Contract #: AR3097

STATE OF UTAH COOPERATIVE CONTRACT

1. CONTRACTING PARTIES: This contract is between the Utah Division of Purchasing and the following Contractor:

Confi-Chek, Inc. (formerly Enformion)
Name

1921 21st Street
Street Address

Sacramento	CA	95811
City	*State*	*Zip*

Vendor # VC226564 Commodity Code #: 920-05 Legal Status of Contractor: Limited Liability Company

Contact *Name:* Scott Johnson *Phone Number:* 916-825-4901 *Email:* scott@enformion.com

2. CONTRACT PORTFOLIO NAME: Cloud Solutions.

3. GENERAL PURPOSE OF CONTRACT: Provide Cloud Solutions under the service models awarded in Attachment B.

4. PROCUREMENT: This contract is entered into as a result of the procurement process on FY2018, Solicitation# SK18008

5. CONTRACT PERIOD: Effective Date: Monday, April 15, 2019. Termination Date: Tuesday, September 15, 2026 unless terminated early or extended in accordance with the terms and conditions of this contract.

6. Administrative Fee: Contractor shall pay to NASPO ValuePoint, or its assignee, a NASPO ValuePoint Administrative Fee of one-quarter of one percent (0.25% or 0.0025) of contract sales no later than 60 days following the end of each calendar quarter. The NASPO ValuePoint Administrative Fee shall be submitted quarterly and is based on sales of the Services.

7. ATTACHMENT A: NASPO ValuePoint Master Terms and Conditions, including the attached Exhibits
ATTACHMENT B: Scope of Services Awarded to Contractor
ATTACHMENT C: Pricing Discounts and Schedule
ATTACHMENT D: Contractor's Response to Solicitation # SK18008
ATTACHMENT E: Service Offering EULAs, SLAs

Any conflicts between Attachment A and the other Attachments will be resolved in favor of Attachment A.

9. DOCUMENTS INCORPORATED INTO THIS CONTRACT BY REFERENCE BUT NOT ATTACHED:
   a. All other governmental laws, regulations, or actions applicable to the goods and/or services authorized by this contract.
   b. Utah Procurement Code, Procurement Rules, and Contractor's response to solicitation #SK18008.

10. Each signatory below represents that he or she has the requisite authority to enter into this contract.

IN WITNESS WHEREOF, the parties sign and cause this contract to be executed. Notwithstanding verbal or other representations by the parties, the "Effective Date" of this Contract shall be the date provided within Section 5 above.

CONTRACTOR

4/11/19

Contractor's signature Date

Rob Miller Chairman

Type or Print Name and Title

DIVISION OF PURCHASING

Christopher Hughes Apr 11, 2019

Christopher Hughes (Apr 11, 2019)

Director, Division of Purchasing Date

Attachment A: NASPO ValuePoint Master Agreement Terms and Conditions

1. Master Agreement Order of Precedence

a. Any Order placed under this Master Agreement shall consist of the following documents:

(1) A Participating Entity's Participating Addendum[1] ("PA");
(2) NASPO ValuePoint Master Agreement Terms & Conditions, including the applicable Exhibits[2] to the Master Agreement;
(3) The Solicitation;
(4) Contractor's response to the Solicitation, as revised (if permitted) and accepted by the Lead State; and
(5) A Service Level Agreement issued against the Participating Addendum.

b. These documents shall be read to be consistent and complementary. Any conflict among these documents shall be resolved by giving priority to these documents in the order listed above. Contractor terms and conditions that apply to this Master Agreement are only those that are expressly accepted by the Lead State and must be in writing and attached to this Master Agreement as an Exhibit or Attachment.

2. Definitions - Unless otherwise provided in this Master Agreement, capitalized terms will have the meanings given to those terms in this Section.

Confidential Information means any and all information of any form that is marked as confidential or would by its nature be deemed confidential obtained by Contractor or its employees or agents in the performance of this Master Agreement, including, but not necessarily limited to (1) any Purchasing Entity's records, (2) personnel records, and (3) information concerning individuals, is confidential information of Purchasing Entity.

Contractor means the person or entity providing solutions under the terms and conditions set forth in this Master Agreement. Contractor also includes its employees, subcontractors, agents and affiliates who are providing the services agreed to under the Master Agreement.

Data means all information, whether in oral or written (including electronic) form,

[1] A Sample Participating Addendum will be published after the contracts have been awarded.
[2] The Exhibits comprise the terms and conditions for the service models: PaaS, IaaS, and PaaS.

created by or in any way originating with a Participating Entity or Purchasing Entity, and all information that is the output of any computer processing, or other electronic manipulation, of any information that was created by or in any way originating with a Participating Entity or Purchasing Entity, in the course of using and configuring the Services provided under this Agreement.

Data Breach means any actual or reasonably suspected non-authorized access to or acquisition of computerized Non-Public Data or Personal Data that compromises the security, confidentiality, or integrity of the Non-Public Data or Personal Data, or the ability of Purchasing Entity to access the Non-Public Data or Personal Data.

Data Categorization means the process of risk assessment of Data. See also “High Risk Data”, “Moderate Risk Data” and “Low Risk Data”.

Disabling Code means computer instructions or programs, subroutines, code, instructions, data or functions, (including but not limited to viruses, worms, date bombs or time bombs), including but not limited to other programs, data storage, computer libraries and programs that self-replicate without manual intervention, instructions programmed to activate at a predetermined time or upon a specified event, and/or programs purporting to do a meaningful function but designed for a different function, that alter, destroy, inhibit, damage, interrupt, interfere with or hinder the operation of the Purchasing Entity’s’ software, applications and/or its end users processing environment, the system in which it resides, or any other software or data on such system or any other system with which it is capable of communicating.

Fulfillment Partner means a third-party contractor qualified and authorized by Contractor, and approved by the Participating State under a Participating Addendum, who may, to the extent authorized by Contractor, fulfill any of the requirements of this Master Agreement including but not limited to providing Services under this Master Agreement and billing Customers directly for such Services. Contractor may, upon written notice to the Participating State, add or delete authorized Fulfillment Partners as necessary at any time during the contract term. Fulfillment Partner has no authority to amend this Master Agreement or to bind Contractor to any additional terms and conditions.

High Risk Data is as defined in FIPS PUB 199, Standards for Security Categorization of Federal Information and Information Systems (“High Impact Data”).

Infrastructure as a Service (IaaS) as used in this Master Agreement is defined the capability provided to the consumer to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications; and possibly limited control of select networking components (e.g., host firewalls).

Intellectual Property means any and all patents, copyrights, service marks, trademarks, trade secrets, trade names, patentable inventions, or other similar proprietary rights, in tangible or intangible form, and all rights, title, and interest therein.

Lead State means the State centrally administering the solicitation and any resulting Master Agreement(s).

Low Risk Data is as defined in FIPS PUB 199, Standards for Security Categorization of Federal Information and Information Systems ("Low Impact Data").

Master Agreement means this agreement executed by and between the Lead State, acting on behalf of NASPO ValuePoint, and the Contractor, as now or hereafter amended.

Moderate Risk Data is as defined in FIPS PUB 199, Standards for Security Categorization of Federal Information and Information Systems ("Moderate Impact Data").

NASPO ValuePoint is the NASPO ValuePoint Cooperative Purchasing Program, facilitated by the NASPO Cooperative Purchasing Organization LLC, a 501(c)(3) limited liability company (doing business as NASPO ValuePoint) is a subsidiary organization the National Association of State Procurement Officials (NASPO), the sole member of NASPO ValuePoint. The NASPO ValuePoint Cooperative Purchasing Organization facilitates administration of the cooperative group contracting consortium of state chief procurement officials for the benefit of state departments, institutions, agencies, and political subdivisions and other eligible entities (i.e., colleges, school districts, counties, cities, some nonprofit organizations, etc.) for all states and the District of Columbia. The NASPO ValuePoint Cooperative Development Team is identified in the Master Agreement as the recipient of reports and may be performing contract administration functions as assigned by the Lead State.

Non-Public Data means High Risk Data and Moderate Risk Data that is not subject to distribution to the public as public information. It is deemed to be sensitive and confidential by the Purchasing Entity because it contains information that is exempt by statute, ordinance or administrative rule from access by the general public as public information.

Participating Addendum means a bilateral agreement executed by a Contractor and a Participating Entity incorporating this Master Agreement and any other additional Participating Entity specific language or other requirements, e.g. ordering procedures specific to the Participating Entity, other terms and conditions.

Participating Entity means a state, or other legal entity, properly authorized to enter into a Participating Addendum.

Participating State means a state, the District of Columbia, or one of the territories of the United States that is listed in the Request for Proposal as intending to participate.

Upon execution of the Participating Addendum, a Participating State becomes a Participating Entity.

Personal Data means data alone or in combination that includes information relating to an individual that identifies the individual by name, identifying number, mark or description can be readily associated with a particular individual and which is not a public record. Personal Information may include the following personally identifiable information (PII): government-issued identification numbers (e.g., Social Security, driver's license, passport); financial account information, including account number, credit or debit card numbers; or Protected Health Information (PHI) relating to a person.

Platform as a Service (PaaS) as used in this Master Agreement is defined as the capability provided to the consumer to deploy onto the cloud infrastructure consumer-created or -acquired applications created using programming languages and tools supported by the provider. This capability does not necessarily preclude the use of compatible programming languages, libraries, services, and tools from other sources. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations.

Product means any deliverable under this Master Agreement, including Services, software, and any incidental tangible goods.

Protected Health Information (PHI) means individually identifiable health information transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium. PHI excludes education records covered by the Family Educational Rights and Privacy Act (FERPA), as amended, 20 U.S.C. 1232g, records described at 20 U.S.C. 1232g(a)(4)(B)(iv) and employment records held by a covered entity in its role as employer. PHI may also include information that is a subset of health information, including demographic information collected from an individual, and (1) is created or received by a health care provider, health plan, employer or health care clearinghouse; and (2) relates to the past, present or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual; and (a) that identifies the individual; or (b) with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Purchasing Entity means a state, city, county, district, other political subdivision of a State, and a nonprofit organization under the laws of some states if authorized by a Participating Addendum, who issues a Purchase Order against the Master Agreement and becomes financially committed to the purchase.

Services mean any of the specifications described in the Scope of Services that are supplied or created by the Contractor pursuant to this Master Agreement.

Security Incident means the possible or actual unauthorized access to a Purchasing

Entity's Non-Public Data and Personal Data the Contractor believes could reasonably result in the use, disclosure or theft of a Purchasing Entity's Non-Public Data within the possession or control of the Contractor. A Security Incident also includes a major security breach to the Contractor's system, regardless if Contractor is aware of unauthorized access to a Purchasing Entity's Non-Public Data. A Security Incident may or may not turn into a Data Breach.

Service Level Agreement (SLA) means a written agreement between both the Purchasing Entity and the Contractor that is subject to the terms and conditions in this Master Agreement and relevant Participating Addendum unless otherwise expressly agreed in writing between the Purchasing Entity and the Contractor. SLAs should include: (1) the technical service level performance promises, (i.e. metrics for performance and intervals for measure), (2) description of service quality, (3) identification of roles and responsibilities, (4) remedies, such as credits, and (5) an explanation of how remedies or credits are calculated and issued.

Software as a Service (SaaS) as used in this Master Agreement is defined as the capability provided to the consumer to use the Contractor's applications running on a Contractor's infrastructure (commonly referred to as 'cloud infrastructure). The applications are accessible from various client devices through a thin client interface such as a Web browser (e.g., Web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

Solicitation means the documents used by the State of Utah, as the Lead State, to obtain Contractor's Proposal.

Statement of Work means a written statement in a solicitation document or contract that describes the Purchasing Entity's service needs and expectations.

3. Term of the Master Agreement: Unless otherwise specified as a shorter term in a Participating Addendum, the term of the Master Agreement will run from contract execution to September 15, 2026.

4. Amendments: The terms of this Master Agreement shall not be waived, altered, modified, supplemented or amended in any manner whatsoever without prior written approval of the Lead State and Contractor.

5. Assignment/Subcontracts: Contractor shall not assign, sell, transfer, or sublet rights, or delegate responsibilities under this Master Agreement, in whole or in part, without the prior written approval of the Lead State.

The Lead State reserves the right to assign any rights or duties, including written assignment of contract administration duties to the NASPO Cooperative Purchasing Organization LLC, doing business as NASPO ValuePoint.

6. Discount Guarantee Period: All discounts must be guaranteed for the entire term of the Master Agreement. Participating Entities and Purchasing Entities shall receive the immediate benefit of price or rate reduction of the services provided under this Master Agreement. A price or rate reduction will apply automatically to the Master Agreement and an amendment is not necessary.

7. Termination: Unless otherwise stated, this Master Agreement may be terminated by either party upon 60 days written notice prior to the effective date of the termination. Further, any Participating Entity may terminate its participation upon 30 days written notice, unless otherwise limited or stated in the Participating Addendum. Termination may be in whole or in part. Any termination under this provision shall not affect the rights and obligations attending orders outstanding at the time of termination, including any right of any Purchasing Entity to indemnification by the Contractor, rights of payment for Services delivered and accepted, data ownership, Contractor obligations regarding Purchasing Entity Data, rights attending default in performance an applicable Service Level of Agreement in association with any Order, Contractor obligations under Termination and Suspension of Service, and any responsibilities arising out of a Security Incident or Data Breach. Termination of the Master Agreement due to Contractor default may be immediate.

8. Confidentiality, Non-Disclosure, and Injunctive Relief

a. Confidentiality. Contractor acknowledges that it and its employees or agents may, in the course of providing a Product under this Master Agreement, be exposed to or acquire information that is confidential to Purchasing Entity's or Purchasing Entity's clients. Any reports or other documents or items (including software) that result from the use of the Confidential Information by Contractor shall be treated in the same manner as the Confidential Information. Confidential Information does not include information that (1) is or becomes (other than by disclosure by Contractor) publicly known; (2) is furnished by Purchasing Entity to others without restrictions similar to those imposed by this Master Agreement; (3) is rightfully in Contractor's possession without the obligation of nondisclosure prior to the time of its disclosure under this Master Agreement; (4) is obtained from a source other than Purchasing Entity without the obligation of confidentiality, (5) is disclosed with the written consent of Purchasing Entity or; (6) is independently developed by employees, agents or subcontractors of Contractor who can be shown to have had no access to the Confidential Information.

b. Non-Disclosure. Contractor shall hold Confidential Information in confidence, using at least the industry standard of confidentiality, and shall not copy, reproduce, sell, assign, license, market, transfer or otherwise dispose of, give, or disclose Confidential Information to third parties or use Confidential Information for any purposes whatsoever other than what is necessary to the performance of Orders placed under this Master Agreement. Contractor shall advise each of its employees and agents of their obligations to keep Confidential Information confidential. Contractor shall use commercially reasonable efforts to assist Purchasing Entity in identifying and preventing any unauthorized use or disclosure of any Confidential Information. Without limiting the generality of the foregoing, Contractor shall advise Purchasing Entity, applicable Participating Entity, and the Lead State immediately if Contractor learns or has reason

to believe that any person who has had access to Confidential Information has violated or intends to violate the terms of this Master Agreement, and Contractor shall at its expense cooperate with Purchasing Entity in seeking injunctive or other equitable relief in the name of Purchasing Entity or Contractor against any such person. Except as directed by Purchasing Entity, Contractor will not at any time during or after the term of this Master Agreement disclose, directly or indirectly, any Confidential Information to any person, except in accordance with this Master Agreement, and that upon termination of this Master Agreement or at Purchasing Entity's request, Contractor shall turn over to Purchasing Entity all documents, papers, and other matter in Contractor's possession that embody Confidential Information. Notwithstanding the foregoing, Contractor may keep one copy of such Confidential Information necessary for quality assurance, audits and evidence of the performance of this Master Agreement.

c. Injunctive Relief. Contractor acknowledges that breach of this section, including disclosure of any Confidential Information, will cause irreparable injury to Purchasing Entity that is inadequately compensable in damages. Accordingly, Purchasing Entity may seek and obtain injunctive relief against the breach or threatened breach of the foregoing undertakings, in addition to any other legal remedies that may be available. Contractor acknowledges and agrees that the covenants contained herein are necessary for the protection of the legitimate business interests of Purchasing Entity and are reasonable in scope and content.

d. Purchasing Entity Law. These provisions shall be applicable only to extent they are not in conflict with the applicable public disclosure laws of any Purchasing Entity.

9. Right to Publish: Throughout the duration of this Master Agreement, Contractor must secure prior approval from the Lead State or Participating Entity for the release of any information that pertains to the potential work or activities covered by the Master Agreement , including but not limited to reference to or use of the Lead State or a Participating Entity's name, Great Seal of the State, Coat of Arms, any Agency or other subunits of the State government, or any State official or employee, for commercial promotion which is strictly prohibited. News releases or release of broadcast e-mails pertaining to this Master Agreement or Participating Addendum shall not be made without prior written approval of the Lead State or a Participating Entity.

The Contractor shall not make any representations of NASPO ValuePoint's opinion or position as to the quality or effectiveness of the services that are the subject of this Master Agreement without prior written consent. Failure to adhere to this requirement may result in termination of the Master Agreement for cause.

