FileLocal

Executive Board:

Susy Haugen, Chair
City of Everett

Toni Battersby
City of Bellevue

Glen Lee
City of Seattle

Andy Cherullo
City of Tacoma

Executive Board Agenda

November 18, 2016

SEATTLE MUNICIPAL TOWER CONFERENCE ROOM 4070
SEATTLE, WA

1. CALL TO ORDER

A. Introductions

2. PUBLIC COMMENT*

3. ACTION ITEMS

A. Resolution FL2016-09: Kubra Contract
   I. Briefing Paper: Resolution FL2016-09 **Page 2**
   II. Resolution FL2016-09 **Page 3**
      a. Attachment A: Kubra Contract **Page 5**
      b. Attachment B: Scope of Work **Page 51**
      c. Attachment C: Service Level Agreement **Page 56**

4. NEXT MEETINGS:

A. Operations Committee meeting: Monday, November 28, 2016 at 2:00 pm
B. Executive Board meeting: Monday, December 12, 2016 at 12:00 pm

5. ADJOURNMENT

*A public comment period is provided to allow the public to briefly present information, topics or issues that they feel should be considered by the board. Presentation should be limited to three minutes and be summary in nature. The board may decide to discuss the topic briefly at that time or to request its placement on a future agenda.

File Local Resolution FL2016-09
Briefing Paper

Date: November 18, 2016

Issue: Will the Washington Multi-City Business License and Tax Portal Agency ("Portal Agency") Executive Board authorize the chair to execute a contract for electronic payment services with Kubra Data Transfer, LTD

Options: Maintain the current contract which is a contract between the City of Seattle and the Vendor (Kubra Data Transfer, LTD) or have the Portal Agency Executive Board authorize the chair to execute a contract between the Agency and the vendor.

Operations Committee Recommendation: The Operations Committee Recommends signing a contract directly between the Agency and the Vendor.

Rationale: The portal development was done under the City of Seattle and later assigned to the Portal Agency (FL2016-03). As part of this development, the portal developer developed the payment process utilizing an existing contract with the City of Seattle. Executing a contract with Kubra would maintain the enabling technology between the payment processor (Kubra) and Portal software (FileLocal) and not disrupt service to our customers.

RESOLUTION NO. 2016-09

A Resolution of the Washington Multi-City Business License and Tax Portal Agency Executive Board authorizing the chair to execute a contract for electronic payment services.

Whereas, Kubra Data Transfer, Ltd. ("Kubra"), has previously contracted to provide payment processing services in support of the FileLocal product via a contract executed between Kubra and the City of Seattle; and

Whereas, the launch of the FileLocal product is now complete and the ongoing stewardship and management of the FileLocal product has been transferred from the City of Seattle to the Washington Multi-City Business License and Tax Portal Agency ("Portal Agency") via Agency Resolution 2016-03; and

Whereas, the Executive Board has determined that it is in the best interest of the Agency to enter into a direct contractual relationship with a payment processing services provider – rather than having these services continue to be provided under a contract with the City of Seattle – in order to better support and fulfill the Agency's role as steward and manager of the FileLocal product; and

Whereas, Executive Board of the Agency has determined that Kubra, because of its uniquely valuable experience and expertise with the FileLocal portal solution, is the best qualified vendor for processing electronic payments made through the FileLocal portal; **Now Therefore**

BE IT RESOLVED by the Executive Board of the Washington Multi-City Business License and Tax Portal Agency:

SECTION 1. The Executive Board authorizes the Chair to execute the "Electronic Payment Processing Services Agreement" (attachment A), and the associated Scope of Work (attachment B) and Service Level Agreement (attachment C).

ADOPTED this 18th day of November, 2016.

ATTEST:

Washington Multi-City Business License and Tax Portal Agency Executive Board
Seattle, Washington

Board Secretary

Board Chair

FILE LOCAL AGENCY

ELECTRONIC PAYMENT PROCESSING SERVICES AGREEMENT

Contract Title: KUBRA Contract

Contract No. FL2016-09

This Agreement is entered into by and between the Washington Multi-City Business License and Tax Portal Agency d/b/a File Local ("Agency") and KUBRA Data Transfer Ltd., a corporation incorporated under the laws of the State of New York ("Payment Vendor"), and is effective as of _____, 2016 ("**Effective Date**").

WHEREAS, the Agency desires to have certain electronic payment processing services (as defined below) performed for the benefit of the Agency, participating cities ("Agency Clients"), the tax portal vendor ("Portal Vendor") and Payment Vendor wishes to provide such services; and

WHEREAS, the Agency has selected Payment Vendor to perform such services on the terms and conditions set forth in this Agreement;

NOW, THEREFORE, in consideration of the mutual terms, conditions, and covenants set forth below, the Agency and Payment Vendor agree as follows:

1 SERVICES

Payment Vendor agrees to provide and perform the electronic payment services (the "**Services**") to the Agency, Agency Clients and Portal Vendor on the terms set forth in Schedule F ("Scope of Work") and at the service levels set forth in Schedule C ("Service Level Agreement" or "SLA"), both of which are attached to and made part of this Agreement.

2 WARRANTY

In performing the Services, Payment Vendor shall comply with all federal, state, and local laws and regulations applicable to the Services to be provided under this Agreement. Payment Vendor represents and warrants that all staff that it assigns to provide the contracted services (and anyone performing work on Payment Vendor's behalf or under its direction) have the requisite training, skill, and experience necessary to provide the Services and have all requisite licenses or certifications. In addition to meeting the requirements of the SLA as described in Schedule C, Payment Vendor shall perform the Services provided under this Agreement diligently, thoroughly, with due care, and in accordance with applicable standards of conduct and performance for members of Payment Vendor's profession.

3 TITLE

Title and all ownership rights in and to the documentation describing or relating to the Services, including, but not limited to, any and all formats, computer programs, specifications, and

user guides (the "**Documentation**") shall remain at all times solely with the Payment Vendor. The Services and the Documentation are agreed to be the proprietary, confidential, and trade secret information of Payment Vendor, except for any element of such Documentation that is available or generally known to the public via lawful means and without breach of any duty of confidentiality. The Agency has no right, title, or interest in or to the Documentation, whether or not such Documentation has been developed specifically for performance of this Agreement. The Agency has the right to make a reasonable number of copies of the Documentation for the sole purpose of accessing and utilizing the Services in a reasonable and effective manner.

4 TERM AND TERMINATION

4.1 Term.

This Agreement will remain in full force and effect for twenty-six (26) consecutive months following the Effective Date of this Agreement (the **"Initial Term**"), and will automatically renew and extend for successive twelve (12) month terms (each a "**Renewal Term**"), commencing at the conclusion of the Initial Term or any Renewal Term, unless written notice of termination is given by either party to the other at least ninety (90) days prior to the end of the Initial Term or Renewal Term, as applicable. The Initial Term, together with any Renewal Term(s), is referred to in this Agreement as the "**Term**".

4.2 Termination with Cause.

Either party may terminate this Agreement upon delivery of written notice to the other party in the event that such other party:

(a) ceases to do business or otherwise terminates business operations;

(b) seeks protection under any bankruptcy, receivership, trust deed, creditors arrangement, composition or comparable proceeding, or if any such proceeding is instituted against the other; or

(c) breaches any material representation, warranty, obligation, or other provision of this Agreement and fails to fully cure such breach within thirty (30) days of receiving written notice of such breach from the terminating party. For greater certainty, for the purposes of this Agreement, the Agency's failure to pay a Delinquent Balance (as hereinafter defined), after being given notice and a reasonable opportunity to cure, is a breach of a material obligation.

4.3 Payment and Disabling of Agency Accounts on Termination or Expiration.

Upon termination or expiration of this Agreement:

(a) The Agency shall pay Payment Vendor all amounts due and owing under this Agreement, including without limitation any and all amounts owing in respect of

Charges and any Additional Charges, and such payment shall be invoiced and governed in accordance with Section 7 of this Agreement; and

(b) Payment Vendor may disable all accounts and passwords which allow the Agency and or Agency Clients access to the Services, but only after making reasonable efforts to coordinate with Agency personnel to avoid undue hardship to the Agency and its Agency Clients.

4.4 Disposition of Materials on Termination or Expiration.

Within thirty (30) days following the date of expiration or termination of this Agreement, the Agency shall furnish Payment Vendor with specific written instructions for the disposition of any supplies, material, and data then in the possession of Payment Vendor. If written instructions are not received by Payment Vendor within this 30-day period, Payment Vendor may dispose of such supplies, material, and data in any reasonable manner which Payment Vendor deems appropriate.

Upon termination of this Contract, Payment Vendor will provide PCI compliant protection to cardholder data until data is destroyed or returned to the Agency or Agency Clients. A statement of Work will be developed and mutually agreed upon by the Agency, Agency Clients and the Payment Vendor for this protection. Hours will be billed at agreed upon hourly rates.

Payment Vendor shall return all Agency or Agency Clients data to the Agency or Agency Clients in a useable electronic form, and erase, destroy, and render unreadable all Agency or Agency Clients data in its entirety in a manner that prevents its physical reconstruction through the use of commonly available file restoration utilities, and certify in writing that these actions have been completed within 30 days of the termination of this Agreement or within 5 business days of the request of the Agency or Agency Clients CISO's, whichever shall come first.

4.5 Other Legal Remedies for Nonperformance

A termination of this Agreement by either party for cause will not prevent the terminating party from seeking any other legal remedies it may otherwise have for the violation or nonperformance of any provisions of this Agreement.

5 EXCLUSIVITY

During the entire Term of this Agreement, the Agency shall solely and exclusively utilize Payment Vendor as its sole Payment Vendor of the Services or any other services similar in nature to the Services.

6 CHARGES

6.1 Charges.

The Agency agrees to pay Payment Vendor for the Services and any equipment or products related thereto, in accordance with the charges set out in the attached Schedule A (the "**Charges**"). Except as otherwise provided in the Schedules, the Charges shall remain fixed during the Initial Term. Following the expiration of the Initial Term, except as otherwise provided in the Schedules, the Charges may be increased by no more than five (5%) percent per Renewal Term, and Payment Vendor must provide the Agency written notice of such an increase, if any, at least ninety (90) days prior to the implementation of same.

6.2 Additional Charges.

In addition to the Charges, the Agency further agrees to pay such additional charges (the "**Additional Charges**") as may arise in connection with the supply by Payment Vendor or by any third party of the Services or any products related thereto, but only if such Additional Charges are authorized by the Agency in writing. In the event Additional Charges are payable in advance by the Agency and the amount of such Additional Charges cannot be precisely ascertained in advance, Payment Vendor shall estimate the amount of such Additional Charges and shall subsequently reconcile the Agency's advance payment with the actual amount of such Additional Charges, once ascertained, by refunding any overpayments to the Agency as necessary.

7 INVOICING AND PAYMENT

7.1 Monthly Invoice.

All Charges, and any applicable Additional Charges, and other charges, costs, or expenses incurred pursuant to this Agreement, payable by the Agency to Payment Vendor, and all applicable taxes in respect thereof (collectively, the "**Monthly Charges**"), shall be billed by Payment Vendor to the Agency by monthly invoice on the first day of each month for any Monthly Charges incurred in the preceding month. Monthly Charges are payable within thirty (30) days from the date the invoice is received by the Agency, and will be considered a delinquent balance ("**Delinquent Balance**") if unpaid within such thirty (30) day period.

7.2 Interest on Delinquent Balance.

A Delinquent Balance is payable with interest calculated at twelve percent (12%) per annum (one percent per month or part thereof), in accordance with Washington law, from the date of the invoice until the date payment is received by Payment Vendor. Payment Vendor's failure to charge interest on any Delinquent Balance will not constitute a waiver of its right to do so in the future.

7.3 Ceasing Services on Delinquent Balance.

In the event of a Delinquent Balance, Payment Vendor is entitled, upon notice to the Agency and a reasonable opportunity cure, to cease providing the Services until such time as the Delinquent Balance and any interest accrued thereon is paid in full, and such a stoppage by Payment Vendor will not be considered a breach by Payment Vendor under this Agreement. Payment Vendor's decision not to cease Services pursuant to this subsection will not constitute a waiver of Payment Vendor's right to terminate this Agreement in accordance with subsection 4.2(c) of this Agreement, or to exercise any other rights to recover for defaults under this Agreement, whether at law or in equity.

8 TAXES, FEES AND LICENSES

a. Taxes: Where required by state statute, ordinance or regulation, Payment Vendor shall pay for and maintain in current status all taxes that are necessary for contract performance. Unless otherwise indicated, the Agency agrees to pay State of Washington sales or use taxes on all applicable consumer services and materials purchased, and all business and occupation ("B&O") taxes owed to the State and/or local jurisdictions, as applicable. Payment Vendor may not charge the Agency for federal excise taxes, and the Agency agrees to furnish Vendor with an exemption certificate where appropriate.

b. Fees and Licenses: Payment Vendor shall pay for and maintain in a current status, any license fees, assessments, permit charges, etc., which are necessary for contract performance. It is the Payment Vendor's sole responsibility to monitor and determine any changes or the enactment of any subsequent requirements for said fees, assessments, or charges, and to immediately comply with said changes during the entire term of this Contract. Payment Vendor must pay all custom duties, brokerage, or import fees where applicable as part of the contract price. Payment Vendor shall take all necessary actions to ensure that materials or equipment purchased are expedited through customs. Payment Vendor agrees to maintain current business licenses in each of the participant cities of the Agency (presently: Seattle, Everett, Bellevue, and Tacoma).

c. Payment Vendor is to calculate and enter the appropriate Washington State and local sales tax on the invoice. Tax is to be computed on new items after deduction of any trade-in, in accordance with WAC 458-20-247.

9 ADJUSTMENTS

Requests by the Agency for any billing adjustments must be made within one hundred and twenty (120) days of the invoice date. Any amounts determined to be in error will be credited against the next month's invoice. Such request for adjustment is not cause for delay in payment of the balance due.

10 RELIANCE ON INFORMATION PROVIDED

10.1 Customer Responsible for Data.

The Agency, Agency Clients and Portal Vendor solely responsible for the adequacy and accuracy of the Agency's data and the instructions, programs, and procedures supplied by it. The Agency, Agency Clients or its Portal Vendor shall provide audit controls, operating methods, and checkpoints necessary to satisfy the Agency's requirements with respect to detection of machine errors, security, and adequacy of the data provided by the Agency, Agency Clients (or the Portal Vendor) to Payment Vendor and necessary to enable recommencement and recovery in the event of any malfunction. Payment Vendor is entitled to rely on the accuracy of all data and information provided to it by the Agency, Agency Clients and its Portal Vendor.

10.2 Incorrect Data.

The Agency, Agency Clients or Portal Vendor shall promptly inform Payment Vendor of any incorrect data or information. The Agency shall bear the cost of any correction of data or information if such a correction results in additional costs to Payment Vendor and such costs exceed those which are incurred in the process of routinely receiving and preparing correct data for normal usage. Any such additional costs will be billed on the Agency's monthly invoice for Services and will be subject to all relevant provisions of this Agreement, including without limitation, Section 7 hereof.

11 DATA TRANSMISSION

11.1 Data Transmission from Customer to Payment Vendor.

The Agency, through the Portal Vendor's system, agrees to transmit its data to Payment Vendor electronically in such manner as may be mutually agreed upon by the Agency, Agency Clients, Portal Vendor, and Payment Vendor from time to time; such data transmission shall be effected by the Agency, through the Portal Vendor's system, in a timely manner in order to enable Payment Vendor to satisfy its obligations to the Agency under this Agreement.

