Contract #: AR3101

STATE OF UTAH COOPERATIVE CONTRACT

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

Experian Information Solutions, Inc.
Name

475 Anton Boulevard Costa
Street Address

Mesa	CA	92626
City	*State*	*Zip*

Vendor # 37577DB Commodity Code #: 920-05 Legal Status of Contractor: For-Profit Corporation

Contact *Name:* Bradley Uhlenhoff *Phone Number:* 208-249-2288 *Email:* bradley.uhlenhoff@experian.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: Thursday, August 01, 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

Heather Richey 8/1/2019
Contractor's signature Date

Heather Richey Compliance Director
Type or Print Name and Title

DIVISION OF PURCHASING

Aug 2, 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.

Except as otherwise set forth in the Indemnification section above, the limit of liability shall be as follows:

i. Contractor's liability for any claim, loss or liability arising out of, or connected with the Services provided, and whether based upon default, or other liability such as breach of contract, warranty, negligence, misrepresentation or otherwise, shall in no case exceed direct damages in: (i) an amount equal to two (2) times the charges specified in the Purchase Order for the Services, or parts thereof forming the basis of the Purchasing Entity's claim, (said amount not to exceed a total of twelve (12) months charges payable under the applicable Purchase Order) or (ii) five million dollars ($5,000,000), whichever is greater.

ii. The Purchasing Entity may retain such monies from any amount due Contractor as may be necessary to satisfy any claim for damages, costs and the like asserted against the Purchasing Entity unless Contractor at the time of the presentation of claim shall demonstrate to the Purchasing Entity's satisfaction that sufficient monies are set aside by the Contractor in the form of a bond or through insurance coverage to cover associated damages and other costs.

iii. Notwithstanding the above, neither the Contractor nor the Purchasing Entity shall be liable for any consequential, indirect or special damages of any kind which may result directly or indirectly from such performance, including, without limitation, damages resulting from loss of use or loss of profit by the Purchasing Entity, the Contractor, or by others.

iv. The limitations of liability in this section will not apply to claims for bodily injury or death as set forth in Section 13, and Section 31 – Data Privacy when made applicable under a specific purchase order.

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 or authorized 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, or an equivalent rating with a similar rating agency. 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: (may be provided as part of a professional liability policy)

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, that provides coverage for its work undertaken pursuant to each Participating Addendum.

c. Contractor shall pay premiums on all insurance policies. Contractor or its insurer shall provide thirty (30) calendar days prior written notice to Purchasing Entity and Participating Entity before the cancellation or non-renewal of any required policies.

d. The Contractor's general liability policy shall (1) name the Participating States identified in the Request for Proposal as additional insureds, (2) provides thirty (30) days prior written notice to the Participating States before the cancellation or non-renewal, 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. 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. Service specific terms and conditions included in Attachment E will be provided to the Participate States at the time of procurement.

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 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

[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.

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 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.

Experian Data. The parties acknowledge and agree that the Services may include the delivery, access or use of (i) personal data or information that does or could be used to identify a consumer, (ii) credit data or data that is a consumer report as defined under the Fair Credit Reporting Act, as may be amended, (iii) data that has been furnished or otherwise provided by or on behalf of AGENCY to Experian and is included in Experian databases, and (iv) any other data or information related to consumers and/or businesses, in each case provided or made available by or on behalf of Experian to AGENCY (including, without limitation, business credit data and marketing data); and (v) any copies or derivatives of such data or information, whether or not such data or information is or could be linked back to an individual consumer (collectively, "Experian Data"). AGENCY represents and warrants that it shall not resell the Experian Data, and that it shall only access, receive and use the Experian Data in the manner explicitly permitted in a Statement of Work.

Retained Rights. AGENCY acknowledges that Experian has expended substantial time, effort and funds to develop, create, compile, provide and deliver the Services, Experian Data, Experian Confidential Information and various databases, improvements, technologies, inventions, developments, ideas, and discoveries associated therewith; all of which, when used in connection with the provision of, or access to, the Services shall be deemed part of the Services. AGENCY agrees that the Services, all data in Experian's databases and any other intellectual property that are part of the Services or related to the Services are owned by Experian (or its licensors or providers, as applicable). Nothing contained in the Agreement shall be deemed to convey to AGENCY or to any other party any ownership interest in or to any intellectual property or data provided in connection with the Services, Experian Data or Experian Confidential Information. AGENCY shall not acquire any license to use the Services, Experian Data or any Experian Confidential Information in excess of the scope and/or duration described in the Agreement.