10. Defaults and Remedies

a. The occurrence of any of the following events shall be an event of default under this Master Agreement:

(1) Nonperformance of contractual requirements; or

(2) A material breach of any term or condition of this Master Agreement; or

(3) Any certification, representation or warranty by Contractor in response to the

solicitation or in this Master Agreement that proves to be untrue or materially misleading; or

(4) Institution of proceedings under any bankruptcy, insolvency, reorganization or similar law, by or against Contractor, or the appointment of a receiver or similar officer for Contractor or any of its property, which is not vacated or fully stayed within thirty (30) calendar days after the institution or occurrence thereof; or

(5) Any default specified in another section of this Master Agreement.

b. Upon the occurrence of an event of default, Lead State shall issue a written notice of default, identifying the nature of the default, and providing a period of 30 calendar days in which Contractor shall have an opportunity to cure the default. The Lead State shall not be required to provide advance written notice or a cure period and may immediately terminate this Master Agreement in whole or in part if the Lead State, in its sole discretion, determines that it is reasonably necessary to preserve public safety or prevent immediate public crisis. Time allowed for cure shall not diminish or eliminate Contractor's liability for damages.

c. If Contractor is afforded an opportunity to cure and fails to cure the default within the period specified in the written notice of default, Contractor shall be in breach of its obligations under this Master Agreement and Lead State shall have the right to exercise any or all of the following remedies:

(1) Exercise any remedy provided by law; and

(2) Terminate this Master Agreement and any related Contracts or portions thereof; and

(3) Suspend Contractor from being able to respond to future bid solicitations; and

(4) Suspend Contractor's performance; and

(5) Withhold payment until the default is remedied.

d. Unless otherwise specified in the Participating Addendum, in the event of a default under a Participating Addendum, a Participating Entity shall provide a written notice of default as described in this section and have all of the rights and remedies under this paragraph regarding its participation in the Master Agreement, in addition to those set forth in its Participating Addendum. Nothing in these Master Agreement Terms and Conditions shall be construed to limit the rights and remedies available to a Purchasing Entity under the applicable commercial code.

11. Changes in Contractor Representation: The Contractor must notify the Lead State of changes in the Contractor's key administrative personnel, in writing within 10 calendar days of the change. The Lead State reserves the right to approve changes in key personnel, as identified in the Contractor's proposal. The Contractor agrees to propose replacement key personnel having substantially equal or better education, training, and experience as was possessed by the key person proposed and evaluated in the Contractor's proposal.

12. Force Majeure: Neither party shall be in default by reason of any failure in

performance of this Contract in accordance with reasonable control and without fault or negligence on their part. Such causes may include, but are not restricted to, acts of nature or the public enemy, acts of the government in either its sovereign or contractual capacity, fires, floods, epidemics, quarantine restrictions, strikes, freight embargoes and unusually severe weather, but in every case the failure to perform such must be beyond the reasonable control and without the fault or negligence of the party.

13. Indemnification

a. The Contractor shall defend, indemnify and hold harmless NASPO, NASPO ValuePoint, the Lead State, Participating Entities, and Purchasing Entities, along with their officers, agents, and employees as well as any person or entity for which they may be liable, from and against claims, damages or causes of action including reasonable attorneys' fees and related costs for any death, injury, or damage to property arising directly or indirectly from act(s), error(s), or omission(s) of the Contractor, its employees or subcontractors or volunteers, at any tier, relating to the performance under the Master Agreement.

b. Indemnification – Intellectual Property. The Contractor shall defend, indemnify and hold harmless NASPO, NASPO ValuePoint, the Lead State, Participating Entities, Purchasing Entities, along with their officers, agents, and employees as well as any person or entity for which they may be liable ("Indemnified Party"), from and against claims, damages or causes of action including reasonable attorneys' fees and related costs arising out of the claim that the Product or its use, infringes Intellectual Property rights ("Intellectual Property Claim") of another person or entity.

(1) The Contractor's obligations under this section shall not extend to any claims arising from the combination of the Product with any other product, system or method, unless the Product, system or method is:

(a) provided by the Contractor or the Contractor's subsidiaries or affiliates;

(b) specified by the Contractor to work with the Product; or

(c) reasonably required, in order to use the Product in its intended manner, and the infringement could not have been avoided by substituting another reasonably available product, system or method capable of performing the same function; or

(d) It would be reasonably expected to use the Product in combination with such product, system or method.

(2) The Indemnified Party shall notify the Contractor within a reasonable time after receiving notice of an Intellectual Property Claim. Even if the Indemnified Party fails to provide reasonable notice, the Contractor shall not be relieved from its obligations unless the Contractor can demonstrate that it was prejudiced in defending the Intellectual Property Claim resulting in increased expenses or loss to the Contractor and then only to the extent of the prejudice or expenses. If the Contractor promptly and

reasonably investigates and defends any Intellectual Property Claim, it shall have control over the defense and settlement of it. However, the Indemnified Party must consent in writing for any money damages or obligations for which it may be responsible. The Indemnified Party shall furnish, at the Contractor's reasonable request and expense, information and assistance necessary for such defense. If the Contractor fails to vigorously pursue the defense or settlement of the Intellectual Property Claim, the Indemnified Party may assume the defense or settlement of it and the Contractor shall be liable for all costs and expenses, including reasonable attorneys' fees and related costs, incurred by the Indemnified Party in the pursuit of the Intellectual Property Claim. Unless otherwise agreed in writing, this section is not subject to any limitations of liability in this Master Agreement or in any other document executed in conjunction with this Master Agreement.

14. Independent Contractor: The Contractor shall be an independent contractor. Contractor shall have no authorization, express or implied, to bind the Lead State, Participating States, other Participating Entities, or Purchasing Entities to any agreements, settlements, liability or understanding whatsoever, and agrees not to hold itself out as agent except as expressly set forth herein or as expressly agreed in any Participating Addendum.

15. Individual Customers: Except to the extent modified by a Participating Addendum, each Purchasing Entity shall follow the terms and conditions of the Master Agreement and applicable Participating Addendum and will have the same rights and responsibilities for their purchases as the Lead State has in the Master Agreement, including but not limited to, any indemnity or right to recover any costs as such right is defined in the Master Agreement and applicable Participating Addendum for their purchases. Each Purchasing Entity will be responsible for its own charges, fees, and liabilities. The Contractor will apply the charges and invoice each Purchasing Entity individually.

16. Insurance

a. Unless otherwise agreed in a Participating Addendum, Contractor shall, during the term of this Master Agreement, maintain in full force and effect, the insurance described in this section. Contractor shall acquire such insurance from an insurance carrier or carriers licensed to conduct business in each Participating Entity's state and having a rating of A-, Class VII or better, in the most recently published edition of Best's Reports. Failure to buy and maintain the required insurance may result in this Master Agreement's termination or, at a Participating Entity's option, result in termination of its Participating Addendum.

b. Coverage shall be written on an occurrence basis. The minimum acceptable limits shall be as indicated below, with no deductible for each of the following categories:

(1) Commercial General Liability covering premises operations, independent contractors, products and completed operations, blanket contractual liability, personal injury (including death), advertising liability, and property damage, with a limit of not less than $1 million per occurrence/$3 million general

aggregate;

(2) CLOUD MINIMUM INSURANCE COVERAGE:

Level of Risk	**Data Breach and Privacy/Cyber Liability including Technology Errors and Omissions** Minimum Insurance Coverage
Low Risk Data	$2,000,000
Moderate Risk Data	$5,000,000
High Risk Data	$10,000,000

(3) Contractor must comply with any applicable State Workers Compensation or Employers Liability Insurance requirements.

(4) Professional Liability. As applicable, Professional Liability Insurance Policy in the minimum amount of $1,000,000 per occurrence and $1,000,000 in the aggregate, written on an occurrence form that provides coverage for its work undertaken pursuant to each Participating Addendum.

c. Contractor shall pay premiums on all insurance policies. Such policies shall also reference this Master Agreement and shall have a condition that they not be revoked by the insurer until thirty (30) calendar days after notice of intended revocation thereof shall have been given to Purchasing Entity and Participating Entity by the Contractor.

d. Prior to commencement of performance, Contractor shall provide to the Lead State a written endorsement to the Contractor's general liability insurance policy or other documentary evidence acceptable to the Lead State that (1) names the Participating States identified in the Request for Proposal as additional insureds, (2) provides that no material alteration, cancellation, non-renewal, or expiration of the coverage contained in such policy shall have effect unless the named Participating State has been given at least thirty (30) days prior written notice, and (3) provides that the Contractor's liability insurance policy shall be primary, with any liability insurance of any Participating State as secondary and noncontributory. Unless otherwise agreed in any Participating Addendum, the Participating Entity's rights and Contractor's obligations are the same as those specified in the first sentence of this subsection. Before performance of any Purchase Order issued after execution of a Participating Addendum authorizing it, the Contractor shall provide to a Purchasing Entity or Participating Entity who requests it the same information described in this subsection.

e. Contractor shall furnish to the Lead State, Participating Entity, and, on request, the Purchasing Entity copies of certificates of all required insurance within thirty (30) calendar days of the execution of this Master Agreement, the execution of a Participating Addendum, or the Purchase Order's effective date and prior to performing any work. The insurance certificate shall provide the following information: the name and address of the insured; name, address, telephone number and signature of the authorized agent; name of the insurance company (authorized to operate in all states);

a description of coverage in detailed standard terminology (including policy period, policy number, limits of liability, exclusions and endorsements); and an acknowledgment of the requirement for notice of cancellation. Copies of renewal certificates of all required insurance shall be furnished within thirty (30) days after any renewal date. These certificates of insurance must expressly indicate compliance with each and every insurance requirement specified in this section. Failure to provide evidence of coverage may, at sole option of the Lead State, or any Participating Entity, result in this Master Agreement's termination or the termination of any Participating Addendum.

f. Coverage and limits shall not limit Contractor's liability and obligations under this Master Agreement, any Participating Addendum, or any Purchase Order.

17. Laws and Regulations: Any and all Services offered and furnished shall comply fully with all applicable Federal and State laws and regulations.

18. No Waiver of Sovereign Immunity: In no event shall this Master Agreement, any Participating Addendum or any contract or any Purchase Order issued thereunder, or any act of a Lead State, a Participating Entity, or a Purchasing Entity be a waiver of any form of defense or immunity, whether sovereign immunity, governmental immunity, immunity based on the Eleventh Amendment to the Constitution of the United States or otherwise, from any claim or from the jurisdiction of any court.

This section applies to a claim brought against the Participating State only to the extent Congress has appropriately abrogated the Participating State's sovereign immunity and is not consent by the Participating State to be sued in federal court. This section is also not a waiver by the Participating State of any form of immunity, including but not limited to sovereign immunity and immunity based on the Eleventh Amendment to the Constitution of the United States.

19. Ordering

a. Master Agreement order and purchase order numbers shall be clearly shown on all acknowledgments, shipping labels, packing slips, invoices, and on all correspondence.

b. This Master Agreement permits Purchasing Entities to define project-specific requirements and informally compete the requirement among other firms having a Master Agreement on an "as needed" basis. This procedure may also be used when requirements are aggregated or other firm commitments may be made to achieve reductions in pricing. This procedure may be modified in Participating Addenda and adapted to Purchasing Entity rules and policies. The Purchasing Entity may in its sole discretion determine which firms should be solicited for a quote. The Purchasing Entity may select the quote that it considers most advantageous, cost and other factors considered.

c. Each Purchasing Entity will identify and utilize its own appropriate purchasing procedure and documentation. Contractor is expected to become familiar with the Purchasing Entities' rules, policies, and procedures regarding the ordering of supplies and/or services contemplated by this Master Agreement.

d. Contractor shall not begin providing Services without a valid Service Level Agreement or other appropriate commitment document compliant with the law of the Purchasing Entity.

e. Orders may be placed consistent with the terms of this Master Agreement during the term of the Master Agreement.

f. All Orders pursuant to this Master Agreement, at a minimum, shall include:

(1) The services or supplies being delivered;
(2) The place and requested time of delivery;
(3) A billing address;
(4) The name, phone number, and address of the Purchasing Entity representative;
(5) The price per unit or other pricing elements consistent with this Master Agreement and the contractor's proposal;
(6) A ceiling amount of the order for services being ordered; and
(7) The Master Agreement identifier and the Participating State contract identifier.

g. All communications concerning administration of Orders placed shall be furnished solely to the authorized purchasing agent within the Purchasing Entity's purchasing office, or to such other individual identified in writing in the Order.

h. Orders must be placed pursuant to this Master Agreement prior to the termination date of this Master Agreement. Contractor is reminded that financial obligations of Purchasing Entities payable after the current applicable fiscal year are contingent upon agency funds for that purpose being appropriated, budgeted, and otherwise made available.

i. Notwithstanding the expiration or termination of this Master Agreement, Contractor agrees to perform in accordance with the terms of any Orders then outstanding at the time of such expiration or termination. Contractor shall not honor any Orders placed after the expiration or termination of this Master Agreement. Orders from any separate indefinite quantity, task orders, or other form of indefinite delivery order arrangement priced against this Master Agreement may not be placed after the expiration or termination of this Master Agreement, notwithstanding the term of any such indefinite delivery order agreement.

20. Participants and Scope

a. Contractor may not deliver Services under this Master Agreement until a Participating Addendum acceptable to the Participating Entity and Contractor is executed. The NASPO ValuePoint Master Agreement Terms and Conditions are applicable to any Order by a Participating Entity (and other Purchasing Entities covered by their Participating Addendum), except to the extent altered, modified, supplemented or amended by a Participating Addendum. By way of illustration and not limitation, this

authority may apply to unique delivery and invoicing requirements, confidentiality requirements, defaults on Orders, governing law and venue relating to Orders by a Participating Entity, indemnification, and insurance requirements. Statutory or constitutional requirements relating to availability of funds may require specific language in some Participating Addenda in order to comply with applicable law. The expectation is that these alterations, modifications, supplements, or amendments will be addressed in the Participating Addendum or, with the consent of the Purchasing Entity and Contractor, may be included in the ordering document (e.g. purchase order or contract) used by the Purchasing Entity to place the Order.

b. Subject to subsection 20c and a Participating Entity's Participating Addendum, the use of specific NASPO ValuePoint cooperative Master Agreements by state agencies, political subdivisions and other Participating Entities (including cooperatives) authorized by individual state's statutes to use state contracts is subject to the approval of the respective State Chief Procurement Official.

c. Unless otherwise stipulated in a Participating Entity's Participating Addendum, specific services accessed through the NASPO ValuePoint cooperative Master Agreements for Cloud Services by state executive branch agencies, as required by a Participating Entity's statutes, are subject to the authority and approval of the Participating Entity's Chief Information Officer's Office[3].

d. Obligations under this Master Agreement are limited to those Participating Entities who have signed a Participating Addendum and Purchasing Entities within the scope of those Participating Addenda. States or other entities permitted to participate may use an informal competitive process to determine which Master Agreements to participate in through execution of a Participating Addendum. Financial obligations of Participating States are limited to the orders placed by the departments or other state agencies and institutions having available funds. Participating States incur no financial obligations on behalf of political subdivisions.

e. NASPO ValuePoint is not a party to the Master Agreement. It is a nonprofit cooperative purchasing organization assisting states in administering the NASPO ValuePoint cooperative purchasing program for state government departments, institutions, agencies and political subdivisions (e.g., colleges, school districts, counties, cities, etc.) for all 50 states, the District of Columbia and the territories of the United States.

f. Participating Addenda shall not be construed to amend the terms of this Master Agreement between the Lead State and Contractor.

g. Participating Entities who are not states may under some circumstances sign their own Participating Addendum, subject to the approval of participation by the Chief Procurement Official of the state where the Participating Entity is located. Coordinate

[3] Chief Information Officer means the individual designated by the Governor with Executive Branch, enterprise-wide responsibility for the leadership and management of information technology resources of a state.

requests for such participation through NASPO ValuePoint. Any permission to participate through execution of a Participating Addendum is not a determination that procurement authority exists in the Participating Entity; they must ensure that they have the requisite procurement authority to execute a Participating Addendum.

h. Resale. Subject to any explicit permission in a Participating Addendum, Purchasing Entities may not resell goods, software, or Services obtained under this Master Agreement. This limitation does not prohibit: payments by employees of a Purchasing Entity as explicitly permitted under this agreement; sales of goods to the general public as surplus property; and fees associated with inventory transactions with other governmental or nonprofit entities under cooperative agreements and consistent with a Purchasing Entity's laws and regulations. Any sale or transfer permitted by this subsection must be consistent with license rights granted for use of intellectual property.

21. Payment: Orders under this Master Agreement are fixed-price or fixed-rate orders, not cost reimbursement contracts. Unless otherwise stipulated in the Participating Addendum, Payment is normally made within 30 days following the date of a correct invoice is received. Purchasing Entities reserve the right to withhold payment of a portion (including all if applicable) of disputed amount of an invoice. After 45 days the Contractor may assess overdue account charges up to a maximum rate of one percent per month on the outstanding balance. Payments will be remitted by mail. Payments may be made via a State or political subdivision "Purchasing Card" with no additional charge.

22. Data Access Controls: Contractor will provide access to Purchasing Entity's Data only to those Contractor employees, contractors and subcontractors ("Contractor Staff") who need to access the Data to fulfill Contractor's obligations under this Agreement. Contractor shall not access a Purchasing Entity's user accounts or Data, except on the course of data center operations, response to service or technical issues, as required by the express terms of this Master Agreement, or at a Purchasing Entity's written request.

