greater than 10% of previous Contract Price, the Service Provider must notify their bonding company.

Revised Contract Price: $ 0.00 (including PST)

*Note: price increase amount to include all overhead on any additional contract time.

NET ADJUSTMENT TO CONTRACT TIME:

Previous completion date (including Change Orders authorized to date): _____

Contract Time is hereby: **(a) increased* by** _____ working days

(b) decreased by _____ working days

Revised completion date: _____

*Note: price increase amount to include all overhead on any additional contract time.

Approval of and commencement of work under this Change Order is subject to the Owner's authorization.

	NAME	SIGNATURE	DATE
Consultant recommendation:			
Service Provider acceptance:			
Initialed by Project Manager:			
Initialed by Manager:			
Initialed by Hazardous Materials:			

Owner authorization*:			

To be signed by General Manager or approved delegate. If impact is materially significant ensure that an Internal Change Consent is authorized and on file prior to issuance.

Distribution:	☐ File	☐ SCM	☐ Finance
	☐ Service Provider	☐ Consultant	

Confirmation of Funding Availability: (to be completed if new funding is required for execution of this Change Order)

☐ Operating	☐ Capital	Source:

If request is for more than $50K of new Capital funding, it must be approved by Council through the quarterly budget adjustment process prior to proceeding. All new funding requests must be submitted through a shopping cart.

☐ Quarterly Budget adjustment has been requested (if applicable)	**Council Review Date:**	

Confirmed by:	**NAME**	**SIGNATURE**	**DATE**
Dept. Finance			
Corp. Finance			

Review and Approval from Supply Chain: (to be completed if change is materially significant* to original contract price)

DEPARTMENT	**NAME**	**SIGNATURE**	**DATE**
Supply Chain			

*Impact is materially significant if it is estimated to be greater than 15% of project budget for projects under $500K, greater than 10% of project budget for projects under $2M, or greater than $200K in absolute value.

00592488.DOCX-revised January 2016

SCHEDULE I - Service Level Agreement

1.0 Service Levels

The Service Provider provides an uptime service level guarantee surrounding all of the mission critical parts of the Services. Uptime guarantees are inclusive of all planned and unplanned outages by the Service Provider and exclusive of outages related to third party suppliers, including, but not limited to payment gateways, messaging suppliers, telephony suppliers, 3rd party revenue control and / or enforcement handheld systems.

System Element	SLA[1]	SLA Details	Measurement Period
Mobile Applications: iOS & Android	99.9%	Service Provider's mobile applications shall be available and fully functional for end users 99.9% of the time based on a standard 24-hour day	30 days
Mobile Website	99.9%	Service Provider's mobile website shall be available and fully functional for end users 99.9% of the time based on a standard 24-hour day	30 days
Interactive Voice Response Payment	99.9%	Service Provider's IVR application shall be available and fully functional for end users 99.9% of the time based on a standard 24-hour day	30 days
Consumer Website	99.9%	Service Provider's consumer web site shall be available for use by the public 99.9% of the time based on a standard 24-hour day	30 days
Back Office	99.9%	Service Provider's back office web site shall be available for use by City staff 99.9% of the time based on a standard 24-hour day	30 days
Parking Enforcement API	99.9%	Service Provider's parking enforcement API shall respond within 1 second of request 99.9% of the time based on a standard 24-hour day	30 days
Payment Processing	99.9%	Payments shall process within 4 seconds 99.9% of the time based on a standard 24-hour day	30 days
Reminder Message Delivery	99.9%	Reminder messages shall be sent 5 minutes before parking expiration 99.9% of the time based on a standard 24-hour day	30 days
Time Synchronization	99.9%	Server time shall deviate by no more than two seconds from the NTP source 99.9% of the time based on a standard 24-hour day	30 days
Parking Policies	99.9%	The service shall accurately enforce all parking policies including time limits, no stopping, and rates - for 99.9% of all transactions	30 days
Data Delivery Services	99.9%	The service shall deliver real-time notification of Parking Sessions to integrated systems within 4 seconds	30 days