Any data supplied to Payment Vendor by the Agency, Agency Clients or the Portal Vendor must be compatible with Payment Vendor's equipment and processing filters, and the Agency's programs necessary to accomplish transmission of its data in useable form must comply with reasonable industry standards. If the data submitted by the Agency, through the Portal Vendor's system, to Payment Vendor for processing is not in the required format for processing, the Agency agrees to pay Payment Vendor such reasonable charges as may be necessarily incurred by Payment Vendor to prepare such data for processing or reprocessing.

11.2 Data Transmission from Payment Vendor to Customer.

Payment Vendor shall use all commercially reasonable means to ensure the safe and prompt transfer of data from Payment Vendor to the Agency. The Agency understands that

Payment Vendor utilizes various third party Payment Vendors of online payment systems and that these third parties act as wholly independent entities. Payment Vendor will use reasonable care to select and utilize competent third party Payment Vendors of online payment services; however,

12 ADDITIONAL SERVICES AT CUSTOMER'S REQUEST

In addition to the Services described in Schedule F, further special services or third-party supplied products, services, or equipment may be provided by Payment Vendor at the Agency's request, but only if the Agency executes and delivers to Payment Vendor a Payment Vendor Supply Request Form detailing the special services or third-party products, services, or equipment required by the Agency and the charges payable by the Agency for such special services and/or equipment. Payment Vendor shall arrange on behalf of the Agency for the supply of such special services and/or equipment, subject to payment in advance by the Agency, or subject to payment in such other manner as may be provided in Schedule F, the Payment Vendor Statement of Work (SOW).

13 MODIFICATIONS TO THE SERVICES

Upon giving reasonable advance notice to the Agency, Payment Vendor may make any modifications, changes, adjustments, or enhancements to the Services that it considers to be reasonable under the circumstances or that are required by law or governmental regulation or any guidelines, directives, or policies issued by any regulatory authority.

14 TECHNICAL PROBLEM RESOLUTION

14.1 Erroneous Work-Product.

Payment Vendor agrees to reprocess any work-product containing erroneous results due to a malfunction of Payment Vendor's equipment or operating system or error on the part of Payment Vendor's operators, on the condition that the Agency notifies Payment Vendor of the erroneous results within a reasonable time of discovery of the error(s) in question. The Agency shall implement data security procedures and checkpoints necessary to avoid excessive rerun times to restore a file to its required status.

14.2 Service Interruptions.

If the Services are partially or wholly interrupted owing to a malfunction in Payment Vendor's equipment, operating system, or telecommunication channels, the party detecting the interruption shall promptly notify the other party orally, and Payment Vendor shall promptly remedy the malfunction, with the assistance, if necessary, of the Agency's suppliers of maintenance services for the remote terminal equipment or telecommunications channels.

15 BACK-UP PROCEDURES

15.1 Customer to Back-Up Data.

The Agency shall maintain adequate back-up material that will enable the regeneration of Agency data, computer files, printer output, and other data in the event of loss, damage, or destruction of such data. Accordingly, the Agency shall produce and keep copies of the source documents of the information delivered to Payment Vendor and shall maintain a backup procedure for reconstruction of lost or altered Agency computerized files and records to the extent deemed necessary by the Agency.

15.2 Lost, Damaged, or Destroyed Data.

Payment Vendor shall use commercially reasonable measures to prevent the loss, damage, or destruction of the Agency's data. If the Agency's or Agency Client's data is lost, damaged, or destroyed after its transmission to Payment Vendor, Payment Vendor shall notify the Agency promptly, and the Agency will retransmit the data to Payment Vendor for processing. Both Payment Vendor and the Agency agree to co-operate reasonably to remedy any such loss, damage, or destruction and to enable the processing of the Agency's data by Payment Vendor as quickly as is reasonably possible.

16 FILE SECURITY

Payment Vendor shall take all reasonable steps to ensure that access to the Agency's computerized files and records is available only to Payment Vendor, the Portal Vendor, the Agency, Agency Clients, and, where appropriate, the Agency's authorized users. Payment Vendor reserves the right, at its own expense and with adequate notice to the Agency, to issue and change procedures from time-to-time to improve or protect file security.

17 DISCLAIMER

The Agency acknowledges and agrees that the Services are provided on an "as-is, as available basis," and Payment Vendor does not warrant that the Services will operate uninterrupted or error-free. Rather, the Services will be provided consistent with the attached SLA or any duly executed amendments thereto.

18 LIMITATIONS OF LIABILITY

Payment Vendor shall not be liable for any indirect, consequential, special, incidental, punitive, or other damages of any kind or nature whatsoever, whether claimed by the Agency or any other person, which arise out of the provision of the Services or the Agency's use of or reliance on them, except to the extent such damages result from Payment Vendor's negligence or willful misconduct.

19 INDEMNITIES

19.1 Payment Vendor's Indemnity of Customer.

Payment Vendor agrees to defend, indemnify, and hold the Agency, its officials, board members, officers, employees, agents, and authorized volunteers harmless from all liabilities, claims, injuries, damages, and expenses, including without limitation reasonable attorneys' fees, arising from any breach by Payment Vendor of its representations, warranties, covenants, or obligations under this Agreement or any acts or omissions related thereto. If a court of competent jurisdiction determines that this agreement is subject to RCW 4.24.115, then for any bodily injury or property damage caused by the concurrent negligence of Payment Vendor, on the one hand, and the Agency, its participating cities, and/or the Portal Vendor on the other, Payment Vendor's liability (including its duty to indemnify Agency for its costs of defense) is limited to the Payment Vendor's own proportionate fault or negligence.

In addition to all other indemnities, Payment Vendor shall defend, indemnify and hold the Agency and Agency Clients harmless from any damages, claims, liabilities, costs and expenses resulting from Payment Vendor's failure to be and to remain PCI DSS compliant.

19.2 Customer's Indemnity of Payment Vendor.

The Agency agrees to defend, indemnify, and hold Payment Vendor, its directors, officers, employees, agents, affiliates, suppliers, and vendors harmless from all liabilities, claims, and expenses, including without limitation reasonable attorneys' fees, arising from any breach by the Agency of its representations, warranties, covenants, or obligations under this Agreement. Notwithstanding the foregoing, the Agency is not obligated to defend or indemnify Payment Vendor against any claim, liability, damages, or expense resulting from Payment Vendor's own breach of this Agreement, negligence, or willful misconduct.

20 INSURANCE

Payment Vendor shall procure and maintain, for the duration of this Agreement and any renewal period, insurance against claims for injuries to persons or damage to property which may arise from or in connection with the performance of this Agreement by Payment Vendor, its agents, representatives, subcontractors, or employees. Payment Vendor's maintenance of insurance as required herein does not limit the liability of Payment Vendor to the coverage provided by such insurance or otherwise limit the Agency's recourse to any remedy available at law or in equity. Payment Vendor's insurance must be placed with insurers with a current A.M. Best rating of not less than A:VII.

20.1 Required coverages.

At a minimum, Payment Vendor shall obtain and maintain the following types of insurance:

(a) Automobile Liability insurance covering all owned, non-owned, hired, and leased vehicles. Coverage shall be written on Insurance Services Office (ISO) form CA 00 01 or a substitute form providing equivalent liability coverage. If necessary, the policy shall be endorsed to provide contractual liability coverage.

(b) Commercial General Liability insurance shall be written at least as broad as ISO occurrence form CG 00 01 and shall cover liability arising from premises, operations, stop-gap, independent contractors, and personal injury and advertising injury. The Agency shall be named as an additional insured under Payment Vendor's insurance policy with respect to the work performed for the Agency, using an additional-insured endorsement as least as broad as ISO CG 20 26.

(c) Technology Errors and Omissions/Professional Liability insurance for those services delivered pursuant to this Contract that, either directly through Payment Vendor's employees or indirectly through contractual or other arrangements with third parties, involve providing professional services. "Professional services" as used in this subsection include, but are not limited to, any services provided by any licensed professional.

(d) Workers' Compensation coverage as required by the Industrial Insurance laws of the State of Washington.

(e) Network Security (Cyber) and Privacy Insurance, including, but not limited to, coverage, including defense, for the following losses or services:

(i) Liability arising from theft, dissemination, and/or use of the Agency's confidential and personally identifiable information, including but not limited to, any information about an individual maintained by the Agency, including any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; taxpayer information; and any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information regardless of how or where the information is stored or transmitted.

(ii) Network security liability arising from the unauthorized access to, use of, or tampering with computer systems, including hacker attacks; or the inability of an authorized third party to gain access to supplier systems and/or Agency data, including denial of service, unless caused by a mechanical or electrical failure; or introduction of any unauthorized software computer code or virus causing damage to the Agency or any other third party data.

(iii) Lawfully insurable fines and penalties resulting or alleging from a data breach.

(iv) Event management services and first-party loss expenses for a data breach response including crisis management services, credit monitoring for individuals, public relations,

legal service advice, notification of affected parties, independent information security forensics firm, and costs to re-secure, re-create, and restore data or systems.

20.2 Minimum Limits.

Payment Vendor shall maintain at least the following minimum insurance limits:

(a) Automobile Liability insurance with a minimum combined single limit for bodily injury and property damage of no less than $1,000,000 per accident.

(b) Commercial General Liability insurance limits of no less than $1,000,000 per occurrence, $2,000,000 general aggregate.

(c) Technology Errors and Omissions/Professional Liability insurance with limits of no less than $1,000,000 per claim, $1,000,000 policy aggregate limit.

(d) Workers' Compensation insurance with statutory limits.

(e) Network Security (Cyber) and Privacy Insurance with limits no less than $1,000,000 per claim, $1,000,000 policy aggregate limit for network security and privacy coverage; $100,000 per claim for regulatory action (fines and penalties); and $250,000 per claim for event management services.

20.3 Required provisions.

Payment Vendor's Automobile Liability and Commercial General Liability insurance must contain, or be endorsed to contain, provision stating that they are primary insurance with respect to the Agency. Any insurance, self-insurance, or self-insured pool coverage maintained by the Agency is excess of Payment Vendor's insurance and will not contribute with it.

20.4 Notice of cancellation.

Payment Vendor shall provide the Agency written notice of any policy cancellation within two business days of Payment Vendor's receipt of such notice.

20.5 Coverage verification.

Payment Vendor shall furnish the Agency with original certificates and a copy of the amendatory endorsements, including but not limited to the additional insured endorsement, evidencing the minimum insurance requirements of this Agreement. Certificates of coverage and endorsements required hereunder must be delivered to the Agency within thirty (30) days of execution of this Agreement.

20.6 Failure to Maintain Insurance.

Payment Vendor's failure to maintain the required insurance constitutes a material breach of this Agreement. If such breach is not cured within five (5) business days after demand by the Agency to Payment Vendor, the Agency may immediately terminate the contract or, at its discretion, procure or renew such insurance and pay any and all premiums in connection therewith, with any sums so expended to be repaid to the Agency on demand, or at the sole discretion of the Agency, offset against funds due Payment Vendor from the Agency.

20.7. Availability of Full Coverage Limits.

If Payment Vendor maintains higher insurance limits than the minimums listed above, the Agency will likewise be insured for the full available limits of Commercial General and Excess or Umbrella liability maintained by Payment Vendor, irrespective of whether such limits maintained by Payment Vendor are greater than those required by this Agreement or whether any certificate of insurance furnished to the Agency evidences limits of liability lower than those actually maintained by Payment Vendor.

20.8. Self Insurance.

Any self-insured retention not fronted by an insurer must be disclosed. Any defense costs or claim payments falling within a self-insured retention are the responsibility of Payment Vendor.

21 CONFIDENTIALITY AND PRIVACY

21.1 Confidential Information.

For the purposes of this Section, "**Confidential Information**" includes:

(a) non-public financial information concerning either party;

(b) information about either party's product line (both current and planned), research, development, customer data, and pricing and marketing plans, unless and until publicly announced;

(c) customer billing information;

(d) any information designated as confidential in writing at or prior to disclosure;

(e) any information otherwise disclosed in a manner consistent with its confidential nature;

(f) "tax information" and "taxpayer identity," as those terms are defined in RCW 82.32.330(c) and (e), respectively; and

(g) "Personal information," as that term is defined in RCW 19.255.010.

For the purposes of this Section, "**Confidential Information**" specifically excludes information that:

(a) has become publicly known without breach of this Agreement or any other confidentiality obligation by the receiving party;

(b) has been given to the receiving party by a third party with a legal right to so disclose;

(c) was known to the receiving party at the time of disclosure as evidenced by its written records;

(d) was independently developed by the receiving party; or

(e) is required to be disclosed by applicable law.

Each party agrees to use good faith efforts, and at least the same care that it uses to protect its own Confidential Information of like importance, to prevent unauthorized dissemination or disclosure of the other party's Confidential Information both during and after the Term of this Agreement. In addition, each party may use the other party's Confidential Information solely as necessary for the performance of this Agreement. Payment Vendor acknowledges that the Agency and its participating cities are subject to Washington's Public Records Act, RCW 42.56, and nothing in this Agreement is intended to limit or restrict the Agency or its participating cities from complying with any disclosure obligations imposed by state law.

21.2 Privacy of Customer's Clients.

Payment Vendor's Privacy Policy, attached hereto as Schedule B, applies to all data received by Payment Vendor from the Agency pursuant to this Agreement. In the event of a conflict between Schedule B and/or D and Section 21 of this Agreement, Section 21 controls. Except as provided herein, Payment Vendor will comply with all applicable laws relating to personal, confidential, and/or financial information and will not share any such information with any other companies, the government, or any third party without the express written consent of the owner of the information, unless required to do so by law or court order. Payment Vendor may not sell information it receives from the Agency or the Agency's customers to any party.

Payment Vendor may not use or disclose Confidential Information in any manner that would constitute a violation of federal law or applicable provisions of Washington State law. Payment Vendor agrees to comply with all federal and state laws and regulations, as currently enacted or revised, regarding data security and electronic data interchange of Confidential Information.

Payment Vendor shall ensure its directors, officers, employees, subcontractors and agents use Confidential Information solely for the purposes of accomplishing the services set forth in the Agreement. Payment Vendor shall protect Confidential Information collected, used, or acquired

from the Agency or its customers against unauthorized use, disclosure, modification, or loss by using the same or greater level of care that it uses with its own Confidential Information, and not less than reasonable care. Payment Vendor agrees to implement physical, electronic, and managerial policies, procedures, and safeguards to prevent unauthorized access, use, or disclosure of Confidential Information.

Payment Vendor shall notify the Agency in writing immediately upon becoming aware of any unauthorized access, use or disclosure of Confidential Information belonging to the Agency or its customers. Payment Vendor shall take necessary steps to mitigate the harmful effects of such use or disclosure. Payment Vendor is financially responsible for notification of any unauthorized access, use, or disclosure, but must consult with the Agency before providing such notice. The details of the notification must be approved by the Agency.

Payment Vendor shall certify the return or destruction of all Confidential Information of the Agency or its customers upon expiration or termination of the Agreement, and Payment Vendor may not retain copies. If Payment Vendor and the Agency mutually determine that return or destruction is not feasible, Payment Vendor may not use the Confidential Information in a manner other than those permitted or authorized by state and federal laws.

Any breach of this subsection is grounds for termination of this agreement.

