

**AMENDMENT #1 TO THE PERSONAL SERVICES CONTRACT WITH
Lexis-Nexis VitalChek (RES 17-155)**

THIS AMENDMENT #1 is dated this ___ day of May, 2019 by and between LexisNexis VitalChek Network Inc., hereinafter referred to as "CONTRACTOR" and COUNTY OF NEVADA, hereinafter referred to as "COUNTY", collectively the "Parties." Said Amendment will amend the prior Agreement between the parties entitled Personal Services Contract, as approved on April 11, 2017 per Resolution No. 17-155; and

WHEREAS, the CONTRACTOR provides credit, debit and electronic payment processing services on behalf of participating COUNTY departments for the contract term of April 11, 2017 through June 30, 2020; and

WHEREAS, the Parties desire to amend their Agreement to amend the Exhibit "A" Schedule of Services to clarify that COUNTY is not limited to utilizing CONTRACTOR as its sole and exclusive provider of credit, debit and electronic payment processing services, and that COUNTY and COUNTY departments may, at their option, contract with other providers of credit, debit and electronic payment processing services during the term of this Agreement.

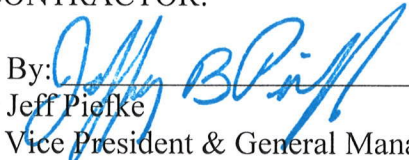
NOW, THEREFORE, the parties hereto agree as follows:

1. That Amendment #1 shall be effective as of May __, 2019.
2. That Exhibit "A", "Schedule of Services", shall be amended and replaced, as set forth in the amended Exhibit "A" attached hereto and incorporated herein.
3. That references to "LexisNexis VitalChek" in the Agreement shall mean "LexisNexis VitalChek Network Inc."
4. That in all other respects the prior Agreement of the parties shall remain in full force and effect.

COUNTY OF NEVADA:

By: _____
Honorable Richard Anderson

CONTRACTOR:

By:  _____
Jeff Piefke
Vice President & General Manager

ATTEST:

By: _____
Julie Patterson-Hunter
Clerk of the Board of Supervisors

EXHIBIT "A"

SCHEDULE OF SERVICES AND EQUIPMENT

(Provided By CONTRACTOR)

CONTRACTOR shall provide, at his expense, all the hardware and/or software required for electronic payment processing services to provide consumers who desire to pay for services rendered by participating COUNTY departments, the option of paying for such services using certain credit or debit cards. If requested, CONTRACTOR agrees to serve as an expert witness for COUNTY in any third party action or proceeding arising out of this Contract. The Parties understand and agree that this Agreement does not establish CONTRACTOR as COUNTY'S sole and exclusive provider of credit, debit and electronic payment processing services, and that COUNTY and its departments may, at their option, contract with other providers of services of credit, debit and electronic payment processing services during the term of this Agreement, which shall not constitute a breach of this Agreement.

The services provided by CONTRACTOR are described in accordance with this Service Schedule and are subject to and governed by the terms and conditions of the Agreement. In the case of conflict between the Contract ("Contract" or "Agreement") and **Exhibit A, B or C**, the provisions of the applicable Exhibit shall govern. Attached to this Schedule of Services and incorporated by reference into the Agreement at **Exhibit B** is the **Schedule of Charges and Payments**, which lists the fees to be paid to CONTRACTOR by the Customer and/or COUNTY for the Services.

The services to be provided by CONTRACTOR

1. Electronic Payment Services: CONTRACTOR agrees to accept electronic payments from customers using a major credit card or debit card, including VISA®, MasterCard®, American Express® and Discover®. CONTRACTOR will provide payments to be made through Point-of-sale(POS), a secure centralized web hosted payment system (described as VPS back office system) designed to allow County departments to accept payments via phone, access various reporting, and provide meta-data information as well as facilitate manual settlement (if not automatic), a secure branded website payment pages (either integrated and/or non-integrated) to allow County departments to offer constituents to pay online via check, or credit / debit cards. A Call Center provides a toll-free phone number for County constituents to call and make specific validated or non-validated payments to the County, while speaking to a live operator.
2. Business Continuity and Disaster Recovery: Documented incident response procedures are in place to guide activities in the event of a failure, security threat, or related operational event at the primary data center. In the event of system failure, the disaster recovery plan is executed by the network operations personnel. The plan includes switching the hosting to the backup site through rerouting domain addresses as well as switching the database clusters at the destination site from passive to active. Disaster recovery will be covered in our training program.