Contractor may not share a Purchasing Entity's Data with its parent corporation, other affiliates, or any other third party without the Purchasing Entity's express written consent.

Contractor will ensure that, prior to being granted access to the Data, Contractor Staff who perform work under this Agreement have successfully completed annual instruction of a nature sufficient to enable them to effectively comply with all Data protection provisions of this Agreement; and possess all qualifications appropriate to the nature of the employees' duties and the sensitivity of the Data they will be handling.

23. Operations Management: Contractor shall maintain the administrative, physical, technical, and procedural infrastructure associated with the provision of the Product in a manner that is, at all times during the term of this Master Agreement, at a level equal to or more stringent than those specified in the Solicitation.

24. Public Information: This Master Agreement and all related documents are subject to disclosure pursuant to the Purchasing Entity's public information laws.

25. Purchasing Entity Data: Purchasing Entity retains full right and title to Data provided by it and any Data derived therefrom, including metadata.
Contractor shall not collect, access, or use user-specific Purchasing Entity Data except as strictly necessary to provide Service to the Purchasing Entity. No information regarding Purchasing Entity's use of the Service may be disclosed, provided, rented or sold to any third party for any reason unless required by law or regulation or by an order of a court of competent jurisdiction. The obligation shall extend beyond the term of this Master Agreement in perpetuity.

Contractor shall not use any information collected in connection with this Master Agreement, including Purchasing Entity Data, for any purpose other than fulfilling its obligations under this Master Agreement.

26. Records Administration and Audit.

a. The Contractor shall maintain books, records, documents, and other evidence pertaining to this Master Agreement and orders placed by Purchasing Entities under it to the extent and in such detail as shall adequately reflect performance and administration of payments and fees. Contractor shall permit the Lead State, a Participating Entity, a Purchasing Entity, the federal government (including its grant awarding entities and the U.S. Comptroller General), and any other duly authorized agent of a governmental agency, to audit, inspect, examine, copy and/or transcribe Contractor's books, documents, papers and records directly pertinent to this Master Agreement or orders placed by a Purchasing Entity under it for the purpose of making audits, examinations, excerpts, and transcriptions. This right shall survive for a period of six (6) years following termination of this Agreement or final payment for any order placed by a Purchasing Entity against this Agreement, whichever is later, to assure compliance with the terms hereof or to evaluate performance hereunder.

b. Without limiting any other remedy available to any governmental entity, the Contractor shall reimburse the applicable Lead State, Participating Entity, or Purchasing Entity for any overpayments inconsistent with the terms of the Master Agreement or orders or underpayment of fees found as a result of the examination of the Contractor's records.

c. The rights and obligations herein exist in addition to any quality assurance obligation in the Master Agreement requiring the Contractor to self-audit contract obligations and that permits the Lead State to review compliance with those obligations.

d. The Contractor shall allow the Purchasing Entity to audit conformance to the Master Agreement and applicable Participating Addendum terms. The purchasing entity may perform this audit or contract with a third party at its discretion and at the purchasing entity's expense.

27. Administrative Fees: The Contractor shall pay to NASPO ValuePoint, or its

assignee, a NASPO ValuePoint Administrative Fee of one-quarter of one percent (0.25% or 0.0025) no later than 60 days following the end of each calendar quarter. The NASPO ValuePoint Administrative Fee shall be submitted quarterly and is based on sales of the Services. The NASPO ValuePoint Administrative Fee is not negotiable. This fee is to be included as part of the pricing submitted with proposal.

Additionally, some states may require an additional administrative fee be paid directly to the state on purchases made by Purchasing Entities within that state. For all such requests, the fee level, payment method and schedule for such reports and payments will be incorporated into the Participating Addendum that is made a part of the Master Agreement. The Contractor may adjust the Master Agreement pricing accordingly for purchases made by Purchasing Entities within the jurisdiction of the state. All such agreements shall not affect the NASPO ValuePoint Administrative Fee percentage or the prices paid by the Purchasing Entities outside the jurisdiction of the state requesting the additional fee. The NASPO ValuePoint Administrative Fee shall be based on the gross amount of all sales at the adjusted prices (if any) in Participating Addenda.

28. System Failure or Damage: In the event of system failure or damage caused by Contractor or its Services, the Contractor agrees to use its best efforts to restore or assist in restoring the system to operational capacity.

29. Title to Product: If access to the Product requires an application program interface (API), Contractor shall convey to Purchasing Entity an irrevocable and perpetual license to use the API.

30. Data Privacy: The Contractor must comply with all applicable laws related to data privacy and security, including IRS Pub 1075. Prior to entering into a SLA with a Purchasing Entity, the Contractor and Purchasing Entity must cooperate and hold a meeting to determine the Data Categorization to determine whether the Contractor will hold, store, or process High Risk Data, Moderate Risk Data and Low Risk Data. The Contractor must document the Data Categorization in the SLA or Statement of Work.

31. Warranty: At a minimum the Contractor must warrant the following:

a. Contractor has acquired any and all rights, grants, assignments, conveyances, licenses, permissions, and authorization for the Contractor to provide the Services described in this Master Agreement.

b. Contractor will perform materially as described in this Master Agreement, SLA, Statement of Work, including any performance representations contained in the Contractor's response to the Solicitation by the Lead State.

c. Contractor represents and warrants that the representations contained in its response to the Solicitation by the Lead State.

d. The Contractor will not interfere with a Purchasing Entity's access to and use of the

Services it acquires from this Master Agreement.

e. The Services provided by the Contractor are compatible with and will operate successfully with any environment (including web browser and operating system) specified by the Contractor in its response to the Solicitation by the Lead State.

f. The Contractor warrants that the Products it provides under this Master Agreement are free of malware. The Contractor must use industry-leading technology to detect and remove worms, Trojans, rootkits, rogues, dialers, spyware, etc.

32. Transition Assistance:

a. The Contractor shall reasonably cooperate with other parties in connection with all Services to be delivered under this Master Agreement, including without limitation any successor service provider to whom a Purchasing Entity's Data is transferred in connection with the termination or expiration of this Master Agreement. The Contractor shall assist a Purchasing Entity in exporting and extracting a Purchasing Entity's Data, in a format usable without the use of the Services and as agreed by a Purchasing Entity, at no additional cost to the Purchasing Entity. Any transition services requested by a Purchasing Entity involving additional knowledge transfer and support may be subject to a separate transition Statement of Work.

b. A Purchasing Entity and the Contractor shall, when reasonable, create a Transition Plan Document identifying the transition services to be provided and including a Statement of Work if applicable.

c. The Contractor must maintain the confidentiality and security of a Purchasing Entity's Data during the transition services and thereafter as required by the Purchasing Entity.

33. Waiver of Breach: Failure of the Lead State, Participating Entity, or Purchasing Entity to declare a default or enforce any rights and remedies shall not operate as a waiver under this Master Agreement or Participating Addendum. Any waiver by the Lead State, Participating Entity, or Purchasing Entity must be in writing. Waiver by the Lead State or Participating Entity of any default, right or remedy under this Master Agreement or Participating Addendum, or by Purchasing Entity with respect to any Purchase Order, or breach of any terms or requirements of this Master Agreement, a Participating Addendum, or Purchase Order shall not be construed or operate as a waiver of any subsequent default or breach of such term or requirement, or of any other term or requirement under this Master Agreement, Participating Addendum, or Purchase Order.

34. Assignment of Antitrust Rights: Contractor irrevocably assigns to a Participating Entity who is a state any claim for relief or cause of action which the Contractor now has or which may accrue to the Contractor in the future by reason of any violation of state or federal antitrust laws (15 U.S.C. § 1-15 or a Participating Entity's state antitrust provisions), as now in effect and as may be amended from time to time, in connection

with any goods or services provided to the Contractor for the purpose of carrying out the Contractor's obligations under this Master Agreement or Participating Addendum, including, at a Participating Entity's option, the right to control any such litigation on such claim for relief or cause of action.

35. Debarment : The Contractor certifies, to the best of its knowledge, that neither it nor its principals are presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from participation in this transaction (contract) by any governmental department or agency. This certification represents a recurring certification made at the time any Order is placed under this Master Agreement. If the Contractor cannot certify this statement, attach a written explanation for review by the Lead State.

36. Performance and Payment Time Frames that Exceed Contract Duration: All maintenance or other agreements for services entered into during the duration of an SLA and whose performance and payment time frames extend beyond the duration of this Master Agreement shall remain in effect for performance and payment purposes (limited to the time frame and services established per each written agreement). No new leases, maintenance or other agreements for services may be executed after the Master Agreement has expired. For the purposes of this section, renewals of maintenance, subscriptions, SaaS subscriptions and agreements, and other service agreements, shall not be considered as "new."

37. Governing Law and Venue

a. The procurement, evaluation, and award of the Master Agreement shall be governed by and construed in accordance with the laws of the Lead State sponsoring and administering the procurement. The construction and effect of the Master Agreement after award shall be governed by the law of the state serving as Lead State (in most cases also the Lead State). The construction and effect of any Participating Addendum or Order against the Master Agreement shall be governed by and construed in accordance with the laws of the Participating Entity's or Purchasing Entity's State.

b. Unless otherwise specified in the RFP, the venue for any protest, claim, dispute or action relating to the procurement, evaluation, and award is in the Lead State. Venue for any claim, dispute or action concerning the terms of the Master Agreement shall be in the state serving as Lead State. Venue for any claim, dispute, or action concerning any Order placed against the Master Agreement or the effect of a Participating Addendum shall be in the Purchasing Entity's State.

c. If a claim is brought in a federal forum, then it must be brought and adjudicated solely and exclusively within the United States District Court for (in decreasing order of priority): the Lead State for claims relating to the procurement, evaluation, award, or contract performance or administration if the Lead State is a party; the Participating State if a named party; the Participating Entity state if a named party; or the Purchasing Entity state if a named party.

d. This section is also not a waiver by the Participating State of any form of immunity,

including but not limited to sovereign immunity and immunity based on the Eleventh Amendment to the Constitution of the United States.

38. No Guarantee of Service Volumes: The Contractor acknowledges and agrees that the Lead State and NASPO ValuePoint makes no representation, warranty or condition as to the nature, timing, quality, quantity or volume of business for the Services or any other products and services that the Contractor may realize from this Master Agreement, or the compensation that may be earned by the Contractor by offering the Services. The Contractor acknowledges and agrees that it has conducted its own due diligence prior to entering into this Master Agreement as to all the foregoing matters.

39. NASPO ValuePoint eMarket Center: In July 2011, NASPO ValuePoint entered into a multi-year agreement with JAGGAER, formerly SciQuest, whereby JAGGAER will provide certain electronic catalog hosting and management services to enable eligible NASPO ValuePoint's customers to access a central online website to view and/or shop the goods and services available from existing NASPO ValuePoint Cooperative Contracts. The central online website is referred to as the NASPO ValuePoint eMarket Center.

The Contractor will have visibility in the eMarket Center through Ordering Instructions. These Ordering Instructions are available at no cost to the Contractor and provided customers information regarding the Contractors website and ordering information.

At a minimum, the Contractor agrees to the following timeline: NASPO ValuePoint eMarket Center Site Admin shall provide a written request to the Contractor to begin Ordering Instruction process. The Contractor shall have thirty (30) days from receipt of written request to work with NASPO ValuePoint to provide any unique information and ordering instructions that the Contractor would like the customer to have.

40. Contract Provisions for Orders Utilizing Federal Funds: Pursuant to Appendix II to 2 Code of Federal Regulations (CFR) Part 200, Contract Provisions for Non-Federal Entity Contracts Under Federal Awards, Orders funded with federal funds may have additional contractual requirements or certifications that must be satisfied at the time the Order is placed or upon delivery. These federal requirements may be proposed by Participating Entities in Participating Addenda and Purchasing Entities for incorporation in Orders placed under this master agreement.

41. Government Support: No support, facility space, materials, special access, personnel or other obligations on behalf of the states or other Participating Entities, other than payment, are required under the Master Agreement.

42. NASPO ValuePoint Summary and Detailed Usage Reports: In addition to other reports that may be required by this solicitation, the Contractor shall provide the following NASPO ValuePoint reports.

a. Summary Sales Data. The Contractor shall submit quarterly sales reports directly to

NASPO ValuePoint using the NASPO ValuePoint Quarterly Sales/Administrative Fee Reporting Tool found at http://calculator.naspovaluepoint.org. Any/all sales made under the contract shall be reported as cumulative totals by state. Even if Contractor experiences zero sales during a calendar quarter, a report is still required. Reports shall be due no later than 30 day following the end of the calendar quarter (as specified in the reporting tool).

b. Detailed Sales Data. Contractor shall also report detailed sales data by: (1) state; (2) entity/customer type, e.g. local government, higher education, K12, non-profit; (3) Purchasing Entity name; (4) Purchasing Entity bill-to and ship-to locations; (4) Purchasing Entity and Contractor Purchase Order identifier/number(s); (5) Purchase Order Type (e.g. sales order, credit, return, upgrade, determined by industry practices); (6) Purchase Order date; (7) and line item description, including product number if used. The report shall be submitted in any form required by the solicitation. Reports are due on a quarterly basis and must be received by the Lead State and NASPO ValuePoint Cooperative Development Team no later than thirty (30) days after the end of the reporting period. Reports shall be delivered to the Lead State and to the NASPO ValuePoint Cooperative Development Team electronically through a designated portal, email, CD-Rom, flash drive or other method as determined by the Lead State and NASPO ValuePoint. Detailed sales data reports shall include sales information for all sales under Participating Addenda executed under this Master Agreement. The format for the detailed sales data report is in shown in Attachment H.

c. Reportable sales for the summary sales data report and detailed sales data report includes sales to employees for personal use where authorized by the solicitation and the Participating Addendum. Report data for employees should be limited to ONLY the state and entity they are participating under the authority of (state and agency, city, county, school district, etc.) and the amount of sales. No personal identification numbers, e.g. names, addresses, social security numbers or any other numerical identifier, may be submitted with any report.

d. Contractor shall provide the NASPO ValuePoint Cooperative Development Coordinator with an executive summary each quarter that includes, at a minimum, a list of states with an active Participating Addendum, states that Contractor is in negotiations with and any PA roll out or implementation activities and issues. NASPO ValuePoint Cooperative Development Coordinator and Contractor will determine the format and content of the executive summary. The executive summary is due 30 days after the conclusion of each calendar quarter.

e. Timely submission of these reports is a material requirement of the Master Agreement. The recipient of the reports shall have exclusive ownership of the media containing the reports. The Lead State and NASPO ValuePoint shall have a perpetual, irrevocable, non-exclusive, royalty free, transferable right to display, modify, copy, and otherwise use reports, data and information provided under this section.

f. If requested by a Participating Entity, the Contractor must provide detailed sales data

within the Participating State.

43. NASPO ValuePoint Cooperative Program Marketing, Training, and Performance Review:

a. Contractor agrees to work cooperatively with NASPO ValuePoint personnel. Contractor agrees to present plans to NASPO ValuePoint for the education of Contractor's contract administrator(s) and sales/marketing workforce regarding the Master Agreement contract, including the competitive nature of NASPO ValuePoint procurements, the Master agreement and participating addendum process, and the manner in which qualifying entities can participate in the Master Agreement.

b. Contractor agrees, as Participating Addendums become executed, if requested by ValuePoint personnel to provide plans to launch the program within the participating state. Plans will include time frames to launch the agreement and confirmation that the Contractor's website has been updated to properly reflect the contract offer as available in the participating state.

c. Contractor agrees, absent anything to the contrary outlined in a Participating Addendum, to consider customer proposed terms and conditions, as deemed important to the customer, for possible inclusion into the customer agreement. Contractor will ensure that their sales force is aware of this contracting option.

d. Contractor agrees to participate in an annual contract performance review at a location selected by the Lead State and NASPO ValuePoint, which may include a discussion of marketing action plans, target strategies, marketing materials, as well as Contractor reporting and timeliness of payment of administration fees.

e. Contractor acknowledges that the NASPO ValuePoint logos may not be used by Contractor in sales and marketing until a logo use agreement is executed with NASPO ValuePoint.

f. The Lead State expects to evaluate the utilization of the Master Agreement at the annual performance review. Lead State may, in its discretion, terminate the Master Agreement pursuant to section 6 when Contractor utilization does not warrant further administration of the Master Agreement. The Lead State may exercise its right to not renew the Master Agreement if vendor fails to record or report revenue for three consecutive quarters, upon 60-calendar day written notice to the Contractor. This subsection does not limit the discretionary right of either the Lead State or Contractor to terminate the Master Agreement pursuant to section 7.

g. Contractor agrees, within 30 days of their effective date, to notify the Lead State and NASPO ValuePoint of any contractual most-favored-customer provisions in third-part contracts or agreements that may affect the promotion of this Master Agreements or whose terms provide for adjustments to future rates or pricing based on rates, pricing in, or Orders from this master agreement. Upon request of the Lead State or NASPO

ValuePoint, Contractor shall provide a copy of any such provisions.