21.3 Security of Cardholder Data.

Payment Vendor confirms that it will maintain all applicable PCI DSS requirements to the extent that it handles, has access to, or otherwise stores, processes, or transmits the Agency's customers' cardholder data or sensitive authentication data or manages the Agency's data environment on behalf of the Agency. Additionally, the Payment Vendor shall must make the ROC available to the Agency and Agency Clients. The Payment Vendor will, on an annual basis, address PCI compliance requirements in a manner that minimizes risk to the Agency and Agency Clients while also minimizing the Agency and Agency Clients participation in PCI related activities.

21.3.1 Payment Card Industry Data Security Standard (PCI DSS)

21.3.1.1 Payment Vendor shall obtain any agreement, approval, and any permits necessary from all major credit card institutions (such as Visa, MasterCard, Discover, etc.) The Payment Vendor shall maintain PCI compliance.

21.3.1.2 Payment Vendor is responsible for the security of cardholder data that it possesses, including the functions relating to storing, processing, and transmitting of the cardholder data.

21.3.1.3 Payment Vendor affirms that, as of the effective date of this contract, it has complied with all applicable requirements to be considered PCI DSS compliant, and has performed the necessary steps to validate its compliance with the PCI DSS.

21.3.1.4 Payment Vendor will supply the most current PCI DSS compliance status by providing evidence of its most recent validation of compliance (Attestation of Compliance -AOC preferred) upon execution of this addendum to the Agency's designated Project

Manager or Buyer. Thereafter, Payment Vendor will supply to the Agency and Agency Clients Information Security Officer ("CISO") a new PCI DSS compliance status report or AOC annually.

21.3.1.5 Payment Vendor will demonstrate the compliance of any third party it has sub-contracted as part of the service offering. As evidence of compliance, the Payment Vendor shall provide on an annual basis a current attestation of compliance signed by a PCI QSA (Qualified Security Assessor)

21.3.1.6 Payment Vendor will immediately notify the Agency if it learns that it or a subcontractor is no longer PCI DSS compliant and will immediately provide the Agency with the steps being taken to remediate the non-compliance status. In no event should Payment Vendor's notification to the Agency be later than five (5)calendar days after Payment Vendor learns it or a subcontractor is no longer PCI DSS complaint.

21.3.2 Unauthorized Access to Cardholder Data

21.3.2.1 In the event of a confirmed breach or intrusion or otherwise unauthorized access to cardholder data stored at or for Payment Vendor, Payment Vendor shall notify the Agency Program Manager within 24 hours to allow the proper PCI DSS compliant breach notification process to commence.

21.3.2.2 Payment Vendor shall provide appropriate payment card companies, acquiring financial institutions and their respective designees access to the Payment Vendor's and subcontractor's facilities subject to 72 hours prior written notice and all pertinent records to conduct a review of the Payment Vendor's and subcontractor's compliance with the PCI DSS requirements

21.4 Use of Aggregated Data.

The Agency agrees that Payment Vendor may aggregate data it receives from or on behalf of the Agency with data gathered from other Payment Vendor customers to create non-customer specific metrics and statistics (e.g. benchmarking, response analysis and modeling). In no event may such aggregated data identify the Agency or the Agency's customers.

22 PUBLICITY

Neither party may refer to the other party directly or indirectly in any media release, public announcement, or public disclosure relating to this Agreement or its subject matter, in any promotional or marketing materials, lists, or business presentations without consent from the other party for each such use or release in accordance with this section; however, Payment Vendor may include the Agency's name in Payment Vendor's customer list and may identify the Agency as its customer in its sales presentations and marketing materials without obtaining the Agency's prior consent. Notwithstanding the foregoing, at Payment Vendor's request the Agency agrees to issue a joint press release prepared by Payment Vendor to announce the relationship established by the parties hereunder. The Agency agrees that such press release shall be deemed approved by the Agency in the event that, within ten (10) Business Days of receiving Payment

Vendor's proposed press release, the Agency does not provide written notice to Payment Vendor describing in reasonable detail the Agency's objections to the press release.

23 BINDING EFFECT

This Agreement is binding upon and inures to the benefit of the parties hereto and their respective heirs, successors, and permitted assigns. Neither party may voluntarily, or by operation of law, assign or otherwise transfer of all or any part of its rights, obligations, or other interests in or under this Agreement without the other party's prior written consent, which consent may not be unreasonably withheld. Any attempt to assign or transfer rights, obligations, or interests in violation of this provision is null and void. Notwithstanding anything else contained herein, Payment Vendor may assign this Agreement or any rights hereunder without the consent of the Agency, in the event of a merger, sale of assets or business, or other transfer of control by operation of law or otherwise, but only if the assignee expressly agrees in writing to assume all obligations and rights hereunder, and a copy of that agreement is promptly provided to the Agency.

24 CHANGES TO AGREEMENT

Except as otherwise provided for in this Agreement, this Agreement may not be amended or modified in any respect except by written instrument executed by both the Agency and Payment Vendor.

25 DELAYS AND FORCE MAJEURE

Time is of the essence for all parts of this Agreement requiring performance of an act. Except as otherwise expressly provided in this Agreement, neither party may be considered in breach or otherwise held responsible for delays or failures in performance resulting from acts or events beyond the party's reasonable control, including but not be limited to acts of God or Nature, strikes, lock-outs, riots, acts of war, acts of terrorism, epidemics, governmental regulations imposed after the fact, fire, earthquakes, floods, or other disasters. In case of such act or event, the dates and times for performance will be automatically extended for the period of time that Payment Vendor or the Agency, as the case may be, is prevented or inhibited from timely performance.

26 ENTIRE AGREEMENT

This Agreement (including its schedules) supersedes and merges all prior agreements, promises, understandings, statements, representations, warranties, indemnities, and covenants and all inducements to the making of this Agreement relied upon by either party, whether written or oral, and embodies the parties' complete and entire agreement with respect to the subject matter hereof. No statement or agreement, oral or written, made before the execution of this Agreement may vary or modify the written terms hereof in any way whatsoever.

27 INTERPRETATION OF AMBIGUITIES

Neither party to this Agreement is entitled to the benefit of any preferential construction of its meaning on account of the other party having been the sole or primary drafter.

28 THIRD PARTY BENEFICIARIES

Except as expressly provided herein, nothing in this Agreement is intended to confer any rights or remedies on any third party.

29 SEVERABILITY

If any term or provision of this Agreement is determined to be illegal, unenforceable, or invalid in whole or in part for any reason, such illegal, unenforceable, or invalid provision(s) or part(s) shall be stricken from this Agreement and such provision(s) or part(s) will not affect the legality, enforceability, or validity of the remainder of this Agreement, except where enforcing the remaining provisions in the absence of the stricken provision(s) would frustrate an essential purpose of this Agreement. If any provision or part thereof of this Agreement is stricken in accordance with the provisions of this Section, then the parties agree to replace the stricken provision, to the extent possible, with a legal, enforceable, and valid provision that is similar in tenor to the stricken provision.

30 REPRESENTATION OF AUTHORITY

Each party represents and warrants to the other that the execution and delivery of this Agreement and the performance of such party's obligations hereunder have been duly authorized and that the Agreement is a valid and legal agreement binding on such parties and enforceable in accordance with its terms.

31 FURTHER ASSURANCES

The parties shall at their own cost and expense execute and deliver such further documents and instruments and shall take such other actions as may be reasonably required or appropriate to carry out the intent and purposes of this Agreement.

32 LEGAL COMPLIANCE

This Agreement is made expressly subject to all present and future valid orders, rules, regulations, and laws of any regulatory body having jurisdiction over the subject matter hereof. In the event this Agreement, or any of its provisions, is found contrary to or in conflict with any such order, rule, regulation, or law, this Agreement will be deemed modified to the extent necessary to comply with any such order, rule, regulation, or law and shall be modified in such a way as is consistent with the form, intent, and purpose of this Agreement.

33 GOVERNING LAW AND JURISDICTION

This Agreement is made under and shall be construed in accordance with the laws of the State of Washington, excluding its rules governing conflict of laws. The parties hereby submit to the jurisdiction of the state and federal courts located in King County, Washington, for any judicial proceedings relating to this Agreement, including any proceedings seeking emergency or preliminary injunctive relief.

34 ARBITRATION

Any dispute, controversy, or claim between or among the parties arising out of or relating in any way to this Agreement or any related agreements or instruments, including any claim based on or arising from an alleged tort, shall be determined by binding arbitration. Each party waives its right to a jury trial and agrees to arbitration in accordance with the following:

(a) The arbitration shall be heard by a single arbitrator, who is qualified and has the expertise necessary to hear the matter, as mutually agreed to by the parties. If the parties are unable to agree upon a single arbitrator, either party may apply to the King County Superior Court to request the appointment of a single arbitrator;

(b) The arbitration shall take place in King County, Washington, or in such other place as the Payment Vendor and the Agency may agree upon in writing;

(c) All meetings and hearings shall be in private and remain confidential, unless the parties otherwise agree in writing; however nothing in this Section 34 prohibits or is intended to prohibit the Agency from complying with its obligations under the Public Records Act, RCW 42.56.

(d) The arbitration shall be conducted in accordance with the Commercial Arbitration Rules of the American Arbitration Association;

(e) Judgment on the award rendered by the arbitrator may be entered in any court of competent jurisdiction; and

(f) Notwithstanding the duty to arbitrate disputes arising from or related to this Agreement, any party may seek emergency, temporary, or preliminary injunctive relief in the state or federal courts situated in King County, Washington, to avoid imminent and irreparable harm pending resolution of a related arbitration.

35 INDEPENDENT CONTRACTOR

The relationship of Payment Vendor to the Agency by reason of this Agreement is that of an independent contractor. This Agreement does not authorize Payment Vendor to act as the agent or legal representative of the Agency or any participating city for any purpose whatsoever. Payment Vendor is not granted any express or implied right or authority to assume or create any

obligation or responsibility on behalf of or in the name of the Agency or any participating city, nor to bind them in any manner or thing whatsoever. It is the intention and understanding of the parties that Payment Vendor shall be an independent Payment Vendor and that the Agency shall be neither liable for nor obligated to pay sick leave, vacation pay or any other benefit of employment, nor to pay any social security or other tax that may arise as an incident of employment. Payment Vendor shall pay all income and other taxes as due. Industrial or other insurance that is purchased for the benefit of the Payment Vendor does not convert this Agreement into any employment contract. Payment Vendor is an independent contractor responsible for complying with all obligations of an employer imposed under federal or state law. Personnel employed by Payment Vendor do not acquire any rights or status regarding the Agency. Payment Vendor warrants that it did not pay, employ, or retain any company or person, other than a bona fide employee working solely for the Payment Vendor, to solicit or secure this Agreement. For breach or violation of this warranty, the Agency may terminate this Agreement without liability.

36 COUNTERPARTS

This Agreement may be executed in several counterparts, each of which constitutes an original, but all of which constitute one and the same instrument. The reproduction of signatures by facsimile or such similar device will be treated as binding as if original, and each party hereto undertakes to provide each and every other party hereto with a copy of the Agreement bearing original signatures reasonably promptly upon demand.

37 NOTICES

Any notice or other communication required or permitted to be given hereunder shall be in writing and shall be given by e-mail, facsimile, or other means of electronic communication, or by hand-delivery as hereinafter provided. Any such notice or other communication, if sent by e-mail, facsimile, or other means of electronic communication, will be deemed to have been received on the business day following the sending, or, if delivered by hand, will be deemed to have been received at the time it is delivered to the applicable address noted below either to the individual designated below or to an individual at such address having apparent authority to accept deliveries on behalf of the addressee. Notice of change of address are also governed by this Section. Notices and other communications shall be addressed as follows:

For the Payment Vendor:

5050 Tomken Road
Attention: Rick Watkin, President and CEO
Mississauga ON
Canada L4W 5B1
Fax: 905-624-2886
E-Mail: rick.watkin@kubra.com

For the Customer:

FileLocal
Attention: Kevin Fitzpatrick, Program Manager
Seattle Municipal Tower, Room 4080
700 5th Avenue
Seattle, WA 98104
Fax:
E-Mail: Kevin.Fitzpatrick-FLO@seattle.gov

38 EXECUTION OF SEPARATE AGREEMENTS

The Agency is aware that Payment Vendor utilizes third-party consolidators, distribution partners, and electronic payment service Payment Vendors (including but not limited to the United States and Canadian Postal Services, CheckFree, and Paymentech). The Agency agrees to execute separate agreements with these third parties as necessary to facilitate Payment Vendor's provision of Services.

39 PAYMENT PROCESSING SERVICES

The parties hereby agree to the terms relating to the payment processing component of the Services as set out in the attached Schedule D and hereby acknowledge and agree that such Schedule and the terms and conditions set out therein are binding terms of this Agreement. The parties agree to sign the Submitter Merchant Payment Processing Instructions and Guidelines Agreement substantially in the form of Schedule E attached hereto.

40 ADDITIONAL REQUIREMENTS

Any local government entity or public agency that wishes to accept tax payments or licensing fees through the Multi-City Business License and Tax Portal Solution must accept the terms of this Agreement including those relating to the payment processing component of the Services as set out in the attached Schedule D. The local government entity or public agency must also sign the Submitter Merchant Payment Processing Instructions and Guidelines Agreement substantially in the form of Schedule E attached hereto.

AGREED TO BY:

WASHINGTON MULTI-CITY BUSINESS LICENSE AND TAX PORTAL AGENCY

By: _____ Date: _____
Kevin Fitzpatrick, Program Manager

and

KUBRA DATA TRANSFER, LTD.

By: _____ Date: _____

Rick Watkin, President & CEO

SCHEDULE A

SERVICES AND CHARGES

Transactional Pricing

Profile / Set-up	
Supported Channels	WEB
City(s) Supported	Seattle, Bellevue, Everett, Tacoma & File Local Agency
API integration	e-Gov Systems
Customer Authentication	Summary data
Remittance file	Standard
Timelines / Funds availability	8:00 PM EST / Next business Day*
*Next Day Settlement Requires the funds to be Wired	$10.00 per Wire
Payment Processor	Chase Paymentech
Voice Over's	KUBRA
Convenience fee [B2C]	3.00% - CC/DC
Payment Types	ACH - $1.00 each
	Credit Card [Visa/MasterCard/Discover]
	Signature debit [Visa/MasterCard/Discover]
	ATM PIN-less debit [Star, NYCE, Pulse]

Notes:

- The Convenience Fee Amount is reviewed on a regular basis for any material change in fees assessed from the card association, interchange and / or gateway fees. In the event of a material change in any of the assessed fees, KUBRA reserves the right to increase / decrease the amount of the Convenience fee. KUBRA will provide data and consult with the City prior to any change in the Convenience Fee amount.
- All ACH returns (i.e. NSF) or CC charge backs will be billed back to the applicable City based on the convenience fee per return or charge back (i.e. if you have 5 returns in March you will receive an invoice from KUBRA equal to 5 times the current convenience fee being applied to the end customer).
- A Merchant Agreement will need to be signed between KUBRA, Chase Paymentech, FileLocal and each applicable City in order to generate the Merchant ID's

- Each applicable City must agree to the terms of this Agreement including the Payment Processing Terms and Conditions
- American Express is not Supported
- Standard Settlement (+2 Business days) – No additional Fees
- Next Day Settlement- incurs wire fees per file per participating City
- Post implementation Professional Services hours are billed out at **$165.00** per hour for adjustments to the in-production system. An estimate will be created with respect to the number of billable hours required and a statement of work signed prior to work commencing.