		99.9% of the time based on a standard 24-hour day	
Security	100%	Service Provider shall maintain PCI-DSS Level 1 compliance and shall implement highly secure systems to manage the Solution. Service Provider's security for the Solution and all connections thereto shall conform to the most current National Institute of Standards and Technology's (NIST) Security Content Automation Protocol (SCAP) (Internet: http://scap.nist.gov/revision/index.html	Annual
Data Privacy	100%	Service Provider shall at all times conform with Canadian and British Columbia security and privacy policies, including: i.BC's Personal Information Protection Act, SBC 2003 c.36 ii.Federal Personal Information Protection and Electronic Documents Act, SC 2000 c.5 iii. Freedom of Information and Protection of Privacy Act, RSBC 1996, c. 165(FIPPA)	Annual
Scheduled Maintenance		Service Provider will perform scheduled maintenance a maximum of once per month, on a Saturday between 2am-4am Pacific time. Service Provider must notify the City a minimum of 48 hours in advance of scheduled maintenance	Max. of monthly

[1] Uptime guarantees are exclusive of outages related to third-party suppliers, including, but not limited to payment gateways, messaging supplier, telephony supplier, third-party revenue control, and/or enforcement handheld systems.

1.1 Service Impacting Issue Management

Priority	Definition	Response Time	Update Frequency	Restoration Time (Maximum)
1-Urgent	Solution/Service outage or critical component not functioning, causing severe business impact	Less than 30 minutes	30 minutes	2 hours
2-Medium	Component not functioning, but not critical. Critical service used by a limited number of users is	Less than 60 minutes	1 hour	2 business days

	not available, or operation is slow.			
3-Low	Non-critical problem. The service affected is used by a small number of users. The service is still running, but suffering minor degradation.	1 business day	On completion	3 business days
4-General Support	Non-service impacting technical queries.	1 business day	On completion	5 business days

1.2 Service Level Reviews

The Service Provider will review the performance of the support team and the service levels on a monthly basis with the City. The Service Provider will provide key performance indicators (KPIs) at the reviews that will include, but are not limited to:

- A list of all incidents the City has logged with Service Provider during the reporting period, including time, date, details and resolution time
- An indicator if the service level was met for each incident
- Percentage of incidents by severity level
- Trending charts showing service level metrics over the past 12 months, with monthly details, on a rolling timeframe
- A written synopsis of the past period, that shows the analysis of missed service levels and pertinent activities performed or planned to address areas of concern

1.3 Emergency Technical Support

- Emergency technical support is available 24x7x365
- Emergency technical support is accessible to the Client by emailing clientescalations@paybyphone.com. The contact method may be changed from time to time, in which case Service Provider will notify Client of the new contact information;
- The Service Provider will make sure that suitably qualified staff are available on the emergency technical support system at all times

1.4 Problems or Disputes

In the event of problems in relation to the Service Provider's Services that are not resolved pursuant to this Service Level Agreement or under the terms of the Agreement or if a service level has not been met or, in the Service Provider's sole discretion, a service level runs a high risk of not being met, the Service Provider will escalate the matter by immediately contacting the City representatives of Parking Operations & Enforcement and POE Applications support by email or telephone. In addition to the foregoing, if a major unplanned outage of Services occurs during regular City parking hours as defined

in this Service Level Agreement, the Service Provider will also notify the City's Chief Information Officer and the City's Director of Applications by email or telephone.

1.5 Liquidated Damages for Non-Compliant Service Levels

A. If:

(i) any Service Element listed in Section 1.0 of this Schedule I to the Agreement is in operation for less than the percentage of time listed in the "SLA" column of Section 1.0 of this Schedule I to the Agreement over the period of time listed in the "Measurement Period" column of Section 1.0 of this Schedule I to the Agreement; or

(ii) any "Urgent" or "Medium" Service Impacting Issue occurs and the Services are not restored in accordance with the time stated in the "Restoration Time (Maximum)" column of Section 1.1 of this Schedule I to the Agreement;