45. NASPO ValuePoint Cloud Offerings Search Tool: In support of the Cloud Offerings Search Tool here: http://www.naspovaluepoint.org/#/contract-details/71/search Contractor shall ensure its Cloud Offerings are accurately reported and updated to the Lead State in the format/template shown in Attachment I.

46. Entire Agreement: This Master Agreement, along with any attachment, contains the entire understanding of the parties hereto with respect to the Master Agreement unless a term is modified in a Participating Addendum with a Participating Entity. No click-through, or other end user terms and conditions or agreements required by the Contractor ("Additional Terms") provided with any Services hereunder shall be binding on Participating Entities or Purchasing Entities, even if use of such Services requires an affirmative "acceptance" of those Additional Terms before access is permitted.

Exhibit 1 to the Master Agreement: Software-as-a-Service

1. Data Ownership: The Purchasing Entity will own all right, title and interest in its data that is related to the Services provided by this Master Agreement. The Contractor shall not access Purchasing Entity user accounts or Purchasing Entity data, except (1) in the course of data center operations, (2) in response to service or technical issues, (3) as required by the express terms of this Master Agreement, Participating Addendum, SLA, and/or other contract documents, or (4) at the Purchasing Entity's written request.

Contractor shall not collect, access, or use user-specific Purchasing Entity Data except as strictly necessary to provide Service to the Purchasing Entity. No information regarding a Purchasing Entity's use of the Service may be disclosed, provided, rented or sold to any third party for any reason unless required by law or regulation or by an order of a court of competent jurisdiction. This obligation shall survive and extend beyond the term of this Master Agreement.

2. Data Protection: Protection of personal privacy and data shall be an integral part of the business activities of the Contractor to ensure there is no inappropriate or unauthorized use of Purchasing Entity information at any time. To this end, the Contractor shall safeguard the confidentiality, integrity and availability of Purchasing Entity information and comply with the following conditions:

a. The Contractor shall implement and maintain appropriate administrative, technical and organizational security measures to safeguard against unauthorized access, disclosure or theft of Personal Data and Non-Public Data. Such security measures shall be in accordance with recognized industry practice and not less stringent than the measures the Contractor applies to its own Personal Data and Non-Public Data of similar kind.

b. All data obtained by the Contractor in the performance of the Master Agreement shall become and remain the property of the Purchasing Entity.

c. All Personal Data shall be encrypted at rest and in transit with controlled access. Unless otherwise stipulated, the Contractor is responsible for encryption of the Personal Data. Any stipulation of responsibilities will identify specific roles and responsibilities and shall be included in the service level agreement (SLA), or otherwise made a part of the Master Agreement.

d. Unless otherwise stipulated, the Contractor shall encrypt all Non-Public Data at rest and in transit. The Purchasing Entity shall identify data it deems as Non-Public Data to the Contractor. The level of protection and encryption for all Non-Public Data shall be identified in the SLA.

e. At no time shall any data or processes — that either belong to or are intended for the use of a Purchasing Entity or its officers, agents or employees — be copied, disclosed or retained by the Contractor or any party related to the Contractor for subsequent use in any transaction that does not include the Purchasing Entity.

f. The Contractor shall not use any information collected in connection with the Services issued from this Master Agreement for any purpose other than fulfilling the Services.

3. Data Location: The Contractor shall provide its services to the Purchasing Entity and its end users solely from data centers in the U.S. Storage of Purchasing Entity data at rest shall be located solely in data centers in the U.S. The Contractor shall not allow its personnel or contractors to store Purchasing Entity data on portable devices, including personal computers, except for devices that are used and kept only at its U.S. data centers. The Contractor shall permit its personnel and contractors to access Purchasing Entity data remotely only as required to provide technical support. The Contractor may provide technical user support on a 24/7 basis using a Follow the Sun model, unless otherwise prohibited in a Participating Addendum.

4. Security Incident or Data Breach Notification:

a. Incident Response: Contractor may need to communicate with outside parties regarding a security incident, which may include contacting law enforcement, fielding media inquiries and seeking external expertise as mutually agreed upon, defined by law or contained in the contract. Discussing security incidents with the Purchasing Entity should be handled on an urgent as-needed basis, as part of Contractor's communication and mitigation processes as mutually agreed upon, defined by law or contained in the Master Agreement.

b. Security Incident Reporting Requirements: The Contractor shall report a security incident to the Purchasing Entity identified contact immediately as soon as possible or promptly without out reasonable delay, or as defined in the SLA.

c. Breach Reporting Requirements: If the Contractor has actual knowledge of a confirmed data breach that affects the security of any purchasing entity's content that is subject to applicable data breach notification law, the Contractor shall (1) as soon as possible or promptly without out reasonable delay notify the Purchasing Entity, unless shorter time is required by applicable law, and (2) take commercially reasonable measures to address the data breach in a timely manner.

5. Personal Data Breach Responsibilities: This section only applies when a Data Breach occurs with respect to Personal Data within the possession or control of the Contractor.

a. The Contractor, unless stipulated otherwise, shall immediately notify the appropriate Purchasing Entity identified contact by telephone in accordance with the agreed upon security plan or security procedures if it reasonably believes there has been a security incident.

b. The Contractor, unless stipulated otherwise, shall promptly notify the appropriate Purchasing Entity identified contact within 24 hours or sooner by telephone, unless shorter time is required by applicable law, if it has confirmed that there is, or reasonably believes that there has been a Data Breach. The Contractor shall (1) cooperate with the Purchasing Entity as reasonably requested by the Purchasing Entity to investigate and resolve the Data Breach, (2) promptly implement necessary remedial measures, if necessary, and (3) document responsive actions taken related to the Data Breach, including any post-incident review of events and actions taken to make changes in business practices in providing the services, if necessary.

c. Unless otherwise stipulated, if a data breach is a direct result of Contractor's breach of its contractual obligation to encrypt personal data or otherwise prevent its release as reasonably determined by the Purchasing Entity, the Contractor shall bear the costs associated with (1) the investigation and resolution of the data breach; (2) notifications to individuals, regulators or others required by federal and state laws or as otherwise agreed to; (3) a credit monitoring service required by state (or federal) law or as otherwise agreed to; (4) a website or a toll-free number and call center for affected individuals required by federal and state laws — all not to exceed the average per record per person cost calculated for data breaches in the United States (currently $217 per record/person) in the most recent Cost of Data Breach Study: Global Analysis published by the Ponemon Institute at the time of the data breach; and (5) complete all corrective actions as reasonably determined by Contractor based on root cause.

6. Notification of Legal Requests: The Contractor shall contact the Purchasing Entity upon receipt of any electronic discovery, litigation holds, discovery searches and expert testimonies related to the Purchasing Entity's data under the Master Agreement, or which in any way might reasonably require access to the data of the Purchasing Entity. The Contractor shall not respond to subpoenas, service of process and other legal requests related to the Purchasing Entity without first notifying and obtaining the approval of the Purchasing Entity, unless prohibited by law from providing such notice.

7. Termination and Suspension of Service:

a. In the event of a termination of the Master Agreement or applicable Participating Addendum, the Contractor shall implement an orderly return of purchasing entity's data in a CSV or another mutually agreeable format at a time agreed to by the parties or allow the Purchasing Entity to extract it's data and the subsequent secure disposal of purchasing entity's data.

b. During any period of service suspension, the Contractor shall not take any action to intentionally erase or otherwise dispose of any of the Purchasing Entity's data.

c. In the event of termination of any services or agreement in entirety, the Contractor shall not take any action to intentionally erase purchasing entity's data for a period of:

- 10 days after the effective date of termination, if the termination is in accordance with the contract period
- 30 days after the effective date of termination, if the termination is for convenience
- 60 days after the effective date of termination, if the termination is for cause

After such period, the Contractor shall have no obligation to maintain or provide any purchasing entity's data and shall thereafter, unless legally prohibited, delete all purchasing entity's data in its systems or otherwise in its possession or under its control.

d. The purchasing entity shall be entitled to any post termination assistance generally made available with respect to the services, unless a unique data retrieval arrangement has been established as part of an SLA.

e. Upon termination of the Services or the Agreement in its entirety, Contractor shall securely dispose of all Purchasing Entity's data in all of its forms, such as disk, CD/ DVD, backup tape and paper, unless stipulated otherwise by the Purchasing Entity. Data shall be permanently deleted and shall not be recoverable, according to National Institute of Standards and Technology (NIST)-approved methods. Certificates of destruction shall be provided to the Purchasing Entity.

8. Background Checks: Upon the request of the Purchasing Entity, the Contractor shall conduct criminal background checks and not utilize any staff, including subcontractors, to fulfill the obligations of the Master Agreement who have been convicted of any crime of dishonesty, including but not limited to criminal fraud, or otherwise convicted of any felony or misdemeanor offense for which incarceration for up to 1 year is an authorized penalty. The Contractor shall promote and maintain an awareness of the importance of securing the Purchasing Entity's information among the Contractor's employees and agents. If any of the stated personnel providing services under a Participating Addendum is not acceptable to the Purchasing Entity in its sole opinion as a result of the background or criminal history investigation, the Purchasing Entity, in its' sole option shall have the right to either (1) request immediate replacement of the person, or (2) immediately terminate the Participating Addendum and any related service agreement.

9. Access to Security Logs and Reports: The Contractor shall provide reports on a schedule specified in the SLA to the Purchasing Entity in a format as specified in the SLA agreed to by both the Contractor and the Purchasing Entity. Reports shall include latency statistics, user access, user access IP address, user access history and security logs for all public jurisdiction files related to this Master Agreement and applicable Participating Addendum.

10. Contract Audit: The Contractor shall allow the Purchasing Entity to audit conformance to the Master Agreement terms. The Purchasing Entity may perform this audit or contract with a third party at its discretion and at the Purchasing Entity's expense.

11. Data Center Audit: The Contractor shall perform an independent audit of its data centers at least annually at its expense, and provide an unredacted version of the audit report upon request to a Purchasing Entity. The Contractor may remove its proprietary information from the unredacted version. A Service Organization Control (SOC) 2 audit report or approved equivalent sets the minimum level of a third-party audit.

12. Change Control and Advance Notice: The Contractor shall give a minimum forty eight (48) hour advance notice (or as determined by a Purchasing Entity and included in the SLA) to the Purchasing Entity of any upgrades (e.g., major upgrades, minor upgrades, system changes) that may impact service availability and performance. A major upgrade is a replacement of hardware, software or firmware with a newer or better version in order to bring the system up to date or to improve its characteristics. It usually includes a new version number.

Contractor will make updates and upgrades available to Purchasing Entity at no additional costs when Contractor makes such updates and upgrades generally available to its users.

No update, upgrade or other charge to the Service may decrease the Service's functionality, adversely affect Purchasing Entity's use of or access to the Service, or increase the cost of the Service to the Purchasing Entity.

Contractor will notify the Purchasing Entity at least sixty (60) days in advance prior to any major update or upgrade.

13. Security: As requested by a Purchasing Entity, the Contractor shall disclose its non-proprietary system security plans (SSP) or security processes and technical limitations to the Purchasing Entity such that adequate protection and flexibility can be attained between the Purchasing Entity and the Contractor. For example: virus checking and port sniffing — the Purchasing Entity and the Contractor shall understand each other's roles and responsibilities.

14. Non-disclosure and Separation of Duties: The Contractor shall enforce separation of job duties, require commercially reasonable non-disclosure agreements, and limit staff knowledge of Purchasing Entity data to that which is absolutely necessary to perform job duties.

15. Import and Export of Data: The Purchasing Entity shall have the ability to import or export data in piecemeal or in entirety at its discretion without interference from the Contractor at any time during the term of Contractor's contract with the Purchasing Entity. This includes the ability for the Purchasing Entity to import or export data to/from other Contractors. Contractor shall specify if Purchasing Entity is required to provide its' own tools for this purpose, including the optional purchase of Contractors tools if Contractors applications are not able to provide this functionality directly.

16. Responsibilities and Uptime Guarantee: The Contractor shall be responsible for the acquisition and operation of all hardware, software and network support related to the services being provided. The technical and professional activities required for establishing, managing and maintaining the environments are the responsibilities of the Contractor. The system shall be available 24/7/365 (with agreed-upon maintenance downtime), and provide service to customers as defined in the SLA.

17. Subcontractor Disclosure: Contractor shall identify all of its strategic business partners related to services provided under this Master Agreement, including but not limited to all subcontractors or other entities or individuals who may be a party to a joint venture or similar agreement with the Contractor, and who shall be involved in any application development and/or operations.

18. Right to Remove Individuals: The Purchasing Entity shall have the right at any time to require that the Contractor remove from interaction with Purchasing Entity any Contractor representative who the Purchasing Entity believes is detrimental to its working relationship with the Contractor. The Purchasing Entity shall provide the Contractor with notice of its determination, and the reasons it requests the removal. If the Purchasing Entity signifies that a potential security violation exists with respect to the request, the Contractor shall immediately remove such individual. The Contractor shall not assign the

person to any aspect of the Master Agreement or future work orders without the Purchasing Entity's consent.

19. Business Continuity and Disaster Recovery: The Contractor shall provide a business continuity and disaster recovery plan upon request and ensure that the Purchasing Entity's recovery time objective (RTO) of XXX hours/days is met. (XXX hour/days shall be provided to Contractor by the Purchasing Entity.) Contractor must work with the Purchasing Entity to perform an annual Disaster Recovery test and take action to correct any issues detected during the test in a time frame mutually agreed between the Contractor and the Purchasing Entity.

20. Compliance with Accessibility Standards: The Contractor shall comply with and adhere to Accessibility Standards of Section 508 Amendment to the Rehabilitation Act of 1973, or any other state laws or administrative regulations identified by the Participating Entity.

21. Web Services: The Contractor shall use Web services exclusively to interface with the Purchasing Entity's data in near real time.

22. Encryption of Data at Rest: The Contractor shall ensure hard drive encryption consistent with validated cryptography standards as referenced in FIPS 140-2, Security Requirements for Cryptographic Modules for all Personal Data, unless the Purchasing Entity approves in writing for the storage of Personal Data on a Contractor portable device in order to accomplish work as defined in the statement of work.

23. Subscription Terms: Contractor grants to a Purchasing Entity a license to: (i) access and use the Service for its business purposes; (ii) for SaaS, use underlying software as embodied or used in the Service; and (iii) view, copy, upload and download (where applicable), and use Contractor's documentation.

No Contractor terms, including standard click through license or website terms or use of privacy policy, shall apply to Purchasing Entities unless such terms are included in this Master Agreement.

Attachment B – Scope of Services Awarded to Contractor

1.1 Awarded Service Model(s).

Contractor is awarded the following Service Model:

- Software as a Service (SaaS)

1.2 Risk Categorization.*

Contractor's offered solutions offer the ability to store and secure data under the following risk categories:

Service Model	Low Risk Data	Moderate Risk Data	High Risk Data	Deployment Models Offered
SaaS	X Enformion Web, Batch Data Exchange, API Data Integration			Public Cloud Hybrid Cloud

*Contractor may add additional OEM solutions during the life of the contract.

2.1 Deployment Models.

Contractor may provide cloud based services through the following deployment methods:

- **Private cloud.** The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.
- **Community cloud.** The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.
- **Public cloud.** The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.
- **Hybrid cloud.** The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds)

Attachment C - Pricing Discounts and Schedule

Contractor Confi-Chek, Inc.

Pricing Notes

1. % discounts are based on minimum discounts off Contractor's commercially published pricelists versus fixed pricing. Nonetheless, Orders will be fixed-price or fixed-rate and not cost reimbursable contracts. Contractor has the ability to update and refresh its respective price catalog, as long as the agreed-upon discounts are fixed.

2. Minimum guaranteed contract discounts do not preclude an Offeror and/or its authorized resellers from providing deeper or additional, incremental discounts at their sole discretion.

3. Purchasing entities shall benefit from any promotional pricing offered by Contractor to similar customers. Promotional pricing shall not be cause for a permanent price change.

4. Contractor's price catalog include the price structures of the cloud service models, value added services (i.e., Maintenance Services, Professional Services, Etc.), and deployment models that it intends to provide including the types of data it is able to hold under each model. Pricing shall all-inclusive of infrastructure and software costs and management of infrastructure, network, OS, and software.

5. Contractor provides tiered pricing to accompany its named user licensing model, therefore, as user count reaches tier thresholds, unit price decreases.