SCHEDULE B

KUBRA PRIVACY POLICY

At **KUBRA DATA TRANSFER LTD.** ("Kubra", "we", "our" or "us"), we are committed to protecting the privacy and the confidentiality of personal information of our customers and our customer's clients (collectively, "Customers") and employees ("Employees"). In order to comply with applicable privacy legislation and to instill confidence in our Customers and Employees that the personal information they entrust to us is safe, we have developed this Privacy Policy. We want our Customers and Employees to know why we ask for their personal information, how we use it, what safeguards we employ and how to contact us with privacy-related questions.

In this Privacy Policy, "Personal Information" means information that specifically identifies a Customer or Employee as an individual and is provided to or collected by Kubra. The type of personal information Kubra collects, uses and discloses may include a Customer's or Employee's name, age, gender, residential mailing address, residential phone numbers or email addresses, financial, credit and banking information, social insurance number (and other identification numbers), employment experience (past and present) and records, health information and tax records. Personal Information does not, however, include a Customer's or Employee's business title, business address or business telephone number in such individual's capacity as an employee of an organization or enterprise.

In this Privacy Policy, "Personal Health Information" includes information concerning an Employee's physical or mental health collected or generated in the course of Kubra providing an Employee with health services or benefits. In the case of Employees, Personal Information will also include Personal Health Information and all applicable information contained in the Employee's personnel file.

I. IDENTIFYING THE PURPOSES AND USE OF PERSONAL INFORMATION

Before collecting any Personal Information, Kubra will identify why the Personal Information is required and how it will be used. This Personal Information is documented and kept on file at Kubra's offices at 5050 Tomken Road, Mississauga Ontario, Canada L4W 5B1. Kubra will obtain the Customer's or Employee's consent before using or disclosing Personal Information for purposes other than the original reasons given.

Kubra collects and uses Customer's Personal Information for the following purposes:

- Administration, recording and using Personal Information relevant to the relationship between the Customer and Kubra;
- Protecting against fraud and error;
- Offering Customers additional investment opportunities which may be of interest to such Investor;
- Communicating with a Customer generally;
- Communicating Personal Information to an agent, intermediary or other third party during the course of a contract or mandate for the performance of any of the purposes listed in this Privacy Policy;
- Complying with all applicable laws; and
- Such other specific purposes which are communicated to a Customer by Kubra and its representatives before collection of the Personal Information.

Kubra collects and uses an Employee's Personal Information for the following purposes:

- Decision-making regarding an Employee's hiring, duties, transfer, training, discipline, promotion and retention;
- Recording and determining an Employee's eligibility for participation in various Kubra benefit plans, including health and dental benefits;
- Compliance with all municipal, provincial, federal and other applicable laws regarding an Employee;
- Recording and maintaining an Employee's attendance record, service award and bonuses record, performance evaluations, performance improvement plans, remuneration details, or maintaining any other necessary information for establishing, managing or terminating the employment relationship (including its related benefits), as well as the determination of the applicable income and benefits; and
- Such other specific purposes which are communicated to the Employee by Kubra and its representatives before collection of the Personal Information.

We may use, share and disclose a Customer's or Employee's Personal Information to our affiliates, associates, agents, suppliers and such other third parties as Kubra, acting reasonably, may deem necessary for the fulfillment of the purposes noted above or where otherwise permitted by law.

In the unlikely event that Kubra or substantially all of its assets are acquired by a third party, a Customer's and Employee's Personal Information may be one of the assets transferred to such third party and Kubra may reasonably disclose such Personal Information to a prospective third party Taxpayer.

II. CONSENT

Except in certain extraordinary circumstances, Kubra does not collect, use or disclose a Customer's or Employee's Personal Information without their knowledge and consent. Such extraordinary circumstances may include, without limitation, when legal, medical or security reasons make it impossible or impractical to obtain consent.

The Customer's and Employee's consent will be obtained at the time of collection of the Personal Information, or when a new use for the Personal Information is identified. A Customer or Employee may withdraw their consent at any time, subject to any legal or contractual restrictions and on the provision of reasonable notice to Kubra. If a Customer or Employee chooses to withdraw his or her consent, he or she is required to do so in writing to the Chief Compliance Officer (please see section VII of this Privacy Policy). Any implications to withdrawing consent will be explained to the Customer or Employee at the time written notice of such withdrawal is received by Kubra. Such implications may include, but are not limited to, a breakdown, interruption or cessation of Kubra's relationship with the Customer or Employee.

By becoming an employee of Kubra, Employees have consented to the disclosure of their Personal Information to a third party in the circumstances, or for the purposes, set out in this Privacy Policy.

III. LIMITING COLLECTION

Kubra limits the collection of a Customer's or Employee's Personal Information to that which is necessary for the purposes identified in this Privacy Policy, or for any additional purpose identified to the Customer or Employee before collection of the Personal Information.

IV. LIMITING USE, DISCLOSURE AND RETENTION

Personal Information is not used or disclosed for purposes other than those for which it was originally collected, except with the consent of the Customer or Employee, or as permitted by law. Personal Information is only retained as long as may be necessary for the fulfillment of these purposes, or to meet government requirements, whichever is longer, following which it is destroyed, erased, or rendered anonymous.

V. ACCURACY

Kubra strives to ensure that Customer's or Employee's Personal Information is as accurate, complete and up to date as necessary for the purposes for which it is used. Information is updated only when necessary to fulfill specified purposes. Employees are required to notify Kubra of a change of Personal Information as soon as possible for payroll and tax purposes.

VI. SAFEGUARDS

Kubra has security safeguards in place designed to protect against loss, theft, unauthorized access, disclosure, copying, use or modification of Personal Information under the care of Kubra. The nature of the safeguards depends on the sensitivity, format, location and storage of the Personal Information. These security measures may from time to time include locked cabinets, computer passwords, software firewalls to stop hackers, encryption software, restricting access to Personal Information to only those employees or representatives who have a need to know and, if deemed necessary by Kubra in its sole discretion, confidentiality covenants from third parties to whom Personal Information has been disclosed.

E-mail is not a 100% secure medium, and Customers and Employees should be aware of this when contacting us to send Personal Information.

VII. ACCOUNTABILITY AND OPENNESS

Kubra is responsible for the Personal Information under its control and has appointed a Chief Compliance Officer to ensure that we comply with all applicable privacy legislation and the terms of this Privacy Policy. All employees involved in maintaining or collecting Personal Information are trained via this Privacy Policy. Personal Information provided to third party service Payment Vendors with whom Kubra has a contractual agreement will have levels of protection comparable to the internal protection of Personal Information maintained at Kubra.

The Chief Compliance Officer addresses and investigates questions or concerns regarding Customer's or Employee's Personal Information. The Chief Compliance Officer may be reached by mail at Kubra Data Transfer Ltd, 5050 Tomken Road, Mississauga Ontario, Canada L4W 5B1, Attention: Chief Compliance Officer, or by telephone at (905) 624-2220. Copies of this Privacy Policy and any future updates or amendments hereto are available at www.kubra.com and upon request from Kubra.

VIII. INDIVIDUAL ACCESS

Upon written request of a Customer or Employee, Kubra will provide such Customer or Employee with access to his or her Personal Information. Kubra will correct or amend any inaccuracies in the

Customer's or Employee's Personal Information, and such amended information will be forwarded to any third parties who require access to the information. Kubra has the right to refuse a request for access to Personal Information:

- If the information is protected by legal privilege;
- If granting access would reveal confidential commercial or financial information;
- If doing so would reasonably be expected to threaten the life or security of another individual;
- If the information was collected for purposes related to the detection and prevention of fraud;
- If the information was generated in the course of a formal dispute resolution process;
- If the information would likely reveal Personal Information about another Customer or Employee, as the case may be;
- If the request is vexatious or frivolous; or
- To protect Kubra's rights and property.

If the request of a Customer or Employee for such individual's Personal Information is denied, the individual will be informed in writing of the reasons for the denial, as well as any recourse available to such individual.

Access to Customer's or Employee's Personal Information will be at no cost to such Customer or Employee. Minimal charges may apply, however, for the transcription, reproduction or transmission of documents containing Personal Information.

IX. CHALLENGING COMPLIANCE

If a complaint ("Complaint") regarding Kubra's handling of Personal Information is received, an individual (the "Investigator") with the skills necessary to conduct an investigation fairly and impartially will be assigned. The Investigator will have access to all relevant records and will be permitted to speak with the Employee(s) who handled the Personal Information access request. The complainant will receive notification of the outcome of the investigation clearly and promptly. Any inaccurate Personal Information or policy/procedure changes will be modified, if necessary, based on the outcome of the Complaint.

X. CURRENCY OF THIS PRIVACY POLICY

Kubra reserves the right to change this Privacy Policy at any time and from time to time. Any changes or additions to section I of this Privacy Policy regarding those situations where Kubra will collect, use or disclose Personal Information will not apply to a Customer or Employee without the prior consent of such Customer or Employee. All Customers and Employees are encouraged to contact Kubra to determine if any updates have been made to this Privacy Policy.

SCHEDULE C

SERVICE LEVEL AGREEMENT

[SLA TO BE INSERTED ONCE THAT DOCUMENT IS FINALIZED.]

SCHEDULE D

PAYMENT PROCESSING TERMS

1.1 **Transactions.** In furtherance of the provision of the Services, Customer shall submit certain data to Payment Vendor which is the evidence and electronic record of taxpayer transactions ("**Transactions**") between Customer and taxpayer("**Taxpayers**") representing payment by the Taxpayer by (i) credit or debit cards ("**Cards**") or (ii) electronic check processing, through either ACH or facsimile draft transactions ("**ECP**"), which Customer accepts from Taxpayers as payment for their purchases from Customer, and for which Payment Vendor agrees to submit to a third party electronic payment service Payment Vendor ("**Payment Processor**") on Customer's behalf for payment processing.

1.2 **Certain Card Acceptance Policies**. Each sale Customer makes involving a Card shall be evidenced by a Transaction record completed with the transaction date and the transaction amount, and other information as required by (i) Payment Processor, or (ii) the group of Card issuer banks or debit networks that facilitate the use of payment cards (the "**Associations**"), such as the systems operated by MasterCard International, Inc., Visa, Inc. and NYCE, Pulse, Star, and Interlink debit networks. With respect to any Transaction for which a Card is not physically presented, such as in any on-line, mail, telephone or pre-authorized transaction, Customer must have notified Payment Vendor in writing of its intention to conduct such Transactions and Payment Vendor has agreed to accept them. Notwithstanding the foregoing, Customer acknowledges that under the bylaws, rules and regulations of the Association, as they exist from time to time (the "**Association Rules**"), Customer cannot rebut a reversal of a Card sale it previously presented (a "**Chargeback**") where the Taxpayer disputes making the purchase without an electronic record or physical imprint of the Card.

1.3 **ECP Transactions**. Each ECP Transaction shall be evidenced by a Transaction record completed with the sale date and the sale amount, and other information as required by (i) Payment Processor, or (ii) the National Automated Clearing House Association ("**NACHA**"). Customer warrants that the content of the sales data submitted to Payment Vendor in respect of each ECP Transaction is accurate, including the fact that the amount of the Transaction is correct, that the account number and financial institution's ABA number are correct, and that the entry is timely. Customer will not reinitiate ECP Transactions once they have received a "Payment Stopped" as a reason for an ECP Return (as hereinafter defined), unless an authorization from the Taxpayer overriding the "Payment Stopped" has been received. For the purposes of this Agreement, "ECP Return" means the reversal of an amount for which Customer has previously presented as an ECP Transaction, as the result of (i) a non dollar transaction sent to Payment Processor by the

receiving institution which advises that the data contained in the original transaction is either incorrect or has been changed ("**Notification of Change**"), and the Notification of Change provides the correct data allowing for the processing of the transaction; (ii) being initiated by the Taxpayer's bank at the request of the Taxpayer or may be caused due to invalid account data or insufficient funds at the receiving institution; or (iii) any reason allowed by Federal Reserve Regulations pertaining to the ACH system.

1.4 **Requirements for Transactions.** As to each Transaction Customer tenders to Payment Vendor for processing, Customer represents and warrants that:

(a) The Transaction represents payment or refund of payment, for the bona fide sale or lease of the goods, services or both;

(b) The Transaction does not involve any element of credit for any purpose other than payment for a current transaction (including payment of a previously-dishonoured check) and, except in the case of approved instalment or pre-payment plans, the goods have been shipped or services actually rendered to the Taxpayer;

(c) The Transaction is free from any material alteration not authorized by the Taxpayer;

(d) Neither the Customer nor a Customer employee has advanced any cash to the Taxpayer or to the Customer or to any of Customer's representatives, agents or employees in connection with the Transaction, nor has Customer accepted payment for effecting credits to a Taxpayer's account;

(e) Customer has made no representations or agreements for the issuance of refunds except as it states in the Customer's return/cancellation policy, which has been previously submitted to us in writing as provided below;

(f) Customer has no knowledge or notice of information that would lead Customer to believe that the enforceability or collectability of the subject Transaction is in any manner impaired, and the Transaction is in compliance with all applicable laws, ordinances, and regulations;

(g) all Transactions have been originated in compliance with this Agreement and the Association Rules; and

(h) For a sale where the Taxpayer pays in instalments or on a deferred payment plan, a Transaction record has been prepared separately for each instalment transaction or deferred payment, as applicable, on the date(s) the Taxpayer agreed to be charged. All instalments and deferred payments, whether or not they have been

submitted to Payment Vendor for processing, shall be deemed to be a part of the original sale.

1.5 **Lack of Authorization**. Payment Vendor reserves the right to refuse to process any Transaction presented by Customer (i) unless a proper authorization/approval code is recorded, (ii) if Payment Vendor reasonably determines that the Transaction is or will become uncollectible from the Taxpayer to which the Transaction would otherwise be charged, or (iii) if Payment Vendor determines that the Transaction was prepared in violation of any provision of this Agreement.

1.6 **Refunds and Adjustments**. Customer is required to maintain a fair policy with regard to the return/cancellation of goods or services and adjustment of sales. Customer is required to disclose to its customers, and to Payment Vendor, Customer's return/cancellation policy. The amount of the refund/adjustment cannot exceed the amount shown as the total on the original Transaction except by the exact amount required to reimburse the Taxpayer for postage that the Taxpayer paid to return the goods. Customer is not allowed to accept cash or any other payment or consideration from a Taxpayer in return for preparing a refund to be deposited to the Taxpayer's account nor to give cash refunds to a Taxpayer in connection with a sale, unless required by law.

1.7 **Authorized Bank Accounts**. In order to receive funds from Payment Processor and/or Payment Vendor, Customer must maintain one or more bank accounts at a bank that is a member of the Automated Clearing House system and the Canadian Payment Association (the "**Customer Accounts**"). Customer agrees that it shall not close a Customer Account without giving Payment Vendor at least four (4) days' prior written notice and substituting another bank account, if necessary. Customer is solely liable for all fees and costs associated with the Customer Accounts and for all overdrafts. Payment Vendor acknowledges that Payment Processor will initiate electronic credit and debit entries and adjustments to the Customer Accounts at any time without respect to the source of any monies in the Customer Accounts, and such will be the case until Payment Vendor and/or Payment Processor notifies Customer's bank that all monies due from Customer under this Agreement have been paid in full. Payment Vendor will not be liable for any delays in receipt of funds or errors in bank account entries caused by third parties, including but not limited to delays or errors by the Associations or Customer's bank.