LexisNexis has a consistent record of providing greater than 99.9% service availability for payment processing to our customers. Our solutions availability is achieved through a multifaceted approach which includes multiple layers of redundancy, 24/7/365 monitoring/alerting, and response policies to quickly coordinate issue escalation and response. The primary data center has complete redundancy of its operations including all logical and physical aspects of the solution. In addition, LexisNexis maintains a failover disaster recovery site which mirrors data in real time from our primary data center. LexisNexis has specialized network routing equipment which allows us to failover quickly in the event of a catastrophic event.

3. Equipment to be provided: Point-of-Sale Equipment (VX520 and VX810 pin pads) to be provided by the CONTRACTOR to include power cords, and peripherals as needed for internet connection and for the acceptance of credit and debit cards. Equipment provided by CONTRACTOR shall

only be utilized by COUNTY departments in connection with credit, debit and electronic payment processing services provided by CONTRACTOR;

CONTRACTOR shall, at its expense and in its sole discretion, train appropriate personnel designated by COUNTY in the use and operation of the Equipment associated with the Service, at no additional cost to COUNTY.

In the event of equipment failure, replacement (POS) payment terminal will be provided and shipped to the COUNTY at no cost within 24 hours.

4. In conformity with industry security requirements, and in order to maintain the highest level of cardholder data security, CONTRACTOR has instituted, among other policies, Paper and Electronic Media Policies, which are designed to meet or exceed industry security standards (the "CONTRACTOR Policies"). An undated copy of the CONTRACTOR Policies has been provided to COUNTY with this Contract, and COUNTY agrees to comply with VitalChek Network, Inc "Paper and Electronic Media Policies" as set forth below as well as with appropriate industry accepted security practices for handling non-public personal information. CONTRACTOR agrees that the COUNTY is not required to comply with any amended policies adopted by CONTRACTOR from time to time unless CONTRACTOR provides such policies to the COUNTY. COUNTY acknowledges and agrees that (i) Cardholder data may only be used for assisting in completing a card transaction or as required by applicable law; (ii) In the event of a breach or intrusion of or otherwise unauthorized access to cardholder data stored within COUNTY's systems, COUNTY will immediately notify CONTRACTOR, and provide CONTRACTOR and/or its processor or the relevant card company access to COUNTY's facilities and all pertinent records to conduct a review of COUNTY's compliance with the security requirements, as well as fully cooperate with any reviews of facilities and records provided for in this paragraph.

**VITALCHEK NETWORK, INC.
Paper and Electronic Media Policies**

1.1 Policy Applicability

All employees handling hardcopy or electronic media must follow this policy. Departures from this policy will be permitted only if approved in advance and in writing by VitalChek.

1.2 Storage

1.2.1 Hardcopy Media

Hard copy material containing sensitive or confidential information (i.e.: paper receipts, paper reports, faxes, etc.) is subject to the following storage guidelines:

- At no time are printed reports containing sensitive information to be removed from any VitalChek or Agency secure office environment
- At no time is printed material containing sensitive information to be removed from any VitalChek data center or computer room without prior authorization from the General Manager.
- Printed reports containing consumer sensitive data are to be physically retained, stored or archived only within secure VitalChek or Agency office environments, and only for the minimum time deemed necessary for their use.
- All hardcopy material containing confidential or sensitive information should be clearly labeled as such.
- All sensitive hardcopy media must be stored securely in a safe or locking file cabinet

- Sensitive hardcopy material is never to be stored in employee desks or open workspaces

1.2.2 Electronic Media

Electronic media containing sensitive or confidential information (i.e.: CD, DVD, floppy disk, hard disk, tape, etc.) is subject to the following storage guidelines:

- Confidential and sensitive information should never be copied onto removable media without authorization from VitalChek's Information Technology Department.
- At no time is electronic media containing sensitive information to be removed from any VitalChek or Agency secure office environment, with the exception of computer system backups.
- At no time is electronic media containing sensitive information to be removed from any VitalChek data center or computer room without prior authorization from the Information Technology Department
- Electronic media containing consumer sensitive data are to be physically retained, stored or archived only within secure VitalChek or Agency office environments, and only for the minimum time deemed necessary for their use.
- All electronic media containing confidential or sensitive information should be clearly labeled as such.
- All removable, sensitive electronic media must be stored securely in a safe or approved locking file cabinet.
- All hardware (i.e. servers, workstations, modems, etc.) on which sensitive electronic media is stored shall be placed in a secure area and not be removed from a secure agency environment.