Access and Use. AGENCY represents and warrants to Experian that it shall only access and use the Services and Experian Data for AGENCY's own internal business and solely in the manner explicitly permitted in the Agreement. AGENCY further agrees that it shall not, and shall not permit others (including but not limited to any affiliate or related companies and users) to, (i) change, modify, add code or otherwise alter the Services in any manner, (ii) reverse engineer, disassemble, decompile, in any way attempt to derive the source code of, or translate the Services, or (iii) use, transform, modify, or adapt the Services for use for any other purpose, including but not limited to use to assist in the

development or functioning of any product or service that is competitive, in part or in whole, with any existing or reasonably anticipate product or service of Experian.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	X	X	All

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: Experian Information Solutions, 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)

SaaS Minimum Discount % Off

Description	Discount
Account Opening Score (AO)	30.00%
Account Opening KIQ Only	20.00%
ID Screening Score (IDS)	58.00%
ID Screening KIQ Only	15.00%
Compliance (PID4C)	15.00%
Compliance with KIQ Only	15.00%
Business - Check	30.00%
Business - Check with Score	30.00%
Business - Account Opening Score	30.00%
Score Only (IEN Real Time)	10.00%
Score and Attribute (IEN Real Time)	10.00%
Neustar - MPIC Phone	30.00%
Neustar - MPIC Email	30.00%
Synthetic ID High Risk Fraud Score	30.00%
Telesign - One Time Password	30.00%
Credit Card Verification	30.00%
Emailage	30.00%
Fraud Net	30.00%
Digital Risk Score	30.00%
Average SaaS OEM Discount Off	**26.47%**

Additional Value Added Services

	Onsite Hourly Rate		Remote Hourly Rate	
Item Description	**NVP Price**	**Catalog Price**	**NVP Price**	**Catalog Price**
Maintenance Services (Support Services-Technicians and Engineers)-Remote Dispatch Engineer	See detailed prduct catalog	See detailed prduct catalog	See detailed prduct catalog	See detailed prduct catalog
Maintenance Services (Support Services-Technicians and Engineers)-Senior Solutions Engineer	See detailed prduct catalog	See detailed prduct catalog	See detailed prduct catalog	See detailed prduct catalog
Professional Services	See detailed prduct catalog	See detailed prduct catalog	See detailed prduct catalog	See detailed prduct catalog
Deployment Services-Service Technician	See detailed prduct catalog	See detailed prduct catalog	See detailed prduct catalog	See detailed prduct catalog
Deployment Services-Solutions Engineer	See detailed prduct catalog	See detailed prduct catalog	See detailed prduct catalog	See detailed prduct catalog
Integration Services, Project Manager or Business Analyst or Developer Analyst	See detailed prduct catalog	See detailed prduct catalog	See detailed prduct catalog	See detailed prduct catalog
Integration Services, Technical Architect (System or Data)	See detailed prduct catalog	See detailed prduct catalog	See detailed prduct catalog	See detailed prduct catalog
Consulting/Advisory Services, Consultant (includes Assessments)	See detailed prduct catalog	See detailed prduct catalog	See detailed prduct catalog	See detailed prduct catalog
Consulting/Advisory Services, Principal Consultant	See detailed prduct catalog	See detailed prduct catalog	See detailed prduct catalog	See detailed prduct catalog
Architectural Design Services	See detailed prduct catalog	See detailed prduct catalog	See detailed prduct catalog	See detailed prduct catalog

Attachment C - Pricing Discounts and Schedule

Contractor: Experian Information Solutions, Inc.

Statement of Work Services	See detailed prduct catalog	See detailed prduct catalog	See detailed prduct catalog	See detailed prduct catalog
Partner Services	See detailed prduct catalog	See detailed prduct catalog	See detailed prduct catalog	See detailed prduct catalog
Training Deployment Services	See detailed prduct catalog	See detailed prduct catalog	See detailed prduct catalog	See detailed prduct catalog
Professional Services - Project Coordinator	See detailed prduct catalog	See detailed prduct catalog	See detailed prduct catalog	See detailed prduct catalog
Professional Services - Project Manager	See detailed prduct catalog	See detailed prduct catalog	See detailed prduct catalog	See detailed prduct catalog
Professional Services - Strategic Project Manager	See detailed prduct catalog	See detailed prduct catalog	See detailed prduct catalog	See detailed prduct catalog