1.8 **Travel and Entertainment Cards**. Customer cannot submit any Transaction through a travel and entertainment Card issued by American Express, or any other travel and entertainment Card for which Payment Vendor may agree to accept submissions in the future ("**T&E Card**"), for processing, unless Customer has in effect a valid agreement with the respective T&E Card company. Upon transmission of a T&E Card Transaction by

Customer, Payment Processor will forward the Transaction to the appropriate T&E Card company. Except to the extent that Payment Processor may provide funds settlement services for American Express, payment of the proceeds due to Customer will be governed by whatever agreement Customer has with that T&E Card company, and Payment Vendor does not bear any responsibility for a T&E Card company's performance. If Customer's agreement with a T&E Card company requires the T&E Card company's consent for Payment Vendor or for Payment Processor to perform the Services, Customer is responsible for obtaining that consent.

1.9 **Negative Amounts**. To the extent Transactions do not represent sufficient credits or the Customer Accounts do not have a sufficient balance to pay amounts due from Customer under this Agreement, Payment Vendor may pursue one or more of the following options: (i) demand and receive immediate payment for such amounts; (ii) debit the Customer Accounts for the amount of the negative balance; (iii) withhold Customer's settlement payments until all amounts are paid; (iv) delay presentation of Customer's refunds until Customer makes a payment to Payment Vendor of a sufficient amount to cover the negative balance; or (v) pursue any remedies Payment Vendor may have at law or in equity. Furthermore, if the amount represented by the Transactions in any day is negative due to refunds/customer credits being submitted by Customer in excess of Customer's sales, Customer is required to provide Payment Vendor with sufficient funds prior to the submission of the Transactions so as to prevent the occurrence of a negative balance.

1.10 **Delinquency/Customer Fraud**. If (i) there is a material, adverse change in Customer's financial condition or payment record with creditors, or if Customer is in material default of this Agreement; (ii) Customer is receiving excessive Chargebacks or ECP Returns; (iv) Customer significantly alters the nature of Customer's business or product lines; or (v) if Payment Vendor has reasonable grounds to believe that Payment Vendor or Payment Processor may be liable to third parties for the provisional credit extended to Customer, or that Customer may be liable to its Taxpayers, Card issuing banks, NACHA or the Associations, Payment Vendor may temporarily suspend payments to Customer (or direct Payment Processor to temporarily suspend payments to Customer), during an investigation of the issue and/or designate an amount of funds that Payment Vendor must maintain in order to protect Payment Vendor against the risk of existing or anticipated Chargebacks or ECP Returns and to satisfy Customer's other obligations under this Agreement (the "**Reserve Account**"), which may be funded in the same manner as provided for negative balances in Section 1.9. The Reserve Account will contain sufficient funds to cover any unbilled processing costs plus Payment Vendor's estimated exposure based on reasonable criteria for Chargebacks/ECP Returns, returns and unshipped merchandise and/or unfulfilled services. Payment Vendor may apply funds in the Reserve Account toward, and may set off any funds that would otherwise be payable to the

Customer's Accounts against, the satisfaction of any amounts which are or become due from Customer pursuant to this Agreement. The Reserve Account will not bear interest, and Customer will have no right or interest in the funds in the Reserve Account; provided that upon satisfaction of all of Customer's obligations under this Agreement, Payment Vendor will pay (or direct Payment Processor to pay) to Customer any funds then remaining in the Reserve Account. Any funds in the Reserve Account may be commingled with other funds, and need not be maintained in a separate account. Effective upon the establishment of a Reserve Account, Customer irrevocably grants to Payment Vendor a security interest in any and all funds, together with the proceeds thereof, that may at any time be in Payment Vendor or Payment Processor's possession and would otherwise be payable to Customer pursuant to the terms of this Agreement. Customer agrees to execute and deliver to Payment Vendor such instruments and documents that Payment Vendor may reasonably request to perfect and confirm the security interest and right of setoff set forth in this Agreement. Customer's obligations and Payment Vendor's rights under this Section survive termination of this Agreement.

1.11 **Response to Retrieval Requests**. Payment Vendor will send Customer any request for information by a Taxpayer, Card issuer or financial institution relating to a claim or complaint concerning a sale Customer has made ("**Retrieval Request**"), that Payment Vendor cannot satisfy with the information Payment Vendor has on file concerning such sale. In response, Customer must provide Payment Vendor in writing by certified or overnight mail or by confirmed fax (or by other means as agreed by Payment Vendor) the resolution of Customer's investigation of such Retrieval Request and include legible copies of any documentation required by the Retrieval Request within seven business days after Payment Vendor sends it to Customer (or such shorter time as the NACHA or Association Rules may require and of which Payment Vendor notifies Customer). Once Payment Vendor receives Customer's response, Payment Vendor will take the appropriate steps in a timely manner to reduce the probability of the Taxpayer's bank sending an unjustified Chargeback or ECP Return. Customer acknowledges that Customer's failure to fulfill a Retrieval Request in accordance with NACHA or Association Rules may result in an irreversible ECP Return or Chargeback.

1.12 **Chargebacks and ECP Returns**. If Payment Vendor determines that the Customer is receiving an excessive amount of Chargebacks or ECP Returns, in addition to Payment Vendor's other remedies under this Agreement, Payment Vendor may take the following actions: (1) review Customer's internal procedures relating to acceptance of Cards or ECP Transactions, as applicable, and notify Customer of new procedures Customer should adopt in order to avoid future Chargebacks or ECP Returns, as applicable; (2) notify Customer of a new rate Payment Vendor will charge Customer to process Customer's Chargebacks or ECP Returns; or (3) collect from Customer (pursuant to Section 1.10) an

amount reasonably determined by Payment Vendor to be sufficient to cover anticipated Chargebacks or ECP Returns and related fees and fines; or (4) terminate all payment processing services under this Agreement. For purposes of this Agreement, an excessive number of Chargebacks means one Chargeback per 100 Transaction records or the total dollar amount of Chargebacks is greater than or equal to three (3%) percent of the total dollar amount of Transactions for any 30-day period. The foregoing percentages are subject to change in accordance with the Association Rules. Customer also agrees to pay any and all Association or NACHA fees and fines assessed against Customer, Payment Vendor or Payment Processor relating to Customer's violation of this Agreement, the Association Rules or NACHA rules with respect to Customer's Transactions or with respect to excessive Chargebacks or ECP Returns under this Section.

1.13 **Claims of Taxpayers**. Customer has full liability if any Transactions for which Payment Vendor has given (or directed Payment Processor to give) the Customer Accounts provisional credit is the subject of a Chargeback or ECP Return. Subsequently, Customer is allowed to resubmit applicable Transactions for a second presentation, but only in accordance with Association or NACHA Rules, as applicable. To the extent that Payment Vendor or Payment Processor has paid or may be called upon to pay a Chargeback, ECP Return or refund/adjustment for or on the account of a Taxpayer and Customer does not reimburse Payment Vendor as provided in this Agreement, then for the purpose of Payment Vendor obtaining reimbursement of such sums paid or anticipated to be paid, Payment Vendor has all of the rights and remedies of such Taxpayer under applicable federal, state or local law and Customer authorizes Payment Vendor to assert any and all such claims in Payment Vendor's own name for and on behalf of any such Taxpayer individually or all such Taxpayers as a class.

1.14 **Card Advertising.** Wherever Customer accepts Cards, Customer will inform the public of the Cards that it honours. However, Customer may not indicate that any of the Associations endorses its goods or services.

1.15 **Price Changes.** To the extent Customer's actual volume of Transactions, method of processing, type of business and interchange qualification criteria differ from the information provided to Payment Vendor and/or Payment Processor, Payment Vendor may modify the pricing for the payment processing Services with 25 days' prior written notice. In addition, by giving written notice to Customer, Payment Vendor may change Customer's fees, charges and discounts resulting from (i) changes in Association fees (such as interchange, assessments and other charges) or (ii) changes in pricing by any third party Payment Vendor of a product or service used by Customer. Such new prices will be applicable to Customer as of the effective date established by the Association or third

party Payment Vendor, or as of any later date specified in Payment Vendor's notice to Customer.

1.16 **Termination.** Payment Vendor may terminate this Agreement if an Association or NACHA notifies Payment Vendor that it is unwilling to continue accepting Customer's Transactions. Payment Vendor may also terminate this Agreement at any time upon written notice to Customer as a result of any of the following events: (i) any non-compliance with this Agreement, the Association Rules, NACHA Rules or the Operating Procedures, which is not cured within thirty (30) days of Payment Vendor's notice to Customer; except that no cure period is allowed for termination based on Customer's fraud or failure to fund a Reserve Account; (ii) Payment Vendor reasonably deems Customer to be financially insecure, (iii) Customer or any person owning or controlling Customer's business is or becomes listed in the MATCH file (Member Alert to Control High-Risk Merchants) maintained by Visa and MasterCard or any Association or NACHA notifies Payment Vendor or Payment Processor that it is no longer willing to accept Customer's Transactions, or (iv) for a period of more than 60 consecutive days, Customer does not transmit Transactions to Payment Vendor. Upon notice of any termination of this Agreement, Payment Vendor may notify Customer of the estimated aggregate dollar amount of Chargebacks, ECP Returns and other obligations and liabilities that Payment Vendor reasonably anticipates subsequent to termination, and Customer agrees to immediately deposit such amount, or Payment Vendor (or Payment Processor) may withhold such amounts from Customer's credits, in order to establish a Reserve Account pursuant to and governed by the terms and conditions of Section 1.10.

1.17 **Indemnification.** The indemnity provided under this Section 1.17 shall survive the termination of this Agreement. Customer agrees to indemnify Payment Vendor and its affiliates, officers, directors, employees, agents, the Associations and NACHA, from any losses, liabilities, and damages of any and every kind (including, without limitation, any costs, expenses and reasonable attorneys' fees) arising out of any claim, complaint, Chargeback or ECP Return: (i) made or claimed by a Taxpayer with respect to any Transactions submitted by Customer, or (ii) caused by Customer's non-compliance with this Agreement, the Association Rules or NACHA Rules, including any breach of a representation or warranty made by Customer, or (iii) any voluntary or involuntary bankruptcy or insolvency proceeding by or against Customer. The indemnification provided for in this Section does not apply to any claim or complaint to the extent it is caused by Payment Vendor's own breach, negligence, or wilful misconduct.

1.18 **Disclosure of Taxpayer Information**. Customer shall exercise reasonable care to prevent disclosure of Card information or Taxpayer account information, other than to Customer's employees, agents and contractors for the purpose of assisting Customer in completing a

Transaction, or to the applicable Association or NACHA, or as specifically required by law. If at any time Customer determines that Card account or bank account number information has been compromised, Customer will notify Payment Vendor immediately and assist in providing notification to the proper parties.

1.19 **Additional Financial Information**. To the extent not available from public sources, Customer agrees to furnish Payment Vendor within three days of Payment Vendor's request (i) Customer's most recently prepared financial statements and credit information or (ii) if applicable, Customer's three most recent filings with the SEC or any other securities commission in respect of which Customer must file financial disclosure documents.

1.20 **Other Information**. With prior notice and during Customer's normal business hours, a Payment Vendor or Payment Processor duly authorized representative may visit Customer's business premises and may examine only that part of Customer's books and records that pertain to Transactions. Customer agrees to provide Payment Vendor at least twenty (20) days' prior written notice of Customer's intent to change its product line or services, or Customer's trade name, or the manner in which Customer accepts Cards or ECP Transactions. If Payment Vendor determines such a change is material to the relationship between Payment Vendor and Customer, Payment Vendor may refuse to process Transactions made pursuant to the change. Customer agrees to provide Payment Vendor with prompt written notice if Customer is the subject of any voluntary or involuntary bankruptcy or insolvency petition or proceeding.

1.21 **Application and Credit Check.** All statements made on Customer's application for payment processing Services, Schedule I of the Master Account Agreement, are true as of the date of Customer's execution of this Agreement. Customer's signature on this Agreement authorizes Payment Vendor and/or Payment Processor to perform any credit check deemed necessary.

1.22 **Payment Processing Guidelines.** Customer agrees to execute the Agreement attached hereto.

Schedule E

Submitter Merchant Payment Processing Instructions and Guidelines*

***(Definitions in this Schedule E are only applicable to Schedule E)**

Paymentech, LLC ("*Paymentech*" or "we", "us" or "our" and the like), for itself and on behalf of JPMorgan Chase Bank, N.A. ("Member"), is very excited about the opportunity to join Kubra Data Transfer Ltd ("Kubra") in providing you with state-of-the-art payment processing services. When your Customers pay you through Kubra, you may be the recipient of a Card funded payment. The organizations that operate these Card systems (such as Visa U.S.A., Inc. and MasterCard International Incorporated; collectively, the "Payment Brands") require that you (i) enter into a direct contractual relationship with an entity that is a member of the Payment Brand and (ii) agree to comply with Payment Brand Rules as they pertain to applicable Card Transaction you submit through Kubra. You are also required to fill out an Application with Paymentech. The Application provides Paymentech with information relative to your processing practices and expectations.

By executing this document, you are fulfilling the Payment Brand Rule of entering into a direct contractual relationship with a member, and you are agreeing to comply with Payment Brand Rules as they pertain to Transactions you submit for processing through the Kubra service. We understand and acknowledge that you have contracted with Kubra to obtain Card processing services on your behalf and that Kubra may have agreed to be responsible for your obligations to us for such Transactions and as set forth in these guidelines.

The following information is designed to inform and assist you as we begin our relationship.

1. Your Acceptance of Cards

- You agree to comply with all Payment Brand Rules, as may be applicable to you and in effect from time. You understand that we may be required to modify these instructions and guidelines in order to comply with requirements imposed by the Payment Brands.
- In offering payment options to your customers, you may elect any one of the following options. These acceptance options above apply only to domestic transactions:

    1) Accept *all* types of Visa and MasterCard cards, including consumer credit and debit/check cards, and commercial credit and debit/check cards;

    2) Accept *only* Visa and MasterCard credit cards and commercial cards (If you select this option, you must accept all consumer credit cards (but not consumer debit/check cards) and all commercial card products, including business debit/check cards); or

3) Accept *only* Visa and MasterCard consumer debit/check cards (If you select this option, you must accept all consumer debit/check card products (but not business debit/check cards) and refuse to accept any kind of credit cards).

- If you choose to limit the types of Visa and MasterCard cards you accept, you must display appropriate signage to indicate acceptance of the limited acceptance category you have selected (that is, accept only debit/check card products or only credit and commercial products).

- For recurring transactions, you must obtain a written request or similar authentication from your Customer for the goods and/or services to be charged to the Customer's Card, specifying the frequency of the recurring charge and the duration of time during which such charges may be made.

2. Settlement

- Upon our receipt of your Transactions, we will process your Transactions to facilitate the funds transfer between the various Payment Brands, you and Kubra. Unless otherwise agreed to by the parties, after we receive credit for such Transactions, we will provide provisional credit to one or more of the Bank Account(s) you designate herein under the "Funding Schedule" section.

- You must not submit Transactions for payment until the goods are delivered, shipped, or the services are performed. If a Customer disputes being charged for merchandise or services before receiving them, the result may be a Chargeback to you.

3. Chargebacks

- You may receive a Chargeback for a number of reasons. The following are some of the most common reasons for Chargebacks, but in no way is this meant to be an exhaustive list of all Chargeback reasons:

1) You do not issue a refund to a Customer upon the return or non-delivery of goods or services;

2) An authorization/approval code was required and not obtained;

3) The Transaction was fraudulent;

4) The Customer disputes the Card sale or the signature on the sale documentation, or claims that the sale is subject to a set-off, defense or counterclaim; or

5) The Customer refuses to make payment for a Card sale because in the Customer's good faith opinion, a claim or complaint has not been resolved, or has been resolved by you but in an unsatisfactory manner.