Cloud Service Model: Software as a Service (SaaS)

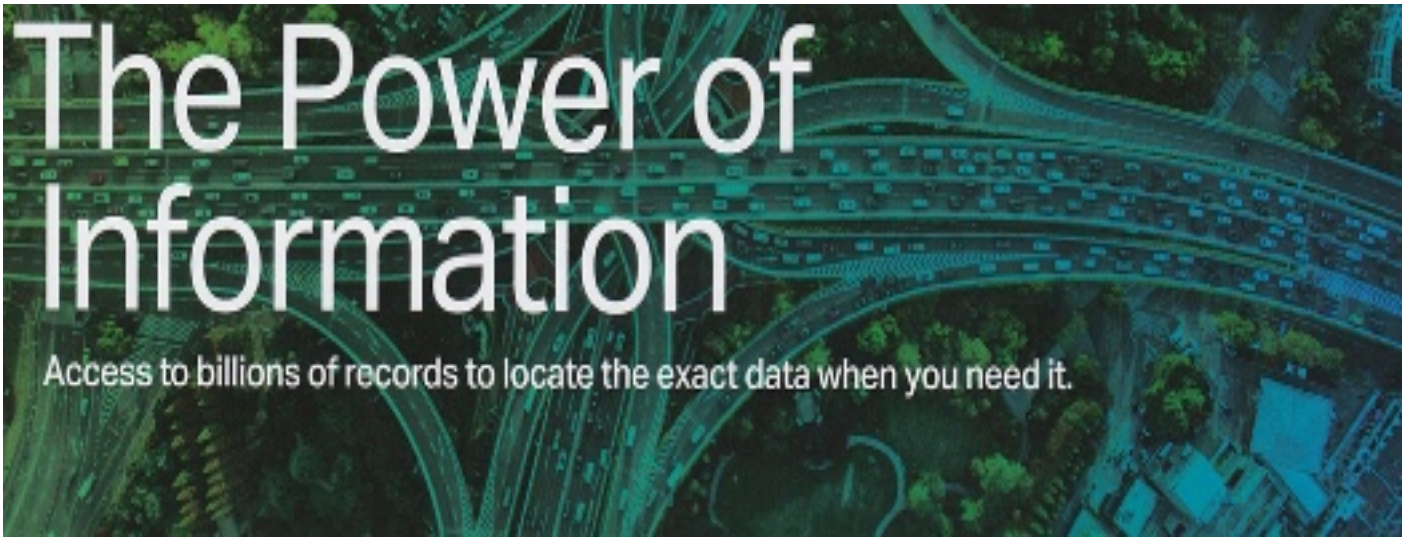
Description	Discount
OEM: Confi-Chek-Enformion Web Core Data Services, Pay Per Use	30.00%
OEM: Confi-Chek-Enformion Unlimited Core Data Subscription	25.00%
OEM: Confi-Chek-Enformion Pay-Per-Use Discount Subscription	30.00%
OEM: Confi-Chek-Premium Data Services	10.00%
OEM: Confi-Chek-Data Batch Services	30.00%
OEM: Confi-Chek-Data Bach Services w/ 100 Seat Enformion Web	100.00%
OEM: Confi-Chek-API Web Services Data Integration	25.00%
Average SaaS OEM Discount Off	**35.71%**

Additional Value Added Services

		Onsite Hourly Rate		Remote Hourly Rate	
Item Description		**NVP Price**	**Catalog Price**	**NVP Price**	**Catalog Price**
Maintenance Services		-	-	-	-
Professional Services					
	Deployment Services	-	-	-	-
	Integration Services	$ 135.00	$ 175.00	$ 125.00	$ 155.00
	Consulting/Advisory Services	$ 135.00	$ 175.00	$ 125.00	$ 155.00
	Architectural Design Services				
	Statement of Work Services				
Partner Services					
Training Deployment Services		$ 135.00	$ 175.00	$ 95.00	$ 135.00

	Deliverable Rates	
	NVP Price	Catalog Price
N/A	N/A	N/A

Confi-Chek
Cloud Solutions



TECHNICAL RESPONSE

Corporate Information:

Confi-Chek Inc.

1821 Q Street, Sacramento, CA 95811

EIN 94-3359257 | DUNS 859038655 | CAGE Code 4DBU1

Primary NAICS 514191 On-Line Information Services

Secondary NAICS 518000 Data Processing, Hosting, Related Services

Point of Contact:

Scott Johnson

Director of Government Services

1821 Q Street, Sacramento, CA 95811

Scott.Johnson@Enformion.com | (916) 250-2300 Desk

TECHNICAL REQUIREMENTS

Offer Overview

Confi-Chek was incorporated in 2000 and has been providing public records and commercial personal data as a service nearly 20 years. The Enformion online platform began production in 2010 and is focused on providing data solutions to commercial and government customers.

The Enformion online platform integrates more than 6,000 data sources. Our powerful algorithms connect billions of records to build comprehensive profiles about individuals. We make this data available through a web software application, a published Application Program Interface (API), and a traditional batch data file exchange service for integration with the customer's third-party applications.

To guard our data records, inclusive of more than 98% of the US adult population, Confi-Chek employs sound information and cyber security practices, including next generation firewall systems, minimum access network provisioning for employees, and multi-factor authentication to internal corporate systems and resources. We comply with the PCI DSS security policies and practices standards and undergo annual audits.

NIST Essential Characteristics (RFP 8.1)

The Enformion online platform is NIST 800-145 compliant and was recently selected for approval by the General Services Administration's cloud software evaluation panel using the NIST 800-145 criteria.

On-Demand Self-Service

The Enformion online platform is available 24 hours per day, 7 days per week, 365 days per year. Once a subscription account has been ordered and provisioned, the subscriber need only log into the website and begin their records search and analysis using common web browsers. The customer's account administrator can provision login IDs to their employees independently of Confi-Chek services and support.

Broad Network Access

The Enformion online platform is accessible with desktop web browsers and mobile devices.

Resource Pooling

The Enformion online platform predominantly operates on shared infrastructure and hardware. To meet security expectations, some government customers will be provisioned on pooled systems with exclusive access to isolated database systems for specialized data requirements.

Rapid Elasticity

Confi-Chek supports thousands of concurrent users at any given time and scales rapidly for new system demand. We constantly monitor our enterprise systems' performance and add computing resources to stay ahead of growing customer demand.

Measured Service

The Enformion online platform is offered to the commercial market under several pricing models, ranging from a lower monthly subscription cost with metered-charges for data access, to an unlimited subscription for access to standard commercial and public records data for a flat monthly fee.

Confi-Chek complies with the provisions and requirements of the RFP's attachments C&D.

As a provider of data, we interpret the Categorization of Risk to be Low to Moderate. Confi-Chek already possesses and utilizes our data assets.

Scope of Services

Confi-Chek offers our data products under a Software as a Service (SaaS) model. The Enformion online platform is a 100% web-delivered service and requires no local installation of software.

Categorization of Risk

The Enformion query logs are created for audit and billing purposes for each customer account and could be considered sensitive in some contexts. Customers using our data for financial purposes, such as locating a delinquent debtor can be considered as a low risk. Law enforcement investigative queries could be interpreted as a moderate risk, the information regarding "who" is being investigated could have a higher level of sensitivity.

Subcontractors (RFP 8.2)

The Company's internal full-time staff delivers and supports our products and services.

We may occasionally leverage our certified partner network for geographic or customer specialization reasons to reduce travel, training, sales and administrative costs.

Working with Purchasing Entities (RFP 8.3)

In the event of a data breach, Confi-Chek will be aware of the incident before any of our customers. Impact to customers will be minimal, since we do not receive, store, or utilize data derived from our customers.

First, Confi-Chek will contact each of our customers and notify them of the incident and status. An appraisal of what was taken, when, and what our estimation of the impact is will be conveyed. Confi-Chek's Information Technology support team will execute our pre-planned response procedures and begin recovery operations.

Second, customers with potential impact from the content of our database query logs will be contacted, informed of the content, and Confi-Chek will coordinate our response as appropriate to the customer's purpose of use.

Third, Confi-Chek will engage our cyber insurance liability carrier to convey details of the event, the estimated impact, and begin the documentation process.

Advertisements

Confi-Chek does not permit the publication of advertisements, adware, bloatware, or any type of tracking software on our business-to-business and business-to-government platforms.

Development and Quality Assurance

The Enformion online platform is a platform that is actively under continuous enhancement and revision release.

To meet the changing needs of our customers and to remain competitive in the marketplace, Confi-Chek is constantly developing new features at the request of our customers.

New development is managed with an agile project management framework model with incremental feature development and defect resolution releases. These releases take place on approximately a bi-weekly schedule, with high-priority items sometimes released more frequently or interim between normal scheduled releases.

Code development is planned by product leadership, designed and developed by our software engineering team, peer-reviewed by other developers, tested by our quality assurance team, and released to production when certified.

Section 508 Compliance

The online platform is developed using industry framework tools that ensure compatibility with operating system and third-party provided accessibility aids that make it suitable for use by people with disabilities in accordance with requirements published by the US General Services Administration.

Browser Compatibility

The online platform is usable by all current versions of common browsers on desktop computers, tablets, and mobile devices.

Some older browsers and mobile devices may not support all of the features of our portal product but remain functional and usable.

Compliance Obligations

Confi-Chek has a well-defined and documented security briefing, compliance agreement, and data licensure that is communicated to our customer prior to the provisioning of services. The customer's designated security representative is required to review and agree to our security terms and conditions, and sub-agreements are provided for acknowledgment to each of our customer's end users.

To prepare our customer for these requirements, we meet with their procurement and technical representatives, and provide training to their staff.

Project Work Plans

Provisioning of the Confi-Chek services is remarkably streamlined. Confi-Chek staff can create user accounts in bulk or designated administrators within the customer's account can create and manage their own end user login profiles. Once provisioned, the end user receives an email to complete their account activation process and configure their password.

Our previous performance demonstrates we can scale out 120 new profiles for a customer within 48 hours of the receipt of the customer's purchase order or contract award. Internal customer organizational change management will typically require more planning and execution time than Confi-Chek's technical requirements.

Confi-Chek's on-boarding for our batch processing services varies by the complexity of the customer's input and output files. For planning purposes, we assume a two-week window for requirements definition, development, testing, and production-release.

Continuous Enhancement and Improvement

Enformion is a continuously developed product. Confi-Chek ensures that we remain at the forefront of data relevancy, interface usability, and system performance. Our customer feedback, particularly from customers that previously subscribed to a competitor's product, often remarks that we have the best usability in the marketplace.

Our development queue is defined in two ways. Primarily, our customers provide ideas and suggestions for improvements that are often added to our development tasks. Second, Confi-Chek leadership defines new functionality, improvements, and security policy to remain competitive in the marketplace.

These developments, quality assurance, and production release activities are continuous and on-going with regular incremental release schedules. Customers rarely notice the subtle differences between versions, often represented only by a new feature on a menu of reports or some performance improvements. Most of the development focus is in the area of data enhancement - which is visible through continuously improving search returns.

Software releases that will be noticeable to the customer are accompanied by a release notes and version commentary emailed to our customers prior.

Customer Service (RFP 8.4)

Confi-Chek evaluates our existing product and newly developed features under our quality assurance program with a dedicated team of software quality assurance professionals.

Defects and requests for new functionality are normally communicated from the customer to their account manager, or through a call to our customer support team. Our normal support team business hours are 8 am to 5 pm Monday-Friday, with expanded customer support coverage to 24x7 for emergency incidents involving enterprise customers.

All requests for service are responded to within one business day.

Normal design and installation service requirements for our services are limited in need and scope to our data batch processing on-boarding services. Confi-Chek provides design, development and implementation of customized data exchange interfaces for Confi-Chek each customer at no cost for Confi-Chek infrastructure. We also provide consultation and advisement to our customer for use of this exported data in their internal or third-party software applications.

Security of Information (RFP 8.5)

Confi-Chek's data assets, the products and services we sell to customers, are continuously aggregated and retained indefinitely. Our breadth and depth of information is the basis of our insight and value proposition to our customers.

The data collected from our customers is in the form of their database query, search, and reporting logs and is the basis of our account billing process for consumption-based subscription agreements. We normally retain these for archival purposes and to support the resolution of billing questions or customer account audits.

Confi-Chek development support may access the customer account search logs during the investigation of a technical service request or to reproduce the circumstances leading to a customer-reported defect.

These logs can be purged by request or by customer policy after receipt of payment for the applicable billing cycle.

Confi-Chek destroys any data storage devices removed from production use prior to disposal in accordance with FIPS 140-2.

Privacy and Security (RFP 8.6)

The online platform complies with the NIST 800-145 definition of cloud computing as described by the Software as a Service product and service description and is deployed under the Hybrid data center computing model.

Confi-Chek is required by industry to comply with PCI Data Security Standards (PCI DSS) and is audited for this compliance on a recurring basis.

Confi-Chek does not acquire data from our customers, and as such we do not have other specific requirements. As an operational practice, our internal policies and procedures comply with PCI DSS v3.0, SOC2, HIPAA, NIST-800-53, FIPS 140-2, and FIPS 200.

Should customer requirements in the future dictate, Confi-Chek's combination of multi-layer firewall security, multi-factor authentication, encryption at-rest and in-transit, minimum-access security model, and physical facility security policies can be readily adapted to meet other governmental security standards.

The data is subscribed to by usage, such as per-query and per-report, or unlimited subscription bases. The visibility of this cloud hosted data is strictly controlled by the content of the subscription. The accounting and search logging are viewable by the account's designated security representative for auditing purpose internal to the customer, but not searchable or visible by normal user access within the account, or users outside of the account.

In accordance with PCI DSS, Confi-Chek maintains a data breach notification procedure. We do not accumulate customer-derived data, minimizing the potential impact to any Confi-Chek customer. Our search and accounting logs are potentially sensitive, for example, if used as a list of potential suspects under investigation by law enforcement. Our notification procedures include special handling of these accounts.

Confi-Chek does not host customer equipment, servers, or other data equipment and does not accumulate customer-derived data. We do not have a need for physical or virtual zones of control or reference architectures.

Confi-Chek internal employees are provisioned for access to physical equipment, data assets, and account information using a minimum-access security model, granted only the access needed for their role.

In the event of an account data security breach of account search logging or account payment information, Confi-Chek will immediately notify customers and bank card issuers. These notifications will be within 48 hours of the discovery of the breach, allowing sufficient time to fully investigate and understand the nature of the incident.

We do not provide details of our security architecture on documents that reside within the public record.

Migration and Redeployment Plan (RFP 8.7)

Confi-Chek's services continuously undergo enhancement developments to remain relevant and competitive in the marketplace while expanding value to our subscribers. Over time some of our older services may reach the end of their life when subscriber interest has diminished and replaced by other technologies.

In the event of such an end of life deprecation, Confi-Chek would retain support for the affected features or services through the end of the subscriber's contract, with notification of the discontinuance with all account subscribers, at least one year prior.

Data content can be more unpredictable. Confi-Chek acquires some specialized data assets through licensing agreements with our peers. It is conceivable that changes to these licensing agreements can occur over time and can affect subscribers. In the event that a specific data asset is being purchased by a customer and is no longer available under this type of circumstance, Confi-Chek will notify the affected customers immediately upon determination and will release the affected customers from any term-based subscription agreements.

Confi-Chek does not acquire data from customers and return of data is not applicable to our product.

Service or Data Recovery (RFP 8.8)

Confi-Chek utilizes several separate geographic sites within the continental United States to guarantee service availability. We do not acquire customer-derived data, and customer-oriented backup and recovery services are not applicable.

Our next generation Hadoop database cluster technology is both extremely fast and highly resilient. In the unlikely event of an outage, our on-site equipment sparing would be used to rapidly recover our services from flash-array backups. Tape-based media is too slow for our requirements, while being generally unreliable.

Confi-Chek production sites have redundant power sources, redundant Internet connections, and on-site diesel power generation with fuel contracts.

Confi-Chek does not use off-shore datacenter locations.

Data Protection (RFP 8.9)

All disk-based storage is encrypted at-rest using SAN array storage encryption. Data is encrypted in-transit within our local area network, and between our sites and our customers using public key infrastructure (PKI) encryption.

Confi-Chek is willing to review and sign customer agreements on a case-by-case basis.

Confi-Chek does not accumulate customer-derived data, negating the question of customer data mining.

Service Level Agreements (RFP 8.10)

Service Level Agreements (SLAs) are not common for the type of SaaS product offered by Confi-Chek. We focus on accuracy of our data assets and the continuous aggregation of data from over 6000 sources. Search queries are normally completed with sub-3 second performance.

Our customers emphasize data breadth and accuracy over incrementally faster database query performance. Many data products, such as vehicle registrations, are called from the government source “on-demand” in real time when one of our customers makes the inquiry. These upstream connections to networks and systems outside of our control make performance SLA’s impractical to guarantee or enforce.

Confi-Chek is willing to negotiate a customer-specific SLA in the context of their specific data requirements, reporting, and performance requirements.

Data Disposal (RFP 8.11)

Confi-Chek’s data assets are our service. We do not destroy our data assets.

Upon request, Confi-Chek will purge customer accounting logs.

Data storage devices are destroyed when removed from service.

Performance Measures and Reporting (RFP 8.12)

Confi-Chek’s availability is greater than 99.5%. We have environmental influences that can temporarily degrade our service, some within our control and some outside of it.

In the event support is needed by a participating entity, Confi-Chek’s toll-free support number, web-based support requests, email, and direct phone numbers to the account management team are provided.

Confi-Chek updates the production platform on a bi-weekly basis, or more frequently. The design of our architecture enables these updates in real time without incurring system downtime. Some temporary performance degradation may be observed in some cases.

The performance capability of the online platform is designed to handle hundreds of thousands of users. The incremental addition of 10, 50, or 100 new users for a typical customer account is not sufficiently impactful to require any type of scale-up or scale-down of hardware.

Cloud Security Alliance (RFP 8.13)

Confi-Chek is not a member of the Cloud Security Alliance. We have completed and provided the NASPO Cloud Solutions self-assessment.

Service Provisioning (RFP 8.14)

Confi-Chek provisions a customer account no later than the next business day after receipt of a customer's purchase order and data services agreement. Individual logins within the account can be provisioned in bulk by Confi-Chek with identity information provided by the customer, or the logins can be provisioned by the customer's account administrator.

