PCI and NACHA Security Addendum

1. PCI, NACHA and Processing Requirements

1.1. Security of Payment Data and Responsibility for Compliance

For any contract in which the Vendor provides a solution that results in credit card payments to the County or Vendor, regardless of whether the County will pay a cost for the services being provided, Vendor is responsible for ensuring the credit card processing portion of the solution secures customer payment data and is compliant with Payment Card Industry Data Security Standard ("PCI-DSS") for the duration of the contract, as determined and verified by the Department of Finance. In addition, for any contract in which the Vendor provides a solution that results in ACH payments to the County or Vendor, regardless of whether the County will pay a cost for the services being provided, Vendor is responsible for ensuring the bank payment processing portion of the solution secures customer payment data and is compliant with National Automated Clearing House Association ("NACHA") Rules and Guidelines.

1.2. MID Ownership

Vendor's solution must use a MID obtained and owned by County from i) County's contracted or accepted processor or ii) if Vendor is a Payment Facilitator, from the Vendor's processor. Otherwise, Vendor's solution must use a MID obtained and owned by the Vendor, from a processor who is listed on the Visa Global Registry of Service Providers, and with whom Vendor has a contract. Vendor must indicate which MID ownership method will be used.

1.3. Card-Not-Present Transactions:

Online Payment Form Host

Vendor's payment solution must be PCI-DSS compliant and listed on the PCI Validated Payment Applications website or the Visa Global Registry of Service Providers website, OR Vendor's payment solution must present users with a payment information page that is **hosted by the processor selected for this solution and presented to customers using iframe or redirection technologies** (Vendor must provide a copy of system code demonstrating iframe or redirection).

1.4. Deposit of MID Funds and Bank to Bank Transmittal of Funds

If MID is owned by County, settled credit card payment funds must be deposited into County's bank account each day within 24 hours from date of transaction. If MID is owned by Vendor, settled credit card payment funds must first be deposited by Vendor's processor into Vendor's bank account before being transferred by Vendor to County's bank account. Vendor agrees to transfer all such funds directly from Vendor's bank account to the County's bank account within 24 hours from date funds were deposited into Vendor's bank account by Vendor's processor.

1.5. Integration with County's Enterprise Resource Planning System

Contractor is required to provide data elements related to Accounts Receivable, Accounts Payable, and General Ledger for accounting purposes on a monthly basis for integration to the County's Enterprise Resource Planning System in a secure and electronic manner.

1.6. Dispute of Chargebacks

If the MID is owned by Vendor, Vendor agrees to dispute credit card chargebacks and provide a method for reversing payment information in County's system in the event a dispute is unsuccessful.

-

1.7. Diagram of Payment Flow

Vendor must maintain and provide to the County a copy of its detailed diagram describing the start to finish payment flow in its payment solution with descriptions of equipment and services incorporated at each stage of the payment process.

1.8. Notice of Lost PCI Compliance

Vendor must immediately notify the County in writing in the event its payment solution, or its processor loses PCI compliance. Such notice will be provided to the County's contract administrator for this Contract.

1.9. Upgrades to Meet Any New Industry Requirements

As part of Vendor's maintenance and support of its payment solution, vendor must upgrade its solution to comply with any new PCI-DSS requirements, Card Brand (Visa, Mastercard, Discover and American Express) requirements, and County or Vendor processor requirements, by deadlines established by PCI, the Card Brands, or County or Vendor processor. Should Vendor fail to upgrade its payment solution to comply with any new PCI-DSS requirements, Card Brand requirements, or County processor requirements, and the County incurs losses as a result of such failure, Vendor must reimburse the County for such losses until Vendor's payment solution is upgraded to meet the new requirements.

1.10. Upgrade and Integrate if New Processor Selected

As part of Vendor's maintenance and support of its payment solution, in the event County replaces its processor with another processor, Vendor agrees to upgrade its payment solution to integrate with County's new processor within one year from notification from County.

2. Security Audit Requirements

2.1. SOC 2 Type 2 Audit Report

Vendor must provide an annual SSAE 18 (Service Organization Controls (SOC 2 Type 2) audit report, prepared by a qualified audit provider, to the County. For any deficiencies noted in the report, the Vendor agrees to also provide the County with the Vendor's remediation plans. Upon the County's request, the Vendor will provide the County a Bridge Letter to cover any portion of the County's fiscal year that is not covered under the Vendor's most current SOC 2 Type 2 audit report, in accordance with the terms and conditions of such report. The Vendor also agrees to provide the County with SOC 2 Type 2 audit reports and relevant remediation plans obtained from any service organizations providing services to the Vendor related to this Contract.