4. Data Security and Privacy

- By signing below, you represent to us that you do not have access to any Card Information (such as the Customer's primary account number, expiration date, security code or personal identification number) and you will not request access to such Card Information from Kubra. In the event that you do happen to receive Card Information in connection with the processing services provided by Kubra or Paymentech under these guidelines, you agree that you will not use it for any fraudulent purpose or in violation of any Payment Brands or applicable law and you will comply with all applicable Payment Brand Rules and Security Standards. If at any time you believe that Card Information has been compromised, you must notify us promptly and assist in providing notification to the proper parties. You must ensure your compliance with all Security Standards that are applicable to you and which may be published from time to time by the Payment Brands. If any Payment Brand requires an audit of you due to a data security compromise event or suspected event, you agree to cooperate with such audit. You may not use any Card Information other than for the sole purpose of completing the Transaction authorized by the Customer for which the information was provided to you, or as specifically allowed by Payment Brand Rules, or required by law. In the event of your failure, including bankruptcy, insolvency or other suspension of business operations, you shall not sell, transfer or disclose any materials that contain Transaction information or Card Information to third parties.

5. Funding Schedule

- In order to receive funds from Paymentech, you must maintain one or more bank account(s) at a bank that is a member of the Automated Clearing House ("ACH") system and the Federal Reserve wire system (the "Bank Account"). You must designate at least one Bank Account for the deposit and settlement of funds and the debit of any fees and costs associated with Paymentech's processing of the Transactions (all such designated Bank Accounts shall be collectively referred to herein as the "Settlement Account"). You authorize Paymentech to initiate electronic credit and debit entries and adjustments to your Settlement Account in accordance with this Section 5. We will not be liable for any

delays in receipt of funds or errors in Settlement Account entries caused by third parties, including but not limited to delays or errors by the Payment Brands or your bank.

- Unless otherwise agreed to by the parties, the proceeds payable to the Settlement Account shall be equal to the amounts received by us in respect of your Card transactions less all Chargebacks, Customer refunds and other applicable charges. Such amounts will be paid into the Settlement Account promptly following our receipt of the funds. If the proceeds payable to the Settlement Account do not represent sufficient credits, or the Settlement Account does not have a sufficient balance to pay amounts due from you under these guidelines, we may pursue one or more of the following options: (i) demand and receive immediate payment for such amounts; (ii) debit a Bank Account for the amount of the negative balance; (iii) withhold settlement payments to the Settlement Account until all amounts are paid, (iv) delay presentation of refunds until a payment is made to us of a sufficient amount to cover the negative balance; and (v) pursue any remedies we may have at law or in equity.
- Unless and until we receive written instructions from you to the contrary, all amounts payable by Paymentech to you will be deposited in the Settlement Account designated and authorized by you as set forth below:

Name of Bank: _____

ABA No.: _____

Account No.: _____

Account Name: _____

Reference: _____

6. Convenience Fee Transactions.

- You and Kubra hereby agree that:
  1) All Convenience Fee Transactions will be submitted by Kubra to Paymentech under that certain Submitter Agreement entered into by and between Kubra and Paymentech; and
  2) All Card transactions will be submitted by Kubra on your behalf to Paymentech under the terms of these Payment Processing Instructions and Guidelines.

7. Definitions

"Application" is a statement of your financial condition, a description of the characteristics of your business or organization, and related information you have previously or concurrently submitted to us, including credit and financial information.

"Card" is an account, or evidence of an account, authorized and established between a Customer and a Payment Brand, or representatives or members of a Payment Brand that you accept from Customers as payment for a good or service. Payment Instruments include, but are not limited to, credit and debit cards, stored value cards, loyalty cards, electronic gift cards, authorized account or access numbers, paper certificates and credit accounts.

"Chargeback" is a reversal of a Transaction you previously presented to Paymentech pursuant to Payment Brand Rules.

"*Convenience Fee Transaction*" is a Transaction representing a charge to a customer's Card for the convenience of using the payment channel offered by you and Kubra.

"*Customer*" is the person or entity to whom a Card is issued or who is otherwise authorized to use a Payment Instrument.

"*Member*" is JPMorgan Chase Bank, N.A. or other entity providing sponsorship to Paymentech as required by all applicable Payment Brand. Your acceptance of Payment Brand products is extended by the Member.

"*Payment Brand*" is any payment method Payment Vendor whose payment method is accepted by Paymentech for processing, including, but not limited to, Visa, U.S.A., Inc., MasterCard International, Inc., Discover Financial Services, LLC and other credit and debit card Payment Vendors, debit network Payment Vendors, gift card and other stored value and loyalty program Payment Vendors. Payment Brand also includes the Payment Card Industry Security Standards Council.

"*Payment Brand Rules*" are the bylaws, rules, and regulations, as they exist from time to time, of the Payment Brands.

"Card Information" is information related to a Customer or the Customer's Card, that is obtained by you or Kubra from the Customer's Card, or from the Customer in connection with his or her use of a Card (for example a security code, a PIN number, or the customer's zip code when provided as part of an address verification system). Without limiting the foregoing, such information may include a the Card account number and expiration date, the Customer's name or date of birth, PIN data, security code data (such as CVV2 and CVC2) and any data read, scanned,

imprinted, or otherwise obtained from the Payment Instrument, whether printed thereon, or magnetically, electronically or otherwise stored thereon.

"*Paymentech*", "*we*", "*our*", and "*us*" is Paymentech, LLC, a Delaware limited liability company, having its principal office at 14221 Dallas Parkway, Dallas, Texas 75254.

"*Security Standards*" are all rules, regulations, standards or guidelines adopted or required by the Payment Brands or the Payment Card Industry Security Standards Council relating to privacy, data security and the safeguarding, disclosure and handling of Payment Instrument Information, including but not limited to the Payment Card Industry Data Security Standards ("PCI DSS"), Visa's Cardholder Information Security Program ("CISP"), Discover's Information Security & Compliance Program, American Express's Data Security Operating Policy, MasterCard's Site Data Protection Program ("SDP"), Visa's Payment Application Best Practices ("PABP"), the Payment Card Industry's Payment Application Data Security Standard ("PA DSS"), MasterCard's POS Terminal Security program and the Payment Card Industry PIN Entry Device Standard, in each case as they may be amended from time to time.

"*Transaction*" is a transaction conducted between a Customer and you utilizing a Card in which consideration is exchanged between the Customer and you.

Please acknowledge your receipt of these instructions and guidelines and your agreement to comply therewith.

Agreed and Accepted by:

_____

MERCHANT LEGAL NAME (Print or Type)

_____

Address (Print or Type)

_____

By (authorized signature)

_____

By, Name, Title (Print or Type)

_____

Date

Agreed and Accepted by:

KUBRA Data Transfer Ltd

MERCHANT LEGAL NAME (Print or Type)

Address (Print or Type)

By (authorized signature)

By, Name, Title (Print or Type)

Date

Agreed and Accepted by:

PAYMENTECH, LLC for itself and on behalf of

JPMORGAN CHASE BANK, N.A.

By:

Print Name:

Title:

Date:

Address:

SCHEDULE F

SCOPE OF WORK

[SOW TO BE INSERTED ONCE THAT DOCUMENT IS FINALIZED.]

FILE LOCAL AGENCY
ELECTRONIC PAYMENT PROCESSING SERVICES AGREEMENT
Contract Title: KUBRA Contract
Contract No. FL2016-09

SCOPE OF WORK for FileLocal Services

1. Service Scope

The Agency requires a payment processing solution that can be integrated into the FileLocal Tax Portal ("Tax Portal) application hosted by e-Gov Systems and integrate with any city participating in the Washington Cities Business License and Tax Portal Agency ("FileLocal"). The solution must allow FileLocal and FileLocal participating cities to receive credit card, debit card and ACH payments without storing customer account information on FileLocal, or other FileLocal participating cities servers.

The Vendor must obtain any agreement, approval, and any permits necessary for all major credit card institutions (such as Visa, MasterCard, Discover and etc.) The vendor must also be certified with Chase Paymentech as the merchant processor. Additionally, the Contractor shall must maintain PCI compliance and make the ROC available to the City on an annual basis address PCI compliance requirements in a manner that minimizes risk to the City while also minimizing the City's participation in PCI related activities.

The Agency requires payment processing solutions that can integrate into the Tax Portal application hosted by e-Gov Systems and integrate with any Agency Client participating in FileLocal. The solution must allow the Agency and Agency Clients to receive credit card, debit card and ACH payments without storing customer account information on FileLocal or Agency Client's servers.

The Agency and Agency Clients payment applications by channels through FileLocal listed below will migrated and supported by the Payment Vendor's platform:

Web Payments:

1. City of Seattle Business license applications
2. City of Seattle Business license renewals
3. City of Seattle Business taxes
4. City of Bellevue Business license applications
5. City of Bellevue Business taxes
6. City of Everett Business license applications
7. City of Everett Business taxes
8. City of Tacoma Business license applications
9. City of Tacoma Business license renewals

10. City of Tacoma Business taxes
11. Washington Cities Business License and Tax Portal Agency ("FileLocal") User Fees

1.1 Functional and Technical Requirements

1.1.1 Payment Processing Platform

There will be a central platform that allows payments to be made via the web through a direct link from FileLocal. Payment Vendor will create and maintain a functional specification document for the tax portal payments handled through Kubra agreed to by the Agency, Agency Clients, Payment vendor and e-Gov Systems.

1.1.3 Web Service / API Payments

The solution will provide a web service/API for processing customer payments from FileLocal. The web service/API will support several methods to give FileLocal flexibility in developing payment applications. Payment Vendor will create and maintain a BRD which will outline the technical requirements for the web services and form fills agreed to between the Agency, Payment Vendor and e-Gov Systems.

1.1.6 Financial Processing and Funds Settlement

Transactions and settlement files will be processed as required through the appropriate authorization and settlement networks. FileLocal cut off times will be 5 p.m. Pacific time and deposited to the FileLocal Agency Clients on the next business day, wire fees will apply. Remittance files for each Agency Client shall be available same day, post cut off time.

All funds must be settled in the Agency and Agency Client's bank accounts and use each Agency and Agency Client's merchant services provider, Chase Paymentech.

1.1.7 Administrative Tools and Reporting

The solution will provide a web-based administrative tool that will allow inquiry capabilities, reporting, and allow for all transactions to be journalized for auditing purpose. This functionality must be available to all participating cities and FileLocal.

1.1.9 ADA Requirements and Infrastructure

The software solution must adhere to ADA websites compliance with WCAG 2.0 Level A and be tested with screen reader such as JAWS during development. If Kubra does not fully comply, Kubra will provide the City of Seattle with a list of how the site complies currently and demonstrate when Kubra will be fully compliant.

The software solution system processes, and partners must adhere to the requirements of the full Payment Card Industry Data Security Standard (PCI DSS) per the contract.

1.1.10 Quality Management and Change Control

The proposed solution must include quality management and change control procedures.

1.1.11 Customer and Technical Support

The Payment vendor will provide customer service with the ability to answer questions from both FileLocal participating cities and the participating cities employees. Based on the Service Level Agreement (SLA), Schedule C, the Payment Vendor will provide technical support that includes guaranteed response times and a documented escalation process and will describe the agreed upon escalation process for notifying the Agency, Agency Clients and e-Gov Systems.

1.2 Security Requirements

1.2.1 Industry and Regulatory Compliance

Payment Vendor must demonstrate compliance with:

- Payment Card Industry (PCI) standards
- Payment Application Best Practices (PABP)
- The Fair Credit Billing Act (FCBA)
- Electronic Fund Transfer Act (EFTA)
- The Gramm-Leach-Bliley Act (GLBA)
- The Sarbanes-Oxley Act (SOA)
- Health Insurance Portability and Accountability Act (HIPPA)
- Fair and Accurate Credit Transactions Act (FACT ACT)
- Regulation CC
- Regulation A

1.2.2 Security Controls

Payment Vendor is responsible for ensuring that appropriate organizational, procedural, and technical controls are in place to safeguard the City's and its customer's information.

1.3 Management Requirements

1.3.1 Personnel Resources

Payment Vendor will not reassign or replace any of the key team members during the execution of the implementation and/or Work Orders under this contract except for extenuating circumstances, for example: death, termination of employment, personnel issues, or illness etc. Should extenuating circumstances arise, Payment Vendor will notify

the Agency Project Manager of such events and a replacement team member will be named. The Payment Vendor shall present to the Agency one or more individual(s) with similar qualifications as a replacement, subject to Agency approval which shall not be unreasonably withheld. The Agency's approval or disapproval shall not be construed to release the vendor from its obligations under this contract.

1.3.2 Project Management

Payment Vendor must provide expertise and experience in the end-to-end installation of the platform. This will include Project Management, Functional and Technical resources.

Payment Vendor must designate the Project Manager who will have overall, daily responsibility for the project. This person will be responsible for the Payment Vendor's project management and coordination with the Agency and e-Gov Systems. The Payment Vendor must work in good faith effort with the FileLocal product and e-Gov Systems, to ensure timely implementation of new Agency Clients or product expansion.

Payment Vendor must provide an estimate of the timeline to complete adding new Agency Clients or any new development of the payment functionality in FileLocal within the agreed to project timeline provided by the Agency and e-Gov Systems.

1.3.3 Training

The Payment Vendor is responsible for providing documentation to Agency and e-Gov Systems to include in the training to FileLocal Agency Clients utilizing the E-Payments Platform. This may include training for different Clients customer service staff (CS), back-office, technical and functional staff, and treasury and business technology staff.

2. Key Objectives

The objective is to provide the City of Seattle acting on behalf of the Washington Cities Business License and Tax Portal Agency ("FileLocal") and participating FileLocal cities with a robust state-of-the-art solution, one that will provide citywide E-Payment solution that will accept payments via the internet via the FileLocal Tax Portal ("Tax Portal") which is developed, supported and maintained by e-Gov Systems (RamWare LLC).

The City expects to achieve the following:

- Allow all FileLocal participating cities and the FileLocal agency to implement different payment processing options for, payment methods, channels, convenience fees, recurring and one time payments, etc.,
- Provide a reliable, cost effective payment solution for the FileLocal and FileLocal participating cities and the customers.
- Provide significant experience implementing and supporting electronic payment applications for a variety of governmental and non-governmental organizations.

- Provide the experience and ability to provide the City with direction, advice, analysis, workflow/business process recommendations, and technical implementation support.
- Meets all PCI compliance standards,
- Provide the ability and resources to provide electronic payment (credit/debit card and one time ACH) processing technology and services. This technology and services will be interfaced to the tax portal that provides customers with the ability to pay for services. The technology should also provide settlement processing with the FileLocal and all FileLocal participating cities.
- Provide the ability for a seamless transaction between the Tax Portal and the Kubra payment solution including all FileLocal branding and design.

3. Work Order

Each work order shall be subject to all of the terms and conditions of Contract FileLocal 2016_XX, and incorporated into this Contract by this reference. The Payment Vendor shall furnish the services ("deliverables") specified in the Work Order in an aggregate, single, complete transaction. For each work order under this Contract, Payment Vendor shall commence work upon issuance of a notice to proceed by the Agency. All work orders shall include the following:

1. Project Deliverables
    a. Project Schedule
    b. Project Status Reports – Periodic reporting on project issues, budget, and schedule.
    c. Design Specifications – Provide functional specifications showing the functionality of the payment and reconciliation process
    d. Development – Provide a technical specification and BRD showing the complete technical solution and the interactions between e-Gov Systems and Kubra. Includes branding of any Kubra owned pages to the FileLocal design and brand.
    e. Training Materials – Payment Vendor will provide final training documentation to be included in the FileLocal training guides.
    f. Support and Maintenance Plan – Update if required with specific work order.