Batch processing of data files will normally require a two-week period for interface design, development, implementation, testing, and certification for the customer.

Confi-Chek's sales cycle and sales practices are intended to avoid the need for emergency or rush services. For example, we normally provide pilot project or system access for testing purposes in parallel with the customer's existing provider contract. If a decision to subscribe to our services is communicated, we will provision production-level access in parallel to the customer's procurement process and enable full-deployment on day-one after receipt of the purchase order. In the unusual circumstance that emergency provisioning services are required, these would be accomplished with the intervention of the customer's account management team to assist with rapid account login provisioning.

Back Up and Disaster Plan (RFP 8.15)

Confi-Chek does not acquire customer-derived data and does not encounter a specific need for customer data backup or recovery. We do retain and archive query search logs for billing and quality control purposes. These search logs can be purged on an interval specified by the customer or retained indefinitely to meet any specific legal retention period.

We do not host or execute applications on behalf of any customer.

Confi-Chek's databases are mirrored between redundant sites and can operate independently of each other.

Hosting and Provisioning (RFP 8.16)

Confi-Chek does not host servers, virtual machines, or applications for any customers, nor do we provision customer-accessible storage.

The Enformion online platform search and query logs are accessible by the customer's administrator using our reporting tools to monitor their consumption, billing activity, and individual user activity.

Trial and Testing Periods, Pre and Post-Purchase (RFP 8.17)

Confi-Chek provides 30-day test account access to prospective customers upon request and following agreement with our data use terms and conditions. If the prospective customer issues a letter-of-intent or similar purchase commitment within the 30-day trial period, Confi-Chek will extend the test-period through the customer's procurement process.

Confi-Chek provides webinar-based and on-site training options to customers, commensurate with the size of the subscription purchase and customizable training document templates for our customers' internal use and distribution.

Integration and Customization (RFP 8.18)

Confi-Chek provides a published standards-based web services application program interface (API) for simple integration of our data assets with third-party applications. We also make our data available using traditional SFTP file data exchange for use with legacy or non-API-enabled applications.

The Enformion online platform can be customized for large enterprise customers, integrating the customer's color schemes, logos, and some navigational customizations without sacrificing performance. This flexibility of the product's theme enables a level of customization to appear as though the application suite has been custom-developed by the customer.

Marketing Plan (RFP 8.19)

Confi-Chek markets proactively to our prospective government agency customers by contacting those that currently subscribe to our competitors. We also combine our solution and data assets with integration companies to enable their applications with our data assets and capabilities.

Confi-Chek responds directly to all suitable requests for information and requests for proposal that are a requirement match to our solution capabilities.

Confi-Chek has already many government agency subscribers through our direct-marketing efforts across state, local, and federal markets.

Related Value-Added Services to Cloud Solutions (RFP 8.20)

Confi-Chek provides our standardized integration and training services for our core products at no cost to the customer.

Supporting Infrastructure (RFP 8.22)

Confi-Chek subscribers require only a modern web browser for full access to and use of our data resources.

Confi-Chek
Cloud Solutions

DETAILED PRODUCT OFFERING

Platform Summary

Confi-Chek, Inc. collects, aggregates, models, and markets public, proprietary, commercial, and historical data on topics relevant to business and personal information. We offer our information services products under a Software as a Service (SaaS) business model, providing access to our information resources.

Our databases aggregate 6,000+ individual data sources and encompass approximately 98% of the adult population of the United States, and virtually all businesses, corporations, and corporate relationships.

TECHNOLOGY

We market our platform as a SaaS solution, presented as a web portal application suitable for interactive data discovery, data mining, and report generation.

Web Application Portal

Our Enformion Investigative web portal (Enformion online platform) subscription is offered via three pricing models.

This Software as a Service application delivers operational efficiency, information security, and best-in-breed data breadth in a feature rich platform that easily enables our customer to locate people, assets, businesses, relatives, licenses and comprehensive background information of adults in the United States.

The subscription offer also includes a Business Data Discovery service, with data sets inclusive of all US corporations and their affiliates, subsidiaries, and company officer

information. Further, company officers can be investigated as to their personal information, known associates, contact, and address information.

The data content for each subscription pricing model is identical, we offer the different options to meet different anticipated usage volumes, customer needs, and budget.

CAPABILITIES AND DESCRIPTIONS

Web Application Subscription Features- Public and Commercial Data Sets

Core data resources within the platform is marketed on a per-hit pay-per-use basis, a discounted subscription with a monthly budget for queries included, or within a flat monthly or annual unlimited use subscription agreement.

Some products access external resources and incur a per-use cost, regardless of subscription agreement level and normally incur a separate regulatory compliance requirement.

Core Service	Detailed Description
SSN Verification	Draws a report history of all individuals to have used a provided Social Security Number.
Premium People Search	Current and Historical Addresses, Emails, Phones, SSN.
Comprehensive Report	Person Addresses, AKA's, Aircraft, Arrests, Assessor, Bankruptcies, Birth, Criminal, DBA/FBN, DEA licenses, Death, Deeds, Divorce, Email Addresses, Evictions, Foreclosures, Hunting/Fishing Licenses, Judgements, Liens, Marriage, Neighbors, Phones, Pilot License, Professional Licenses, Relatives/Associates, Sex Offender Registry, Traffic, US Corporations, Vessels, Wants & Warrants

Vehicle (Aircraft, Auto, Vessel) Report	Returns registered aircraft / vehicles / vessels, searchable by owner, address of registration record, SSN, or registry tag number with variances by individual state regulation.
US Corporations	Registration, filing status and related identifier and contact criteria for every corporation in the United States.
Criminal Record Search	Arrests, Criminal Convictions, Sex Offender Registry, and Wants & Warrants Returned
Arrest Record	Nationwide Records of law enforcement Arrests (Federal, State, Local)
National Sex Offenders	Returns all sex offender registry information
National Liens / Foreclosures / Judgements / Bankruptcy	Returns all records of bankruptcies, judgements, or liens against the subject (person or corporation)
Real Property Combined Report	Returns all current and previous real property owned with assessor records for each.
Public Records Search	Aspects of personal history, including Bankruptcy, Arrests, Liens, Judgements, Criminal Convictions, Evictions, Foreclosures, Sexual Offenses, Wants & Warrants. Data is also included in Comprehensive Person Report

Evictions	Returns previous eviction proceeding docket information
Foreclosures	Returns previous foreclosure docket information
Combined Business Report	Combined Business Reports include information such as executives, affiliated businesses, corporate bankruptcies, status of their corporate filings and annual disclosures, DBAs, incorporated jurisdiction, franchise relationships, IRS tax filing status, legal description, corporate registry number, date of incorporation, and expiration-related information. Liens and UCC filings are also available and included if relevant. Confi-Chek US Corporation reports also include statutory (filing) agent, links to the registry agent's and executive's personal records.
Corporate Affiliations	Franchise relationships, and other affiliated links such as common registration agents or officers.
Pilot License	Query retrieves FAA pilot license information.
Professional License	Query retrieves professional board-issued license, such as medical or legal.
DEA Licenses	Query retrieves the Drug Enforcement Administration (DEA) license and registration number issued to a health care provider allowing the provisioning of prescriptions for controlled substances.

Patriot Act	Queries the Patriot Act watch list for the SSN or name provided

Premium Services	**Detailed Description**
Social Media Report	Exhaustive search of an individual's social media accounts, records, postings and "footprints" around the web.
Traffic Citation / Driving Record	Single State search of an individual's driver record, fees vary by state.
Custom Data Products	Custom integration of Confi-Chek and Third-Party Data

Enformion Web Subscriptions – Core Commercial and Public Data Sets

Customers anticipating frequent data access can subscribe to the Enformion online platform with a pre-purchased volume and discount level, or with an unlimited subscription service. All Enformion data sets are included, premium data products incur an additional charge per-access.

Data Batch Services

Batch services are available for batch data file exchange. Initial batch script development, integration, and activation is free for new customers.

Customer request files are submitted via Secure File Transfer Protocol (SFTP) the customer using any manual or automated SFTP file transfer utility preferred. Confi-Chek's automation systems will detect the presence of the file, compute the output to subscription specifications, and make the file available for download 1 business day later. The customer need only return with their SFTP login to retrieve the output file and import the data into their on-premises third-party software.

Customers that subscribe to the Enformion online platform with a minimum of 100 licensed users receive a monthly data batch exchange service with a 100% discount (no charge).

API Web Services

Similar to our Batch Services, the core data sets available to API Web Services subscribers on-demand via system-to-system API integration. Rather than requesting large numbers of files in bulk, such as with our data batch services, API integration allows the refresh of a single record as it is accessed.

Common use cases include integration with a web-based case management system, parking enforcement, customer relationship management, or other modern technology platforms that support web services API integration. In operation, the user of the customer's system can request a "record refresh" and Confi-Chek would immediately update the record's address, phone numbers, email, and other information in real-time.

SAMPLE SERVICES SUBSCRIBER AGREEMENT (DO NOT SIGN)

This Master Services Agreement (together with the Exhibits attached hereto, this "**Agreement**") is entered into between Confi-Chek, Inc. ("**Confi-Chek**"), a California corporation, having its principal place of business at 1821 Q Street, Sacramento, CA 95811, and ("**Customer**"), a , having its principal place of business at . The Master Services Agreement, together with Exhibits B and C is effective as of ("Effective Date") and each Exhibit A is effective as of the effective data stated on that Exhibit A. Confi-Chek and Customer may execute one or more Exhibit As hereunder and each Exhibit A is subject to the terms of this Agreement.

The parties agree as follows:

1. **CERTAIN DEFINITIONS.** The following definitions apply for purposes of this Agreement:

"Confi-Chek API" means an application programming interface provided by Confi-Chek to Customer that allows Customer to submit Search Requests to the Confi-Chek API.

"Confi-Chek Data" means data that is obtained from the Confi-Chek Services or Network, all of which is comprised of publicly available information as that term is defined by the regulations prescribed under the GLBA, and that includes all languages, editions, issues, versions, revisions, modifications, enhancements and updates thereto during the Term of this Agreement.

"Confi-Chek Products" means Confi-Chek Services, Network, Confi-Chek API and/or Confi-Chek Data, together with any Confi-Chek Confidential Information.

"Confi-Chek Services" means the nationwide public record information, document retrieval and related services provided by Confi-Chek through the Network.

"FCRA" means the Fair Credit Reporting Act, 15 U.S.C.A. § 1681, et seq., as now or hereafter amended.

"GLBA" means the Gramm-Leach-Bliley Act, 15 U.S.C. § 6801 et seq., as now or hereafter amended.

"Network" means Confi-Chek's online data retrieval system of proprietary databases and data and information obtained from third parties.

"Permitted Uses" means the use of Confi-Chek Products in a manner strictly in accordance with purposes permitted under this Agreement and in compliance with all applicable laws and regulations, including, but not limited to, the GLBA and the FCRA.

"Search Request" means a search for Confi-Chek Data through the Confi-Chek API by Customer.

2. SERVICES AND LICENSE.

2.1. Products; Purpose. Confi-Chek provides Confi-Chek Products. Customer hereby agrees to use the Confi-Chek Products for the sole purpose as set forth in Exhibit A (the "Purpose").

2.2. License. Confi-Chek hereby grants to Customer a nonexclusive, nonassignable, nontransferable, limited license to use the Confi-Chek Products solely for the Purpose. Nothing in this Agreement is intended to, or should be construed to prevent Confi-Chek from entering into similar agreements with other persons or entities regarding all or any part of the Confi-Chek Products.

2.3. Restrictions and Limitations. Customer warrants that:

(a) Customer will not, either directly or indirectly, itself or through any agents or third party: (i) request, compile, store, maintain or use any Confi-Chek Products to build its own database or accumulate any Confi-Chek Products or content for any other use; or (ii) copy or reproduce any portion of the Confi-Chek Products; or (iii) redistribute, disclose, market, rent, lease, solicit, supply or transfer to any third party any portion of the Confi-Chek Products; or (iv) store any results returned by the Confi-Chek Products or anything Derived therein, except to the extent necessary for purposes of audits, the Purpose or other purposes required by applicable law. "**Derived**" means data that is directly or indirectly related to the presence or absence of the Confi-Chek Data, or is based on or having its origin in Confi-Chek Data.

(b) Customer will not disassemble, decompile, or in any way reverse engineer the Confi-Chek Products.

(c) Customer will comply with the then current Confi-Chek policies and procedures as communicated by Confi-Chek from time to time ("**Policies**"). Confi-Chek may, from time to time, notify Customer of additional, updated or new Policies. Customer's compliance with such Policies will be a condition of Confi-Chek's continued provision of the Confi-Chek Products hereunder.

(d) Customer will only use the Confi-Chek Products for the Purpose.

(e) Customer will not market the Confi-Chek Products under the Confi-Chek name.

(f) Customer will not distribute, provide, license, transfer or sell the Confi-Chek Products to any third parties.

(g) Upon receipt of any updated Confi-Chek Products from Confi-Chek, Customer will promptly replace and destroy any outdated Confi-Chek Products in its possession prior to the update.

(h) Customer will not merge any Confi-Chek Data with any consumer reports as the term "**consumer report**" is defined in the FCRA.

(i) Customer will not delete, alter, disclose or otherwise modify any security codes or protocols within the Confi-Chek Products or in any way compile and/or offer for use or sale any Confi-Chek Products or other data contained therein in a form where any security codes or protocols are deleted, altered, disclosed or otherwise modified.

2.5 Removal of Data. From time to time, Confi-Chek may, for any reason whatsoever, suppress or remove information pertaining to one or more particular persons from the Confi-Chek Data ("**Removals**"). Confi-Chek will provide Customer with notice of all such Removals. As soon as commercially reasonable, but no later than ten (10) business days after Customer' receipt of the notice of Removals from Confi-Chek, Customer will: (a) remove or suppress such persons who are the subject of the Removals from any and all materials provided by Confi-Chek to Customer; and (b) exclude such persons who are the subject of the Removals from any Confi-Chek Data that Customer may provide in its ordinary course of business.

2.6 Feedback. Customer will provide comments or any other form of feedback ("Feedback") relating to the Confi-Chek Products as reasonably requested by Confi-Chek. Feedback becomes the exclusive property of Confi-Chek and is Confi-Chek Confidential Information.

3. COMPLIANCE WITH LAWS; SECURITY OF DATA.

3.1. Compliance with Laws. Customer will not use the Confi-Chek Products in a manner contrary to or in violation of any applicable federal, state, or local law, rule, or regulation, including, but not limited to, the GLBA and the FCRA. Customer certifies that it will not use any information obtained through the Confi-Chek Products as a factor in establishing a consumer's eligibility for credit or insurance to be used primarily for personal, family, or household purposes, for employment purposes, for governmental licenses, or for any other purpose for which one might properly obtain a consumer report, as defined by the FCRA. Customer specifically agrees that Confi-Chek Products will not be merged with consumer reports as such term is defined in the FCRA. Confi-Chek reserves the right to insert certain information (sometime referred to as seeding) into the data available from the Confi-Chek Products for the purpose of determining Customer's compliance with the terms of this Agreement. Misuse of the Confi-Chek Products will constitute a material breach of this Agreement.

3.2. Privacy and Security Requirements. Customer will comply with all applicable laws concerning the Confi-Chek Products, including without limitation applicable laws regulating how an organization manages, protects and distributes confidential information and laws restricting the collection, use, disclosure, processing and free movement of personal information (collectively, the "**Privacy Regulations**"). The Privacy Regulations include, to the extent applicable, the Federal "Privacy of Consumer Financial Information" Regulation (12 CFP Part 40) and Interagency Guidelines Establishing Information Security Standards (App B to 12 CFR Part 30), as amended from time to time, issued pursuant to the GLBA. Customer expressly agrees that it will comply with the use requirements applicable pursuant to the GLBA and similar laws, including without limitation each of the permissible use requirements set forth on Exhibit C attached hereto. Customer will maintain all appropriate administrative, physical and technological processes and equipment to store and protect the Confi-Chek Products in a secure manner, including without limitation, maintaining an information security program that is designed to protect information processing system(s) and media containing the Confi-Chek Products from internal and external security threats, and the Confi-Chek Products from unauthorized use or disclosure. In addition and to the extent applicable, Customer specifically agrees to comply with each of the security requirements set forth on Exhibit B attached hereto. Confi-Chek may, from time to time, provide written notice to Customer of updates to the security requirements set forth on Exhibit B, and Customer will comply with the updated security requirements following a mutually agreed upon and reasonable period of time. Customer acknowledges and agrees that Customer has an ongoing obligation to protect and preserve the confidentiality, privacy, security and integrity of the Confi-Chek Products, and the standards embodied in this Agreement are merely minimum standards of conduct for Customer in furtherance of the foregoing continuing obligation.