then the City and the Service Provider acknowledge and agree that the Service Provider will pay the City liquidated damages in recognition of the fact that the City will suffer actual damages and there will be a loss of benefit to the public. The City and the Service Provider acknowledge and agree that the exact amount of such damages and loss of benefit will be difficult or impractical to determine under current circumstances. In consideration of the current circumstances, if any scenario described in Sections 1.5(A)(i) or 1.5(A)(ii) occurs, the Service Provider will pay liquidated damages to the City of fifty percent of the City's estimated lost revenue for each minute that any Service Element listed in Section 1.0 of this Schedule I to the Agreement is not in operation or the Services are not operational due to an "Urgent" or "Medium" Service Impacting Issue. The City's estimated lost revenue will be calculated based on the three most recent comparable time periods and an assumption that half of the Consumers would revert to paying for Parking Sessions with cash at parking meters. For clarity, if, for example, an "Urgent" Service Impacting Issue caused the Services to be non-operational from 9 AM to 9:30 AM on Friday, August 24, 2018, then the City and the Service Provider would calculate the average revenue that the City received from Consumers from 9 AM to 9:30 AM on each of Friday, August 17, 2018, Friday, August 10, 2018, and Friday, August 3, 2018, and in recognition of the assumption that half of the Consumers would revert to paying for Parking Sessions with cash at parking meters, then the remaining fifty percent of revenue will be deemed to be the City's estimated lost revenue ("Estimated Lost Revenue"). The Service Provider would pay the City liquidated damages of fifty percent of the Estimated Lost Revenue. The City and the Service Provider acknowledge and agree to revisit the foregoing formula pursuant to which the Service Provider will pay the City liquidated damages and the estimated percentage of lost revenue to the City due to the Services being non-operational to reflect any changes in circumstances or available data during the Term, including, for example, calculations showing that more or less than half of consumers revert to paying for Parking Sessions with cash at parking meters.

B. The Service Provider and the City acknowledge and agree that the liquidated damages described above are not penalties, but represent a fair and reasonable remedy for the damages that the City would incur if the Service Provider failed to perform the Services in accordance with the Agreement, including this Schedule I to the Agreement. If the Service Provider owes the City liquidated damages pursuant to this Schedule I to the Agreement, then the City will send a written assessment to the Service Provider detailing the issue with the System Element or the Service Impacting Issue to the best of the City's knowledge. The City may set off any liquidated damages that the Service Provider owes to the City against amounts that the City otherwise owes to the Service Provider under this Agreement.

C. The City and the Service Provider acknowledge and agree that the maximum liquidated damages that the Service Provider will owe to the City for any one-month period during the Term under this Schedule I to the Agreement is ten percent of the fees that the City owes to the Service Provider under this Agreement for that given month.

D. The Service Provider and the City acknowledge and agree that the Service Provider will not be required to pay the City liquidated damages pursuant to Section 1.5(A) if:

(i) each Service Element listed in Section 1.0 of this Schedule I to the Agreement is in operation for more than the percentage of time listed in the "SLA" column of Section 1.0 of this Schedule I to the Agreement over the period of time listed in the "Measurement Period" column of Section 1.0 of this Schedule I to the Agreement or any "Urgent" or "Medium" Service Impacting Issues occur and the Services are restored in accordance with the times stated in the "Restoration Time (Maximum)" column of Section 1.1 of this Schedule I to the Agreement;

(ii) any Service Elements listed in Section 1.0 of this Schedule I to the Agreement is not in operation or any "Urgent" or "Medium" Service Impacting Issues occur as a result of testing on the Software, the Solution, or the Mobile Application by mutual agreement of the Service Provider and the City;

(iii) any Service Elements listed in Section 1.0 of this Schedule I to the Agreement is not in operation or any "Urgent" or "Medium" Service Impacting Issues occur as a result of the negligent acts or omissions of the City or the City's employees, agents, or contractors;

(iv) any Service Elements listed in Section 1.0 of this Schedule I to the Agreement is not in operation or any "Urgent" or "Medium" Service Impacting Issues occur as a result of failures by third party providers of payment gateways, payment card processing, merchant acquirer services, electrical power, internet access, or cellular communications; or

(v) any Service Elements listed in Section 1.0 of this Schedule I to the Agreement is not in operation or any "Urgent" or "Medium" Service Impacting Issues occur as a result of any "Unavoidable Delays", which, for the purposes of this section, are defined as interruptions that are beyond the control of the Service Provider and that the Service Provider could not have avoided by the exercise of care, prudence, foresight, or diligence, such as: acts of God; floods; windstorms; tornadoes; earthquakes or other natural disasters; acts of terrorism; wars; riots; insurrections; epidemics; quarantine restrictions; strikes and lockouts by employees or workers of entities other than the Service Provider or the Service Provider's related parties, subsidiaries, or parent companies; freight embargoes; acts of governmental agency; priorities or privileges established for the manufacture assembly, or allotment of materials by order of decree, or otherwise of the Canadian Government or by any department bureau, commission, committee, agent, or administrator of any legally constituted public authority; vandalism, theft and accidental damage not caused in any way by the Service Provider, changes in the Services ordered by the City insofar as they necessarily require additional time to complete the Services; or interruption or failure of electrical power affecting the Service Provider's main and backup systems, the internet, or cellular telecommunications caused by the events or causes described herein.