SERVICE LEVEL AGREEMENT (SLA) FOR FL2016-09 WITH KUBRA DATA TRANSFER, LTD

Overview

This Service Level Agreement is Schedule C to FileLocal contract FL2016_09 for payment transaction processing between the Washington Multi-City Business License and Tax Portal Agency (dba FileLocal) and Kubra Data Transfer, LTD in agreement by Ramware LLC (dba e-Gov Systems) for the FileLocal Tax Portal.

The objective of this document is to define the services provided by the FileLocal Agency to each participating technology vendor and to define the services provided between the technology vendors to ensure a single system for the FileLocal business license and tax payer community.

The Service Level Objectives outlined in this document support the Agency in meeting its overall Strategic Objectives of providing a reliable, usable and secure website to apply for and receive local business licenses and file local B&O taxes.

This SLA provides a framework to describe the services and the measures by which they are evaluated. The framework is outlined in the Service Level Standards section of this document, and includes a hierarchy of Critical Success Factors (CSF), Services, Service Level Objectives (SLO), and Measures.

Contents

1. Period and Scope of the Agreement 2
2. Outline of FileLocal Agency Relationships with Parties 2
3. Definition of terms 3
4. Kubra Responsibilities 4
5. Service Level Objectives 9
6. Services Level Failures: 10
7. Incident Management 10
8. SLA Performance Levels (Table 1) 11
9. Agency Responsibilities 12
10. Joint Responsibilities 13
11. Change Order Process for Service Levels 15
12. Supporting Documentation 15

Agreements

1. Period and Scope of the Agreement

The Multi-City Business License and Tax Portal Agency (Agency) has agreements with Kubra Data Transfer, LTD (Payment Vendor) to provide the application, infrastructure, and operational support for the software application and functionalities as described in this document.

Unless otherwise stated, this Agreement will become effective when the contract is signed by Payment Vendor and the Agency, and will continue until the termination date specified in this Agreement.

Applications/Functionality supported by the Provider under this Agreement

Application / Functionality	Number of Licenses
Provide pass-through payment processing with ACH debit and Credit Card Processing (MC and Visa)	Unlimited license for pass-through payment processing

2. Outline of FileLocal Agency Relationships with Parties

The Agency serves as the Product Manager of the FileLocal system.

In December of 2013, each participating city in the Agency signed an Interlocal Agreement which created the Agency. The Agency's purpose is to manage the implementation and maintenance of the FileLocal tax portal which includes managing the use of the system for business and city customers as well as the connections between FileLocal and the participating cities' systems of record.

The Agency contracted with e-Gov Systems to provide the FileLocal tax portal as a SaaS solution. As part of Contract FileLocal 2016_10, e-Gov Systems has agreed to a service level agreement which outlines the service provided to the Agency and the cities. The Agency manages that service on behalf of the cities. No participating city shall manage the vendor service.

In addition, the Agency also contracted with Payment Vendor for the FileLocal payment processing functionality. A SLA is provided for the Payment Vendor through FileLocal 2016_09. There is a direct line of communication between KUBRA's payment processor, Chase Paymentech, and the cities for any communication on specific payments made by tax payers. General communications about the payment process itself is managed by the Agency.

Currently there is a resolution (FL2014-06) in place allowing the City of Seattle to maintain the vendor contracts until implementation is complete. Upon completion of the base implementation, the contracts will transfer via Resolution from the City of Seattle to the Agency. The implementation was completed in April 2016 and resolution FL2016_10 created a new contract with the Payment Vendor to provide services to the Agency to replace the work order under the City of Seattle's contract 2995 Amendment #1.

This SLA is designed to be implemented with the new FileLocal Payment Vendor contract replacing contract 2995 amendment #1 from the City of Seattle to the Agency as the services described here, and the responsibility for those services, does not change during this time.

3. DEFINITION OF TERMS

Downtime means that the Application Services and/or the application data are unavailable to taxpayers or city internet users.

Application Availability is measured as follows: (Total minutes of the month - minutes of scheduled service - minutes of downtime) / (total minutes of the month - minutes of schedule service)

Software as a Service (SaaS) is a software distribution model in which applications are hosted by a vendor or service provider and made available to customers over a network, typically the Internet.

Payment Card Industry Compliance (PCI) represents standards and supporting materials to enhance payment card data security and refers to PCI Standards Council's PCI Data Security Standard (PCI DSS) Version 3.0 and subsequently adopted versions.

Data Retention also called records retention, is the continued storage of an organization's data for compliance or business reasons.

Data Governance is a set of processes that ensures that important data assets are formally managed throughout the enterprise. Data governance ensures that data can be trusted and that people can be made accountable for any adverse event that happens because of low data quality.

Business Continuity (BC) encompasses a loosely defined set of planning, preparatory and related activities which are intended to ensure that an organization's critical business functions will either continue to operate despite serious incidents or disasters that might otherwise have interrupted them, or will be recovered to an operational state within a reasonably short period

Business Requirements Document (BRD)

Disaster Recovery (DR) involves a set of policies and procedures to enable the recovery or continuation of vital technology infrastructure and systems following a natural or human-induced disaster.

Critical Success Factor (CSF) is the term for an element that is necessary for an organization or project to achieve its mission and its Strategic Objectives.

Defect is an issue discovered with functionality post-vendor QA.

Downtime means that the Application Services and/or the application data are unavailable to taxpayers or city internet users. Combination of planned and un-planned outages. Metric - a quantitative measure of a degree to which a system or process possesses some property.

Service Level Objective (SLO) The service levels that will be included in the Service Level Agreements (SLAs) with vendors and member cities. These represent the goals of the services.

Uptime The number of minutes during a calendar month that a system is available and ready for use.

4. KUBRA RESPONSIBILITIES

Payment Processor shall provide robust payment process which is in compliance with PCI standards Version 3.1 and subsequent versions and includes: protection against data loss, security attack protection and detection, and appropriate reaction to security incidents including development of an incident management plan to ensure, in the event of a security breach event, that incidents are documented and security incident reports are generated and other provisions provided in FileLocal FL2016_09 and Statement of Work (Schedule F).

Payment Vendor will provide a development, testing and production environment for both the Agency, participating cities and e-Gov Systems. In addition separate testing environment will be provided to e-Gov systems to connect to e-Gov's QA environment for sole purpose of testing between the FileLocal technology vendors while not interrupting testing for the Client in the UAT environment.

Payment Vendor will provide Functional (business process) and Technical (data interchange) specifications.

Payment Vendor will use commercially reasonable efforts to provide the Services in accordance with the performance standards ("Service Levels") set forth in the Service Level Schedule, Table 1. Performance at or above a Service level shall constitute satisfactory performance by Provider. In the event that, at any time, a monthly Service Level report shows any material failure by Payment Vendor to meet any of the Service Levels, Payment Vendor shall: (i) within thirty (30) days after the date of delivery of such report, deliver to the Agency a remedial plan showing in reasonable specificity and detail (A) Payment Vendor's findings regarding the causes for such failure to meet Service Levels and (B) a remedial plan of actions reasonably designed to eliminate, prevent or reduce the future likelihood of recurrence of such causes; and (ii) diligently proceed to carry out such plan. Except for Client's right to terminate for material breach in accordance with Section 4.2 hereof (in the event that repeated, frequent, or specific material failures by Payment Vendor to meet Service Levels constitute a material breach of this Agreement), the foregoing shall constitute the sole and complete remedy for Client with respect to the corresponding failures by Payment Provider to meet agreed to service levels for implementing any new cities through the FileLocal product roadmap adopted each year.

4.1. SERVICE LEVEL AGREEMENT PERFORMANCE REPORTING

Payment Vendor shall provide reports (the first week of every month) of its performance against the Service Levels on a monthly basis. For any new cities joining FileLocal, those will be added after the production ready date to the monthly Service Level report.

4.2. PAYMENT PROCESSING MANAGEMENT REPORTING FREQUENCY AND CONTENT

For all cities participating in FileLocal, and for the Agency, Payment Vendor will supply daily, weekly and monthly reporting as needed to the applicable parties accessible via the Admin Console. Additionally, Payment Vendor to continue providing daily remittance report by participating city and agency.

A complete list of all reports accessible via this application is available in the i-doxs product user guide. Note: Payment Vendor to continue providing daily remittance reports by participating city to e-Gov. This file will be the basis for the e-Gov to Kubra reconciliation.

4.3. REPLACEMENT SYSTEMS

In the event that any applicable system or function used by Payment Vendor to provide a Service is replaced during the Term by a comparable system or function, the Service Level shall, to the extent reasonably practicable, be defined during the first sixty (60) days of operation of such replacement system or function. Service Levels shall at all times be established at a level intended to achieve performance at least the same as or better than performance under the Service Level associated with the replaced system or function.

4.4. STORAGE

Payment Vendor will ensure Agency and Agency Client data is stored and retained in accordance with the Agency Record Retention policies. Historical bill images and payment history may be loaded into the Service at the election of any City requesting the data: such election will be noted in the Services Fee Schedule, if applicable. Purging of Agency or Agency Client records beyond the standard 36 month retention period will be at the election of the Payment Vendor. The Payment Provider is not the system of record and the cities and Agency have the obligation to retain customer data on a permanent basis, or for any other Client need, and agrees that the loss or destruction of any such data will not result in any liability to Payment Vendor.

4.5. ADDITIONAL STORAGE

Payment Vendor may provide storage services for Agency or Agency Client data beyond the standard period included in the Services, at the election of the Agency, which will be invoiced at the then-current Additional Storage Fee rate and described in the Services and Charges (Schedule A)

4.6. ACCOUNT VOLUME GROWTH

Batch windows and service levels are based on current account volumes as of the Commencement Date. Batch windows and service levels may be adjusted by Payment Vendor in consultation with Client should account volumes exceed 20% growth in a given month.

4.7. APPLICATION HOSTING

Payment Processor assumes responsibility for the computing environment and supporting the contracted applications. This includes provide commercially appropriate technology and procedures in information security and environmental control as outlined in the Operations Support Plan (for more information see Exhibit C).

Hosting is provided 24x7x365 in a secured data center environment and is certified TIER 4. Data center will provide full-time onsite security monitoring, video surveillance, biometric and access card, bullet-resistant walls and glass, and man-trap access only to data center floor. Environmental protection is provided with non-water based FM-200 fire suppression, truly redundant power and air handling systems, and fully redundant power with UPS circuits to each rack. Connectivity and network infrastructure is multi-homed across geographically-diverse Tier-1 internet providers, fully-redundant enterprise-class firewall and network infrastructure, and full-time staffed network operations centers. This includes the underlying hardware and software infrastructure, database and server licenses, maintenance, and database administration.

Payment Vendor may change hosts in the future but will continue to use a secured data environment equal to or greater than the above specifications.

4.8. BUSINESS CONTINUITY AND DISASTER RECOVERY

Provide robust business continuity (BC) and disaster recovery (DR) processes and services to support the application, and the Agency goals including annual review of the processes and review of BC/DR reports, as outlined in the Operations Support Plan (for more information see supporting documentation E).

Provide the following Application Recovery and Disaster Recovery Services:

- Production databases are backed up daily on a weekly retention schedule
- Production web server is backed up twice per month with a monthly retention schedule
- Backups and recovery are facilitated through services such as AmeriVault & RestartIT
- DR is provided in conjunction with services.

In the event the hosted system experiences problems, Payment Vendor shall use all commercially reasonable efforts to meet or exceed the service level targets outlined in the Service Level Standards.

BC and disaster recovery DR processes and services for the application and associated data should be at or above the same level of security as the FileLocal Policies adopted by the Executive Board via Resolution FL2016-04, and individual cities' adopted security policies.

4.9. INFORMATION SECURITY

Provide information security processes and services to support the application, and the Agency goals. The processes and supporting report are to be reviewed on a regular schedule for possible changes or considered for change at any time if requested.

Security processes for the application and associated data should be at or above the same level of security as the FileLocal Security Policies adopted by the Executive Board via Resolution FL2016-04, and individual cities adopted security policies guidelines on:

- Security Planning.
- Application and database security
- Security of data on the system and end-user authority
- Automated security monitoring
- Access Control Lists for all computing systems
- Security problem determination and resolution
- Security audits and review of audit logs
- Evaluation and review of new security software

4.10. SOFTWARE MAINTENANCE

Provide Software maintenance and upgrade services, including upgrades and associated documentation that are provided as supplemental and standard releases to the supported Software. Warranty that any changes will not corrupt existing Client data, nor impose new data defects.

Updates include:

- Standard Release – Release of the software that contains product enhancements and improvements, selected by Payment Vendor and released approximately every other month. Standard Releases will be in accordance with contractual obligations, the annual budget planning session and in alignment with the Agency Release Calendar. Payment Provider will provide Agency release information on a yearly basis beginning in March of the current year for the following year's releases.
- Supplemental Release – Minor release of the software that contains primarily error corrections to an existing Standard Release and may contain limited improvements that do not affect the overall structure of the software, selected by the Provider. Depending on the Agency or Agency Clients specific configuration, a Supplemental Release may not be applicable. Supplemental Releases will be in accordance with contractual obligations, the annual budget planning session and in alignment with the Release Calendar.

Payment Vendor warrants that each Supplemental and Standard Release will be tested and will perform according to Payment Vendor specifications, will not corrupt existing Client owned data nor introduce new data defects or security vulnerabilities, and is agreed upon by the Agency. Errors will be corrected as necessary so that the system will continue to meet the requirements of this SLA and the functional and technical requirements outlined in the Payment Process BRD.

4.11. CLIENT SUPPORT: POST PRODUCTION SUPPORT HOURS

Payment Vendor will provide client support weekdays 8:00 am PST to 5:00 pm PST, excluding holidays. Client support required at another time will be based upon the severity of the problem. Contact will be made in accordance with the support defined in Exhibit C. Telephone support services, available Monday to Friday 8:00 am PST to 5:00 pm PST excluding holidays, will include assistance related to routine questions regarding use of the i-doxs Suite system (i-doxs Suite), assistance in identifying and verifying the causes of suspected errors or malfunctions in the i-doxs Suite system, advice on detours for identified errors or malfunctions, where reasonably available and correction of reproducible errors of the i-doxs Suite system that cause the applicable i-doxs Suite system to deviate materially from the applicable documentation.

4.12. AFTER HOURS SUPPORT (TABLE I)

Payment Vendor will provide support outside of regular business hours as needed. Although the dedicated support team will be unavailable, general support will still be available for any Production related issue. With that in mind, the Client will attempt to make solution specific requests for changes during business hours and use after hours support for service interruptions and issues.

4.13. ON-SITE SUPPORT

On-site services will be provided at the Client's reasonable request. Payment Vendor shall charge Agency for such on-site services at Payment Provider's then-current rates, plus reasonable travel costs and other out-of-pocket expenses directly incurred in performing such services, provided Agency has agreed to pay for on-site services in advance. However, Agency shall have no obligation to pay for services rendered as a result of a failure of the Payment Vendor's solution to satisfy the Service Level Agreement set forth herein, where

Payment Vendor determines in its sole discretion, that such services must be performed on-site at Agency or Agency Client's premises.