4. FEES, AUDIT RIGHTS AND FINANCIAL STATEMENTS.

4.1. Fees. Customer agrees to pay Confi-Chek the applicable charges as set forth in Exhibit A of this Agreement. Any periodic and/or minimum Customer fees under this Agreement are non-refundable, in whole or in part, in the event of a termination of this Agreement, since all such fees are compensation for supplying service and carrying the account. Confi-Chek reserves the right to change the fees by issuing a revised rate schedule, but no change in such charges will become effective as to Customer earlier than thirty (30) days after written notice thereof will have been given by Confi-Chek to Customer. Customer will also pay all the cost of all media, media shipping and insurance costs, taxes, duties or charges of any kind imposed by any federal, state, or local governmental entity for the Confi-Chek Products provided under this Agreement. However, Customer will not be responsible for taxes imposed upon Confi-Chek by any federal, state or local authority against the net income of Confi-Chek. Payment inquiries should be remitted in writing to the following address: Confi-Chek, 1915 21st Street, Sacramento, CA 95811, or by fax to (916) 739-1118.

4.2. Invoicing and Payment. Unless otherwise expressly stated in Exhibit A to this Agreement, Customer will pay all invoices from Confi-Chek issued pursuant to this Agreement within thirty (30) days of the invoice date.

4.3. Unpaid or Outstanding Balances. Without limiting any of Confi-Chek's remedies for non-payment or late payment of any amounts due by Customer to Confi-Chek,

(a) amounts which are not paid within sixty (60) days of the invoice date or the date on which Confi-Chek notifies Customer, whichever is sooner, may be subject to a late charge of one and one-half percent (1.5%) per month (18% per year) or the maximum allowed by law, whichever is less. If collection efforts are required, Customer will pay all costs of collection, including reasonable attorneys' fees.

(b) Confi-Chek reserves the right to immediately suspend Customer's access to Confi-Chek Products until any unpaid or past due amounts are paid in full.

4.4. Audit Rights. Customer will maintain records including, but not limited to complete and accurate accounting records in accordance with generally accepted accounting practices, to substantiate Customer's performance under this Agreement including, without limitation, Customer's compliance with payment, legal and all security requirements. Customer will preserve such records for a period of at least thirty-six (36) months after termination of this Agreement. Moreover, no more than one (1) time per calendar year during the Term of this Agreement and no more than once per calendar year after termination of this Agreement and for no more than thirty-six (36) months thereafter, Confi-Chek will have access to those records of Customer that are necessary to determine Customer's compliance with its obligations under this Agreement and to Customer's facilities for the purpose audit either through its own employees, representatives or an independent public accounting firm selected by Confi-Chek (the "**Auditor**"). Any such review of Customer's records, facilities, or both, may be conducted during Customer's normal business hours upon Confi-Chek providing Customer no less than five (5) business days' prior written notification; provided however, that in the event of a material breach including, but not limited to, any material deficiency in Customer's performance of this Agreement, then such interval restriction and required prior written notification, except for reasonable notice, will not apply. For each third party who provides Confi-Chek Product-related services to Customer, from time to time, Confi-Chek will have the right to review, at Confi-Chek's expense, each such third party's security processes and procedures related to the transmission, storage or processing of Confi-Chek Products. Customer will

reasonably cooperate, and will request each such third party to also reasonably cooperate, with Confi-Chek and any Confi-Chek requests in conjunction with all such reviews including, but not limited to Confi-Chek requests to correct any deficiencies discovered during such audits within a period of time mutually agreed upon and/or suspend any further transmission of Confi-Chek Products until such deficiencies are corrected. Customer agrees that it will reasonably cooperate with all such reasonable Confi-Chek requests for information and audits. Customer's obligations to comply, with the provisions of this Agreement are not contingent upon, or otherwise affected by, the audit rights of Confi-Chek.

5. INTELLECTUAL PROPERTY; CONFIDENTIALITY.

5.1. Intellectual Property. Customer acknowledges that Confi-Chek has expended substantial time, effort, and funds to collect, arrange, compile create and deliver the Confi-Chek Products. Customer agrees not to reproduce, retransmit, republish, or otherwise transfer for any commercial or other purpose any information that Customer receives from Confi-Chek or the Confi-Chek Products except as permitted under this Agreement. Customer acknowledges that Confi-Chek (and/or Confi-Chek's third-party data providers) will retain all right, title, and interest in and to the data and information provided by the Confi-Chek Products and to Derivative Matter under applicable contractual, copyright, intellectual property and related laws, and Customer will use such materials consistent with Confi-Chek's interests and notify Confi-Chek of any threatened or actual infringement of Confi-Chek's rights. Customer further acknowledges and agrees that it will acquire no right, title or interest under applicable copyright or other laws in the Confi-Chek Products and materials provided or accessed under this Agreement. Customer will not remove or obscure the copyright notice or other notices contained on materials accessed through the Confi-Chek Products. "**Derivative Matter**" means any work, invention, new material or data which is based in whole or in part upon the Confi-Chek Products and any intellectual property rights associated therewith, including without limitation derivative work, improvement, extension, revision, modification, translation, compilation, or error correction.

5.2. Confidentiality. "**Confidential Information**" means (a) the terms and conditions of this Agreement, (b) the Confi-Chek Products, (c) Feedback and (d) all Confi-Chek information and materials to which Customer has access in connection with this Agreement and all non-public personally identifiable information including, but not limited to, name, address, date of birth, social security or other government issued social identification number, income and credit histories, bank and credit card numbers, email address, and static IP address. Customer will use Confi-Chek Confidential Information solely for the Purpose and will not use, disseminate or in any way disclose any Confidential Information to any third party other than as required for the Purpose. Additionally, notwithstanding the foregoing, Confi-Chek may disclose the terms and conditions of this Agreement to Confi-Chek's agent(s) and/or processor(s) under appropriate nondisclosure terms solely to the extent necessary to fulfill its obligations under this Agreement. Except as expressly permitted herein, Customer will not disclose any Confidential Information outside of the United States without Confi-Chek's prior written consent.

5.3. Exceptions to Confidentiality. Confidential Information does not include information that (a) is or becomes part of the public domain through no act or omission of Customer or its agents or processors, (b) is rightfully obtained by Customer without breach of any obligation to maintain its confidentiality from a source other than Confi-Chek who is known or should have been known to Customer to be under no obligation to Confi-Chek or its agents or employees to maintain such information in confidence, or (c) is independently developed by Customer without using the Confidential Information. Customer may disclose Confidential Information in response to a valid court or governmental order, if (x) Customer has given Confi-Chek prior written notice and provided reasonable assistance to afford it the opportunity to object and obtain a protective order or other reasonable assurance that confidential treatment will be accorded the information, and (y), in the opinion of Customer's counsel, Customer is compelled as a matter of law to disclose the subject Confidential Information, and (z) Customer discloses to the party compelling disclosure only the part of such Confidential Information as is required by law to be disclosed in the opinion of its counsel, and uses commercially reasonable efforts to obtain confidential treatment therefor.

5.4. Breach of Confidentiality. If there is a breach of Customer's confidentiality obligations under this Agreement, Customer will reasonably cooperate with Confi-Chek in investigating and mitigating, to the extent practicable, any damages due to such breach and/or misappropriation. Such cooperation will not relieve Customer of any liability it may have as a result of such a breach. Except to the extent required by applicable law, Customer will make no public notification, including but not limited to press releases or consumer notifications, of the potential or actual occurrence of such misappropriation and/or unauthorized disclosure without Confi-Chek's prior written consent, which consent will not be unreasonably withheld, conditioned or delayed. To the extent such public notifications are required by applicable law, Customer will provide Confi-Chek written notice prior to releasing such public notifications.

7.1. No Suit. Customer covenants not to sue or maintain any cause of action, claim, demand, cross-claim, third party action or other form of litigation or arbitration against Confi-Chek, its officers, directors, employees, contractors, agents, affiliated bureaus or Customers arising out of or relating in any way to the Confi-Chek Products not being accurate, timely, complete or current.

8. DISCLAIMER OF WARRANTY. Confi-Chek will use reasonable best efforts to deliver the Confi-Chek Products to Customer; provided, however, that Customer accepts that Confi-Chek Products are provided "AS IS." Because the Confi-Chek Products involve conveying information provided to Confi-Chek by other sources, Confi-Chek cannot and will not be an insurer, guarantor or warrantor of the accuracy or reliability of the Confi-Chek Products, data contained in its database or in the Confi-Chek Products. CONFI-CHEK DOES NOT GUARANTEE OR WARRANT THE ACCURACY, TIMELINESS, COMPLETENESS, CURRENTNESS, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OF THE CONFI-CHEK PRODUCTS, INFORMATION IN THE CONFI-CHEK PRODUCTS OR THE MEDIA ON OR THROUGH WHICH THE CONFI-CHEK PRODUCTS ARE PROVIDED. CONFI-CHEK DOES NOT GUARANTEE CONTINUOUS OR UNINTERRUPTED DISPLAY OR DISTRIBUTION OF THE CONFI-CHEK PRODUCTS. CONFI-CHEK WILL NOT BE LIABLE TO CUSTOMER FOR ANY LOSS OR INJURY ARISING OUT OF OR CAUSED IN WHOLE OR IN PART BY ANY OF CONFI-CHEK'S ACTS OR

OMISSIONS, WHETHER NEGLIGENT OR OTHERWISE, IN PROCURING, COMPILING, COLLECTING, INTERPRETING, REPORTING, COMMUNICATING OR DELIVERING THE CONFI-CHEK PRODUCTS OR INFORMATION THEREIN. CONFI-CHEK PROVIDES NO WARRANTIES OTHER THAN AS EXPRESSLY SET FORTH ABOVE AND DISCLAIMS ALL OTHER WARRANTIES, EXPRESS OR IMPLIED.

9. **TEMPORARY TERMINATION OF ACCESS TO NETWORK.** Confi-Chek reserves the right at any time and without prior notice to Customer to change the Network's hours of operation or to limit access to the Network in order to perform repairs, make modifications or as a result of circumstances beyond Confi-Chek's reasonable control.
10. **Representations and Warranties.** Customer represents and warrants to Confi-Chek, as of the Effective Date and such other dates as provided below, the following:
    (a) The United States Foreign Corrupt Practices Act prohibits giving money or items of value to non-United States officials to influence a non-United States government, and also prohibits giving money or items of value to any person or firm when there is reason to believe the money or item of value will be passed on to a government official in an attempt to influence a non-United States government. Customer is in compliance and will continue to comply with all requirements of the United States Foreign Corrupt Practices Act and to refrain from accepting or making payments to third parties, which would cause Confi-Chek or its data providers to violate or otherwise have liability under such Act.
    (b) Customer is an equal opportunity employer. Customer does not discriminate on the basis of race, religion, age, sex, marital status, citizenship status, sexual orientation, veteran status, medical condition, national origin, gender identity, genetic information, physical handicap or disability, or any other legally protected classification, except as may be permitted by applicable law.
    (c) As of the Effective Date, neither Customer nor any entity holding any material ownership in Customer, nor any officer or director of Customer, is the subject of any sanctions administered or enforced by the U.S. Department of the Treasury's Office of Foreign Assets Control ("**OFAC**"), or other relevant sanctions authority (collectively, "**Sanctions**"), nor is Customer or any entity holding any material ownership in Customer, nor any officer or director of Customer, located, organized or resident in a country or territory that is the subject of Sanctions. Customer represents and warrants that it has not, nor will it, violate any Sanctions. Customer will not in connection with this Agreement and the transactions contemplated herein fund or engage in any activities with any individual or entity or in any country or territory that, at the time of such funding or activity, is subject to Sanctions.
    (d) Customer is duly organized, existing and in good standing under the laws of the state of its incorporation. Customer has the requisite power and authority to enter into, and to satisfy all of its obligations under, this Agreement and any related agreements. This Agreement and the transactions contemplated hereby have been duly authorized and approved by the appropriate officers and/or other Personnel of Customer, and no further action or proceeding on the part of Customer is necessary or appropriate with respect to the execution by Customer of this Agreement or any related agreements, or the consummation by Customer of the transactions contemplated hereby or thereby.
11. **FORCE MAJEURE.** Neither party will be liable to the other for failure to perform or delay in performance under this Agreement if, and to the extent, such failure or delay is caused by conditions beyond its reasonable control and which, by the exercise of reasonable diligence, the delayed party is unable to prevent or provide against. Such conditions include acts of God; strikes, boycotts or other concerted acts of workmen; failure of the Internet, utilities or networks; laws, regulations or other orders of public authorities; military action, state of war or other national emergency; fire or flood.
12. **RETENTION OF RIGHTS**. Nothing in this Agreement is intended to or will limit or restrict Confi-Chek's ability to market and sell its services within the geographic areas in which, or to the customers to whom, Customer markets or sells its services.

CONFI-CHEK, INC.	**CUSTOMER:**
By:	By:
Name:	Name:
Title:	Title:

This is an Exhibit to, and subject to the terms of the Master Services Agreement between Confi-Chek and Customer effective .

EXHIBIT A- (insert number; change for additional Exhibit As)

EXHIBIT EFFECTIVE DATE:

PURPOSE (CHECK ALL THAT APPLY):

☐ Purpose A: Internally evaluating and testing the Confi-Chek Products ("Testing")

☐ Purpose B: Performing research in the regular course of Customer's business and (b) if required, temporarily storing (on a storage device in Customer's exclusive control) and/or printing an insubstantial amount of only applicable portions of Confi-Chek Data in order to quote it in memoranda, briefs or similar work product produced in the regular course of Customer's business or to provide to Customer's clients in the regular course of Customer's business.

IF PURPOSE A (TESTING) IS CHECKED ABOVE, CHECK DURATION FOR TESTING*: days

* Note: Duration begins on the Exhibit Effective Date.

FEES:

For Purpose A (Testing), no charge during duration.

For Purpose B, the following fees apply:

INVOICING AND PAYMENT (INSERT ONLY IF DIFFERENT FROM SECTION 4.2 OF THE AGREEMENT):

CONFI-CHEK, INC.	**CUSTOMER**:
By:	
Name:	
Title:	Title:

SAMPLE – DO NOT SIGN

EXHIBIT B

ACCESS SECURITY REQUIREMENTS FOR NON-PUBLIC INFORMATION ACCESS

Customer will maintain an information security program that is designed to protect information processing system(s) and media containing Confi-Chek Products from internal and external security threats, and Confi-Chek Products from unauthorized disclosure. Customer will be responsible to implement this program for all Confi-Chek Products to which Customer or any of its employees, consultants, agents, representatives, contractors or subcontractors ("**Personnel**") have or obtain access. Confi-Chek reserves the right to make changes to this Exhibit and its security requirements without prior notification to Customer. The information provided in this Exhibit provides minimum baseline information security requirements. Customer agrees to follow the requirements outlined below when accessing, transmitting, processing, storing or using (collectively, "**accessing**" or "**access**") any Confi-Chek Products. Customer will strictly comply with the following:

1. Access and Passwords.

1.1. **Confi-Chek Products Access Control Measures**

(a) All credentials such as user names/identifiers (user IDs) and user passwords must be kept confidential and must not be disclosed to an unauthorized party.
(b) If using third party or proprietary system to access Confi-Chek Products, Customer will ensure that the access must be preceded by authenticating users to the application and/or system.
(c) If the third party or third party software or proprietary system or software used to access Confi-Chek Products is replaced or no longer in use, the passwords should be changed immediately.
(d) Customer will cause a unique user ID and password to be created for each user to enable individual authentication and accountability for access to Confi-Chek's Products.
(e) User IDs and passwords will only be assigned to authorized individuals granting the least privilege necessary to perform the Personnel's responsibilities.
(f) Ensure that Personnel who are authorized access to credit information have a business need to access such information and understand these requirements to access such information are only for Permitted Purposes.
(g) Customer will ensure that no Customer Personnel access their own credit reports or those reports of any family member(s), friend(s) or other individual unless in connection with a Permitted Purpose and applicable law.
(h) Customer will implement a process to terminate access rights immediately for users who access Confi-Chek Products when those users are terminated or when they have a change in their job tasks and no longer require access to that credit information.
(i) Customer will implement a process to perform periodic user account reviews to validate whether access is needed as well as the privileges assigned.
(j) Customer will implement a process to periodically review user activities and account usage, ensure the user activities are consistent with the individual job responsibility, business need, and in line with contractual obligations.

1.2. **Use of Passwords with Confi-Chek Products.** Customer will:

(a) Require strong passwords consistent with industry best practices that: (i) cannot be easily determined (i.e. name or company name, repeating numbers and letters or consecutive numbers and letters);
(b) Ensure that passwords are not transmitted, displayed or stored in clear text
(c) Protect all end user (e.g. internal and external) passwords using, for example, encryption or a cryptographic hashing algorithm also known as "one-way" encryption, when using encryption and "salting", ensure that strong encryption algorithm are utilized (e.g. AES 256 or above).
(d) Require active logins to credit information systems to be configured with an appropriate inactive session timeout.

1.3. Change of Passwords. Passwords (user passwords) must be changed immediately when:

(a) Any system access software is replaced by other system access software or is no longer used.
(b) The hardware on which the software resides is changed or disposed.
(c) Any suspicion of a password being disclosed to an unauthorized party.

2. Asset Protection. Customer will maintain commercially reasonable controls, based on Customer's industry (or general best practices if nothing for the industry exists), in place to protect Customer's assets. This should include handling standards for introduction, transfer, removal and disposal of all assets based on asset classification. Without limiting the foregoing, Customer will:

a) Maintain an inventory of critical hardware and critical software assets that access, store or make use of Confi-Chek Products.
b) Have procedures for the disposal and reuse of equipment that access, make use of or store Confi-Chek Products, including notification procedures in the event of any lost or misplaced equipment that may have access to or store information related to Confi-Chek Products.
c) Implement physical security controls to prevent unauthorized entry to Customer's facility and access to Confi-Chek Products. Customer will ensure that access is controlled with badge readers, other systems, or devices that restrict physical access, including but not limited to authorized lock and key.

3. Data and Information Protection. Customer will maintain a documented set of rules and procedures that regulate the use, access and control of information, including without limitation its receipt, transmission, processing, storage, controls, distribution, retrieval, access and presentation. Without limiting the foregoing, these rules will protect the confidentiality and integrity of personal

consumer information as required under the GLB Safeguards Rule. Customer will maintain a formal user registration and de-registration procedure for granting and revoking access and access rights. Without limiting the foregoing, Customer will comply with the following measure to protect all data:

a) Develop and follow procedures to ensure that data is protected throughout its entire information lifecycle.
b) Implement and follow current best security practices for computer virus detection scanning services and procedures
c) Implement and follow current best procedures for transmission, disclosure, storage, destruction and any other information modalities or media should address all aspects of the lifecycle of the information.
d) Encrypt all Confi-Chek Products when stored or transmitted electronically on any system using strong encryption such AES 256 or above.
e) Confi-Chek Products are confidential and must not be stored on personally-owned equipment or portable devices including, but not limited to, laptops, personal digital assistants, MP3 devices, USB devices, removable/portable media or smart tablets or smart phones.
f) When using smart tablets or smart phones to access Confi-Chek Products, ensure that such devices are protected via device pass-code.
g) Applications utilized to access Confi-Chek Products must protect data while in transmission such as SSL protection and/or use of VPN.
h) When no longer in use, all hard-copy materials containing Confi-Chek Products must be crosscut shredded, incinerated, or pulped such that there is reasonable assurance the hard-copy materials cannot be reconstructed.
i) When no longer in use, electronic media containing Confi-Chek Products must be rendered unrecoverable via a secure wipe program in accordance with industry-accepted standards for secure deletion, or otherwise physically destroying the media (for example, degaussing).
j) Require any and all of Personnel permitted under this Agreement to have access to any Confi-Chek Products to maintain effective information security measures designed to protect Confi-Chek Products from unauthorized disclosure or use.
k) Ensure that all data requests from Customer to Confi-Chek include the IP address of the device from which the request originated (i.e., the requesting client's IP address), where applicable.

4. Network Protection.

a) Protect Internet connections with dedicated, industry-recognized firewalls that are configured and managed using industry best security practices. Internal private Internet Protocol (IP) addresses must not be publicly accessible or natively routed to the Internet. Network address translation (NAT) technology should be used.
b) Administrative access to firewalls and servers must be performed through a secure internal wired connection only. Change vendor defaults including but not limited to passwords, encryption keys, SNMP strings, and any other vendor defaults.
c) For wireless networks connected to or used for accessing or transmission of Confi-Chek Products, ensure that networks are configured and firmware on wireless devices updated to support strong encryption for authentication and transmission over wireless networks.
d) When using third party service providers (e.g. application service providers) to access, transmit, store or process Confi-Chek Products, ensure that an independent 3rd party security assessment (one of the following, or a current equivalent: ISO 27001, PCI DSS, EI3PA, SSAE 16 – SOC 2/SOC3, FISMA, or CAI / CCM) has been performed, and that they are found to be compliant.
e) Perform regular tests/scans on information systems (port scanning, virus scanning, internal/external vulnerability scanning). Ensure that issues identified via testing are remediated according to the issue severity (e.g. fix critical issues immediately, high severity in 15 days, etc.)
f) Ensure that audit trails are enabled and active for systems and applications used to access, store, process, or transmit Confi-Chek Products; establish a process for linking all access to such systems and applications.
g) Use current best practices to protect telecommunications systems and any computer system or network device(s) used to provide Confi-Chek Products and to access Confi-Chek Products.

5. Mobile and Cloud Technology.

a) Storing Confi-Chek Products on mobile, cloud or portable devices and services is prohibited. Any exceptions must be obtained from Confi-Chek in writing; additional security requirements will apply.
b) Mobile applications development must follow industry known secure software development standard practices such as OWASP and OWASP Mobile Security Project adhering to common controls and addressing top risks.
c) Mobile applications development processes must follow secure software assessment methodology which includes appropriate application security testing (for example: static, dynamic analysis, penetration testing) and ensuring vulnerabilities are remediated.
d) Under no circumstances are Confi-Chek Products to be exchanged between secured and non-secured applications on the mobile device.
e) In case of non-consumer access, that is, commercial/business-to-business (B2B) users accessing Confi-Chek Products via mobile applications (internally developed or using a third party application), ensure that multi-factor authentication mechanisms are utilized to authenticate users to application.

6. Personnel Background Checks, Policies and Training.

6.1. Background Check.

(a) Customer will conduct, or require, appropriate pre-employment background checks on all Personnel that have access to hardware or software systems that access, use or store Confi-Chek Products.
(b) Customer will comply with all applicable federal, state and local laws, including fair employment practices and equal employment opportunity, when conducting pre-employment background screenings.
(c) Customer will maintain a process to enable it to learn if any Personnel are convicted of any crimes at any time after the pre-employment background screening that would have otherwise disqualified such Personnel during such pre-employment background screening. Regardless of how Customer learns of such violation, in the event such Personnel have access to Confi-Chek Products, it must promptly contact Confi-Chek to discuss the potential impact to information security and confidentiality.
(d) All Personnel must be bound by Non-Disclosure/Confidentiality Agreement before they perform any service requiring access to Confi-Chek Products.

6.2. Policies and Training.
(a) Prior to receiving access to Confi-Chek Products, Personnel will receive security awareness training appropriate to their job function.
(b) The access rights of all Personnel with access to systems or media containing Confi-Chek Products will be removed immediately upon termination of their employment, contract or agreement, or adjusted upon change of job function.
(c) Customer will require its customers to maintain effective information security measures consistent with this Agreement in order to protect confidential information from unauthorized disclosure or use of Confi-Chek Products.

7. Security Audits.
a) Customer understands that its use of Confi-Chek Products and compliance with the security requirements set forth in this Exhibit may be monitored and audited by Confi-Chek. Confi-Chek may from time to time conduct on-site security audits or reviews on Customer's systems containing any Confi-Chek Products as it relates to the Customer's compliance with the terms of this Exhibit or the mechanisms Customer maintains to safeguard access to Confi-Chek Products. Audits may include examination of systems security and associated administrative practices.
b) Reasonable access to audit trail reports of systems utilized to access Confi-Chek Products will be made available to Confi-Chek upon request, for example during breach investigation or while performing audits.

8. Vulnerability Monitoring; Software Development.
(a) Keep operating system(s), firewalls, routers, servers, personal computers (laptops and desktops), mobile devices and all other systems current with appropriate system patches and updates.
(b) Configure infrastructure such as firewalls, routers, servers, tablets, smart phones, personal computers (laptops and desktops), and similar components to industry best security practices, including disabling unnecessary services or features, and removing or changing default passwords, IDs and sample files/programs, and enabling the most secure configuration features to avoid unnecessary risks.
(c) Implement and follow current best security practices for computer virus detection scanning services and procedures:
- Use, implement and maintain a current, commercially available anti-virus software on all systems, if applicable anti-virus technology exists.
- Ensure that all anti-virus software is current, actively running, and generating audit logs; ensure that anti-virus software is enabled for automatic updates and performs scans on a regular basis.
- If you suspect an actual or potential virus infecting a system, immediately cease accessing the system and do not resume the inquiry process until the virus has been eliminated.

9. Security Incidents.
(a) Customer will have a documented plan and associated procedures in case of an information security incident. The plan must clearly articulate the responsibilities of Personnel and identify relevant notification parties.
(b) Unless prohibited by law, Customer will notify Confi-Chek of any security breach involving (i) the theft, loss or unauthorized disclosure, acquisition, access to or misuse of the Confi-Chek Products in the possession or control of Customer or any Authorized End User; or (ii) a compromise of the confidentiality and/or integrity of any hardware, software, network, or telecommunications or information technology systems used by Customer or its Authorized End Users to transmit, store, process or otherwise handle the Confi-Chek Products ("**Security Breach**") as soon as Customer knows or reasonably suspects that such Security Breach exists or did exist, and in any event within twenty-four (24) hours of such knowledge or suspicion. In the event Customer is prohibited by law from providing such notice, it will nonetheless provide as much of the foregoing information as it is permitted to provide under law at the earliest practicable time it is permitted to do so under law. Email notification at customercare@Confi-Chek.com.

10. Head Security Designate. In addition to the above, following requirements apply where Customer or its Personnel are provided access to Confi-Chek Products directly or via Internet **("Internet Access")**:
a) Customer agrees to identify to Confi-Chek in writing an employee it has designated to act on its behalf as a primary interface with Confi-Chek on systems access related matters. This individual will be identified as the "**Head Security Designate**." Customer's Head Security Designate will be responsible for establishing, administering and monitoring all Customer Personnel's

access to Confi-Chek Products which are delivered by Internet Access, or approving and establishing Security Designates to perform such functions

b) Customer will limit the dissemination of the Confi-Chek Data Products to appropriate employees whose duties justify the need to know such Confi-Chek Data Products and will require that all such employees are first subject to obligations of confidentiality substantially similar to those contained herein. Head Security Designate must immediately report any suspicious or questionable activity to Confi-Chek regarding access to Confi-Chek Products and must disable access by any employee if it is or may become likely to result in a security threat, the release or compromise of Confi-Chek Products or if the employee 's employment is terminated by Customer. Confi-Chek reserves the right to terminate any accounts it deems a security threat.

11. Additional Security Terms.

(a) Customer acknowledges and agrees that Customer and each of its Personnel has an ongoing obligation to protect and ensure the confidentiality, privacy, security and integrity of Confi-Chek Products, and the standards embodied in this Agreement are merely minimum standards of conduct in furtherance of the foregoing continuing obligation.

(b) Confi-Chek may provide written notice to Customer of updates to Confi-Chek's information security requirements ("**Updated Security Requirements"**). Customer will comply with the Updated Security Requirements following a mutually agreed upon and reasonable period of time; provided that if the parties cannot reasonably agree to a period of time for Customer's compliance, or if Customer fails to provide Confi-Chek with a written certification of compliance within thirty (30) days after the agreed upon compliance date, then Confi-Chek may terminate this Agreement without any penalty or further obligation.

(c) Before using any third party service providers to access, transmit, or store Confi-Chek Products, Customer must obtain the prior written consent of Confi-Chek. Additional requirements and documentation may be required by Confi-Chek.

12. Breach. Without limiting Confi-Chek's rights or Customer's obligations under any other provision of this Agreement, in the event of a breach by Customer of this Agreement that results in the theft, loss, or unauthorized disclosure, acquisition, access to or misuse of Confi-Chek Products, direct damages in connection with any such breach will include (i) the reasonable costs and expenses of investigation and analysis (including by law firms and forensic firms retained by Confi-Chek, to the extent Customer does not share its investigation and analysis work product, or such work product is not reasonably acceptable to Confi-Chek), (ii) reasonable costs of correction or restoration of any destroyed, lost or altered data or assets, notification to affected consumers (including by mail house firms), and (iii) costs of credit monitoring and other reasonably required remediation services. Customer will reimburse Confi-Chek for any losses incurred by Confi-Chek in correcting Customer's failure to comply with the privacy and/or confidentiality provisions of this Agreement, including Customer's destruction obligations.

EXHIBIT C
PERMISSIBLE USES

Customer understands that Confi-Chek cannot provide legal advice regarding the appropriate uses of non-public, personal information and that it is Customer's obligation and responsibility to seek legal counsel in interpreting the applicable laws. However, regardless of the opinion of Customer's legal counsel, Confi-Chek will allow or restrict access to Confi-Chek Products based on Confi-Chek's understanding of the applicable laws. All such decisions are the sole discretion of Confi-Chek and will be final.

GLBA PERMISSIBLE USES. The GLBA requires financial institutions and credit-reporting agencies to protect personal financial information of customers, and restricts disclosure of such information to non-affiliated third parties. Confi-Chek Products may contain information governed by GLBA. While other uses for non-public records may be allowable under the GLBA, the purposes for which Confi-Chek will allow access to Confi-Chek Products are limited to those listed below.

- To protect against or prevent actual or potential fraud, unauthorized transactions, claims, or other liability.
- To the extent specifically permitted or required under laws other than GLBA, and in accordance with the Right to Financial Privacy Act of 1978, to law enforcement agencies, to self-regulatory organizations, or for an investigation on a matter related to public safety.
- To comply with federal, state, or local laws, rules and other applicable legal requirements.
- As necessary to effect, administer, or enforce a transaction requested or authorized by the consumer.
- Use by persons holding a legal or beneficial interest relating to the consumer.
- Use by persons acting in a fiduciary or representative capacity on behalf of, and with the implied or express consent of, the consumer.
- For required institutional risk control, or for resolving consumer disputes or inquires.

GLBA was enacted to protect the use and disclosure of non-public personal information, including, in certain instances, the use of identifying information only; and GLBA provides limited exceptions under which such information may be used; therefore, Customer hereby certifies to Confi-Chek that (a) it has determined that its use of certain identification-only products (Reference Products), including but not limited to, Credit Header Products, is pursuant to an exception under GLBA and (b) its use of the Reference Products will be for the GLBA exception(s) designated above.

Customer further acknowledges an understanding of the restrictions imposed by the FCRA. Customer agrees to only use non-public information to locate or to further identify the subject of a search. Customer may not and will not use non-public information, in whole or in part, to determine a consumer's eligibility for credit, for employment, or for tenant screening, nor may Customer use non-public information for any other purpose for which Customer might properly obtain a consumer report, except in connection with collection of a debt. If adverse action is to be taken against the subject of a search and the basis for such adverse action is information obtained or derived from non-public information, Customer must verify such information from another source before taking such adverse action.

For a complete reading of the law, visit: http://www.ftc.gov/privacy/glbact/glbsub1.htm and https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/fair-credit-reporting-act

CELL PHONE NUMBERS. Customer acknowledges that the government has placed restrictions upon the use of cell phone numbers. Customer agrees that any use of the cell phone numbers provided by Confi-Chek as part of the Confi-Chek Products will be used in strict accordance with all applicable laws, rules and regulations.

DPPA PERMISSIBLE USES. The Driver's Privacy Protection Act, 18 U.S.C. Section 2721 et seq. ("**DPPA**"), makes it unlawful for any person knowingly to obtain or disclose personal information from a motor vehicle record for any use not permitted by DPPA. Confi-Chek Products may contain information that is governed by the DPPA. Below are the uses permitted by DPPA:

- Use by any government agency, including any court or law enforcement agency, in carrying out its functions, or any private person or entity acting on behalf of a federal, state, or local agency in carrying out that agency's functions.
- Use in the normal course of business by a legitimate business or its agents, employees, or contractors, but only to verify the accuracy of personal information submitted by the individual to the business or its agents, employees, or contractors; and, if such information as so submitted is not correct or is no longer correct, to obtain the correct information, but only for the purposes of preventing fraud by pursuing legal remedies against, or recovering on a debt or security interest against, the individual.
- Use in connection with any civil, criminal, administrative, or arbitral proceeding, in any federal, state, or local court agency, or before any self-regulatory body, including the service of process, investigation and anticipation of litigation, and the execution of enforcement of judgments and orders, or pursuant to an order of a federal, state, or local court.
- Use by any insurer or insurance support organization, or by a self-insured entity, or its agents, employees, or contractors, in connection with claims investigation activities, antifraud activities, rating, or underwriting.
- Use by an employer or its agent or Insurer to obtain or verify information relating to a holder of a commercial driver's license that is required under chapter 313 of title 49, U.S. Code.
- Use by any licensed private investigative agency or licensed security service for any purpose described above.

For a more complete reading of the law, visit: http://www.flhsmv.gov/ddl/FedDPPAStatute.pdf

ACCESS TO AND USE OF DEATH DATA. Customer will not take any adverse action against any consumer without further investigation to verify information from the deceased data, flags or other indicia within the Confi-Chek Products. Access

to the Death Master File as issued by the Social Security Administration requires an entity to have a legitimate fraud prevention interest or a legitimate business purpose pursuant to a law, governmental rule regulation, or fiduciary duty, as such business purposes are interpreted under 15 C.F.R. § 1110.102(a)(1). The National Technical Information Service has issued the Interim Final Rule for temporary certification permitting access to the Death Master File ("**DMF**"). Pursuant to Section 203 of the Bipartisan Budget Act of 2013 and 15 C.F.R. § 1110.102, access to the DMF is restricted to only those entities that have a legitimate fraud prevention interest or a legitimate business purpose pursuant to a law, governmental rule regulation, or fiduciary duty, as such business purposes are interpreted under 15 C.F.R. § 1110.102(a)(1). As many credit bureau data services contain information from the DMF, Customer must be aware of and comply with its continued obligation to restrict any use of deceased flags or other indicia within the Confi-Chek Products to legitimate fraud prevention or business purposes in compliance with applicable laws, rules and regulations and consistent with applicable FCRA or GLBA use. Customer's continued use of Confi-Chek Products affirms Customer's commitment to comply with these terms and all applicable laws.