4.14. ESCALATION PROCEDURES

In order to properly track and monitor, all issues must be reported to Payment Vendor Support via the dedicated 1-800 telephone number and/or to clientsupport@KUBRA.com. Agency may also elect to escalate an issue directly to the Agency's dedicated Client Relationship Manager

4.15. SERVICE LEVELS

4.15.1. System Availability

Payment Vendor shall make access available to the Services twenty-four hours per day, seven days per week, less (a) scheduled maintenance; and (b) excusable downtime resulting from events beyond Payment Vendor's reasonable control (the "Availability Period"). Payment will conduct proactive monitoring of all servers, including monitoring disk space, CPU utilization, memory utilization and critical error messages. Payment Provider will take commercially reasonable efforts to notify Client in advance of any potential server outages or equipment failures that would prevent Client from using the Services. Payment Vendor will provide support 24 hours per day, 7 days per week for all servers. Payment Vendor will maintain at least 99.9 percent (99.9%) server availability during the Availability Period, which availability shall be measured monthly and based on a system-wide average. Events that are beyond the control of Payment Vendor, such as web brownouts, consolidator/payment processor unscheduled downtime, e-Gov Systems outages, and scheduled maintenance are not included.

4.15.2. Scheduled Maintenance

Payment Vendor will schedule all routine system maintenance, hardware and software upgrades, and network changes from 2AM ET to 6AM ET each Sunday. The scheduled maintenance window will not apply towards the Availability Period.

4.15.3. Notice for Changes

Payment Vendor will take commercially reasonable efforts to provide 72 hours advance notice for any unscheduled system maintenance. This notice will go to both the Agency and e-Gov Systems.

4.15.4. Response Time

Payment Vendor will make commercially reasonable efforts to maintain an internal response time of five (5) seconds or less for all transact ions from the time they arrive at the Payment Vendor firewall until they are delivered back to the firewall.

4.15.5. Parsing and Presentment

Upon Payment Vendor's receipt of the document data from Agency or Agency Client, Payment Vendor will process and load the customer documents, no later than the time frame mutually agreed to after receipt. All regularly scheduled files received for parsing individual presentment will be processed

within twenty four (24) hours of receipt by Payment Vendor unless otherwise specified and agreed upon with Agency and Agency Clients. Receipt of the file is identified as the successful completion of the transmission of the file and the relevant return code confirming successful transmission. In the event of exceptionally large, additional, missed, or the reprocessing of files, special arrangements must be made with Payment Vendor client support to determine a mutually agreeable schedule for delivery.

4.15.6. E-MAIL DELIVERY

E-mail messages will be made available to applicable customers within eight hours of the event that triggers the message. Events that are beyond the control of Payment Vendor, such as web brownouts and scheduled maintenance are not included in this time commitment

4.15.7. PAYMENT PROCESSING AND POSTING

If the Client elects to accept ACH payments, Payment Vendor shall create (a) a daily ACH file to be electronically transmitted to the designated financial institution on each business day (Monday through Friday. excluding Bank holidays), for the total amount of the transactions processed, in accordance with me terms and conditions set forth herein; and (b) a separate Accounts Receivable file that is consistent with the ACH file and (c) that Payment Vendor will post the Accounts Receivable (AJR) file each day on a specified FTP server for Client at a mutually agreed-upon time.

If the Client elects to accept Credit or Debit cards, Payment Vendor shall authorize those transactions on a real time basis with the chosen credit card processor and provide a nightly settlement file to the credit card processor for verification. The Credit Card Processor will be responsible for depositing the funds to the designated bank accounts of the Clients.

5. SERVICE LEVEL OBJECTIVES

The Service Level Objectives are the levels at which services are expected to be performed. On a regular cadence the actual service levels will be compared to the objectives in order to determine if the parties are meeting the SLOs and ultimately the Strategic Objectives.

Payment Vendor is responsible for the following services as they relate the application, infrastructure, and operational support for the software application and functionalities as described in this document.

- Software as a Service (SaaS)
- Pass-through from Payment Provider to FileLocal product maintained by Portal Vendor
- Data Retention and Quality
- Application Hosting
- Business Continuity and Disaster Recovery
- Information Security
- Software Maintenance
- Help Desk Customer Service

The Agency is responsible for managing the implementation, maintenance, and use of the FileLocal tax portal for the participating cities, businesses and city customers. The Agency also manages the vendor services for the Agency Clients for both Payment Provider and Portal Vendor. The services the Agency are responsible for include:

- Agency Management
- Agency Customer Service Support
- Agency Problem Management
- Change Management
- City Onboarding

Several of the services require more than one of the parties of this agreement to share responsibility for providing the services. The City, the Agency, and the vendors share responsibilities for the following services:

- Incident Reporting
- Problem Analysis
- User Provisioning
- Network Services
- Relationship Management: Staffing

Agency Clients are responsible for providing business and technical support for city-specific functions covered in the Member City Service Level Agreement (SLA) for the Washington Multi-City Business License and Tax Portal Agency (dba FileLocal).

6. SERVICES LEVEL FAILURES:

6.1. EXCUSED PERFORMANCE PROBLEMS

Payment Vendor shall not be liable to Agency or Agency Client for any failure to meet a Service Level to the extent that such failure is attributable to a Force Majeure event. The foregoing is referred to herein collectively as an "Excused Performance Problem."

6.2. SINGLE POINT OF CONTACT

Regardless of whether any failure by Payment Vendor to meet a Service Level is attributable to Payment Vendor or an Excused Performance Problem, and without limitation on Payment Vendor obligations to address such failure as otherwise specified in this Agreement, Payment Vendor shall provide a single point of contact in the form of a toll-free number to address resolution of such failure and shall act promptly to address the problem causing the failure, as outlined in Exhibit D.

7. INCIDENT MANAGEMENT

All incidents that occur and affect the Client directly and/or indirectly will be managed to resolution by the Payment Vendor Support Team with ongoing communication to the Agency. Resolution of incidents at Payment Vendor is facilitated through:

- Payment Vendor incident management 7 X 24 based on the severity of the issue defined hereto.

- Payment Vendor analysts will track incidents to ensure that they are resolved in a timely manner. Resolution may be in the form of a transfer to the Client's own support service where appropriate.
- Escalation of any incident to Payment Vendor management at any time.
- Communication to all necessary parties as detailed in the contact lists agreed with the Agency Client, Portal Vendor and Agency.
- Classification of the severity level of each incident in accordance with Payment Vendor's Incident Classification Standard
- Integrity and completeness of Incident records

8. SLA Performance Levels (Table 1)

8.1. INCIDENT CLASSIFICATION STANDARD

Payment Vendor shall use all commercially reasonable efforts to respond to incident reports according to the following schedule:

Incident Classification	Action 1	Action 2	Action 3
Severity Level 1	1 hour	24 Hours	15 business days
Severity Level 2	1 hour	1 business day	30 business days
Severity Level 3	1 hour	15 business days	45 business days
Severity Level 4	1 hour	45 business days	as appropriate

8.2. INCIDENT CLASSIFICATION DEFINITION

Severity Level 1	Fatal	Errors preventing all useful work from being done as reasonably determined by the Agency or Agency Clients and Payment Vendor. Specific features include the ability to reasonably access the hosted portal, view an amount due and execute a payment transaction Unauthorized activity, defined as the application executing payment related functions without proper authorization; e.g. Duplicate ACH batch file submissions. Are classified as a Severity One issue. Correction of any duplicate or ACH file issues are dependent on regular Bank processing schedules as defined by the Federal Reserve.
Severity Level 2	Severe Impact	Errors which disable major functions from being performed as reasonably determined by the Agency Client, Agency, Ramware, and/or Payment Vendor
Severity Level 3	Degraded Operations	Errors disabling only certain nonessential functions as reasonably determined by the Agency Client, Agency, Ramware, and/or Payment Vendor
Severity Level 4	Minimal Impact	Minor and cosmetic issues as reasonably determined by the Agency Client, Agency, Ramware, and/or Payment Vendor

8.3. ACTION CLASSIFICATION

Action 1	Acknowledgement of receipt of reported issue or error
Action 2	Provide patch, workaround. temporary fix and document corrective action
Action 3	Official object code fix. update or major release and/or updated documentation

Incidents shall be tracked via a work request "ticket" that documents all correspondence through its entire "life cycle". The ticket is also used to collect vital information for the change management logs which detail all issues and the subsequent adjustments and revisions to the solution in question.

Note: Business days are Monday to Friday, excluding U.S. national holidays.

9. AGENCY RESPONSIBILITIES

The Agency will function as a single point of contact to work with information technology vendors and service vendors on behalf of the Agency Clients. Specifically the Agency is responsible for managing the implementation, maintenance, and use of the FileLocal tax portal for the participating cities, businesses and city customers.

9.1. AGENCY MANAGEMENT

The InterLocal Agreement outlines that the Agency is responsible for managing portal releases, upgrades, rules for access, use and maintenance, and expansion of the scope of Portal services with the approval by the Executive Board.

The Agency will work with the vendors to monitor the services in the Service Level Agreement and make adjustments to the services when necessary.

9.2. AGENCY CUSTOMER SERVICE SUPPORT

The Agency's Customer Service Support responsibilities are covered in the Help Desk Support Plan (Exhibit E). This plan will cover the key elements necessary for the function of a help desk and trace the support path through the system.

Participating City Administrator questions such as requests for data research and escalation to problem management are triaged through the Payment Vendor or Payment Vendor help desk and routed to the Agency when appropriate Monday through Friday from 8:00 a.m. to 5:00 p.m. (Pacific Time).

9.3. AGENCY PROBLEM MANAGEMENT

The Agency will provide a single point of contact to respond to requests for research and will utilize the Problem management process. Problem Management is the process by which problems identified within the FileLocal system are governed and managed. The Problem Management responsibilities are covered in the Problem Management Process Summary (for more information see supporting documentation G). The Agency is responsible for developing and implementing the problem management process. The vendors and cities are responsible for accepting and following the Problem Management process.

9.4. CHANGE MANAGEMENT

As part of Problem Management, the Agency will manage a Change Management process which shall control all changes in system functionality. A completed Change Request Form (for more information see Supporting Documentation J) must be submitted to the Agency to request any system enhancements or updates. For more details on the Change Management Process see the FileLocal Change Management Process Summary (for more information see Supporting Documentation I).

9.5. CITY ONBOARDING

Provide project management, technical and business support to facilitate adding new cities to the FileLocal Portal.

10. JOINT RESPONSIBILITIES

Several of the services described below require more than one of the parties of this agreement to share the responsibility for providing them. The services descriptions below outline which parties will share the responsibilities.

10.1. NEW CITIES IMPLEMENTATION TIME LINE:

The implementation time line starts from the date of contract signing (Effective Date) between the technology vendors, agency and new city and is primarily based on the number of print streams to be parsed, the number of templates to be created, as well as the number of non-standard features required. Once a City implementation documentation is completed then the Payment Vendor can calculate how long the implementation will take. Payment Vendor will present a draft project plan during the kick-off meeting and Client will then have the opportunity to determine if it will meet the time estimates Payment Vendor has identified for the Client's tasks. Once the Agency, the city, e-Gov Systems and Payment Vendor have all agreed on the project plan, every effort on both parties part must be made to meet this time line. Potential delays must be identified at least as soon as known, so that all parties can make suitable adjustments to the time line.

If Payment Vendor is the cause of the project's delay. Payment Vendor will make every reasonable effort to resolve the issue(s), including applicable internal escalation procedures, in order to ensure that the issue(s) will be resolved and new completion times will be estimated.

If the Agency Client, Agency or e-Gov Systems is the cause of the project's delay, the responsible party and/or will make every effort to resolve the issue(s). Failure to resolve the issue(s) in a timely manner (fifteen (15) business days), which causes Payment Vendor assets to be idle, will result in the reassignment of said assets to other projects and the project will be moved to the Payment Vendor project queue to be rescheduled as soon as the above mentioned resources become available.

10.2. INCIDENT REPORTING

Agency Clients will report incidents as appropriate to the Payment Vendor Help Desk as prescribed in the Help Desk Support Plan (Exhibit D).

Incident reporting will include a short description of the issue, the number of users impacted.

10.3. PROBLEM ANALYSIS

The Agency is responsible for providing analysis of incident trends as needed to assess requests for change. City and business users should submit their issues through the Vendor Help Desk Customer Service, who will then compile the issues and escalate them to the Agency Problem Manager.

The Agency will diagnosis and investigate problems, implement work a rounds, and submit Requests for Change as needed to the Change Management Process. This process is outlined in the Problem Management Process Summary (for more information see supporting documentation I).

10.4. USER PROVISIONING

An Agency Client is responsible for requesting new City system administrator's accounts. These accounts will be created by the Payment Vendor within 5 days of the City's request. Shorter Provisioning times may be requested by the City in emergency situations. The City and the Payment Vendor will follow the process outlined in the Operations Support Plan document (for more information see supporting documentation E)

City Administrators are responsible for provisioning City users per the process outlined in the City Maintenance Master Document (for more information see supporting documentation H).

The City is responsible for signing and maintaining the Chase Payment Tech PIGG.

10.5. NETWORK SERVICES

The Payment Vendor is responsible for providing adequate network infrastructure to meet the performance levels specified in this SLA (for more information see supporting documents A). Each Agency Client and e-Gov Systems, is responsible for providing adequate internal network infrastructure so as to not affect the Payment Vendor’s ability to meet those performance metrics. Each party is responsible for their own networks for the support, maintenance, and monitoring of their dedicated LAN and or WAN.

It is the direct responsibility of the Payment Vendor to report any outages as soon as they are known to the Agency Help Desk.

Payment Vendor and Agency bears no responsibility for performance and availability problems on networks within the Agency Client’s control or outside the Agency Client’s control (business user networks).

It should be noted that neither the cities nor Payment Vendor can control any Internet connectivity in between the networks, even if Virtual Private Networks (VPN) are used. Thus performance over any internet links cannot be guaranteed end to end.

10.6. RELATIONSHIP MANAGEMENT: STAFFING

Agency Clients will provide a single point of contact to the Agency. The contact person will triage issues to City technical and business staff related to all aspects of the application for development and operational matters.

The Agency will maintain and share with the Payment Vendor a document identifying the City’s points of contact.

11. Change Order Process for Service Levels

The Agency will maintain the Service Level Agreement with formal documentation denoting agreed upon changes. The Payment Vendor and the Agency will maintain copies of all Change Orders any alteration to the Service Level Agreement that causes an increase or decrease in the time or cost required for the performance of any part of this Service Level Agreement shall not become binding until both the Payment Vendor and the Agency have agreed upon an equitable adjustment and the Service Level Agreement has been modified in writing accordingly.

The Payment Vendor and the Agency must sign any proposed change orders. When this is accomplished, the change order will be incorporated as an official change to the service.

A change order process shall control changes in scope of the Service level Agreement. The Change Request Form (Exhibit H) must be used for all change order requests.

12. Supporting Documentation

A. Ramware Contract, Statement of Work, and Service Level Agreement



FAS3102, SOW, SLA 090816.pdf

B. Statement of Work



FL2016-09 Attachment B SOW.

C. KUBRA Operations Support Plan



Exhibit C_KUBRA Operations Support

D. KUBRA Help Desk Support Plan



Exhibit D_KUBRA Help Desk Support I

E. FileLocal Help Desk Support Plan (e-Gov Systems)



HelpDesk Support Plan V 1 5 7 (004).pd

F. Problem Management Process Summary



Problem Management Proces

G. FileLocal Change Management Process Summary



Change Management Proces

H. Change Request Form



Change Form 050516.pdf