Deliverable Rates

NVP Price	**Catalog Price**
See detailed prduct catalog	

NASPO ValuePoint Master Agreement for Cloud Solutions (Redacted)

For: Utah Solicitation Number SK18008

Submitted by Experian

July 6, 2018

Table of contents

6.0 Technical response

This document should constitute the Offeror’s to the items described in Section 8 of the RFP, and must contain at least the following information:

a. **A complete narrative of the Offeror's assessment of the Cloud Solutions to be provided, the Offerors ability and approach, and the resources necessary to fulfill the requirements. This should demonstrate the Offeror's understanding of the desired overall performance expectations and clearly indicate any options or alternatives proposed.**

   Experian is providing Attachment J – Claim of Business Confidentiality Form in the PDF below.

CLAIM OF BUSINESS CONFIDENTIALITY

Pursuant to Utah Code Annotated, Subsections 63G-2-305(1) and (2), and in accordance with Section 63G-2-309, Experian Information Solutions (company name) asserts a claim of business confidentiality to protect the following information submitted as part of this solicitation. Pricing/Cost Proposals may not be classified as confidential or protected and will be considered public information. **An entire proposal cannot be identified as "PROTECTED", "CONFIDENTIAL" or "PROPRIETARY".**

- ☐ Non-public financial statements
- ☐ Specific employee name and contact information
- ☐ Specific customer information, client lists, or subscription lists
- ☒ Other (specify): proprietary

This claim is asserted because this information requires protection as it includes:

☒ trade secrets as defined in Utah Code Annotated Section 13-24-2 ("Trade secret" means information, including a formula, pattern, compilation, program, device, method, technique, or process, that: (a) derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use; and (b) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy).

☒ commercial information or non-individual financial information obtained from a person if: (a) disclosure of the information could reasonably be expected to result in unfair competitive injury to the person submitting the information or would impair the ability of the governmental entity to obtain necessary information in the future; [and] (b) the person submitting the information has a greater interest in prohibiting access than the public in obtaining access.

This statement of reasons supporting the claim of business confidentiality applies to the following information in this proposal:

Page	Paragraph	Reason
36	8.6.10	The graphic is a description of how our proprietary software is structured
62	8.12.13	The graphic is a desciption of our proprietary processes
T&C		The USPS requires this document to be confidential

Please use additional sheets if needed.

You will be notified if a record claimed to be protected herein under Utah Code Annotated § 63G-2-305(1) or (2) is classified public or if the governmental entity determines that the record should be released after weighing interests under Utah Code Annotated § 63G-2-201(5)(b) or Utah Code Annotated § 63G-2-401(6). See Utah Code Annotated § 63G-2-309.

Signed: Debbie Wynnychenko
On behalf of (company): Experian Information Solutions
Date: July 6, 2018

(Revision 6/4/2015)

Perhaps the most fundamental element of any governmental transaction is the identity of the individual interacting with the government agency. Experian® proposes a set of SaaS based services which will address the challenges and complexities of identity management in the age of modern digital service delivery for state governments across the country. Simply put, our mission is:

To help government organizations eliminate the presence of identity fraud in government programs and improve compliance and performance holistically while providing a seamless and expedient citizen experience.

Market forces and realities are creating complexities and risks which did not exist in simpler times. Dynamic and varying demographics across the country, citizen expectations for conducting transactions online, the delivery of ever increasing number and sophistication of transactions online along with the ever-growing number and scope of data breaches, inventive and persistent bad actors, and changes in the federal government identity management guidelines are some of the notable forces.

These factors impact e-government deployment efforts. Governments are seeking comprehensive identity management solutions from knowledgeable and trusted partners. Governments are seeking solutions based on open standards and platforms that are adaptable and extensible to meet emerging threats. The range of Experian solutions and services proposed is aimed to satisfy these market based requirements.

Our proposal details a set of solutions which address all the areas of our Identity Lifecycle Management approach. Our proposal includes the most comprehensive and advanced set of capabilities offered on the market today.

The staff assigned to our government focused organization are extremely experienced in working with clients and prospective clients is assessing their identity management requirements and evaluating the best methods to address those requirements. The team will then work with clients to develop the combination of our proposed services, help with advice

on configuration options and test these configurations. The average seniority of our client facing team is in excess of 15 years of government market experience. As a company we have decades of experience in applying analytic techniques to business challenges. Our analytic expertise ranges from model development and governance to data management.

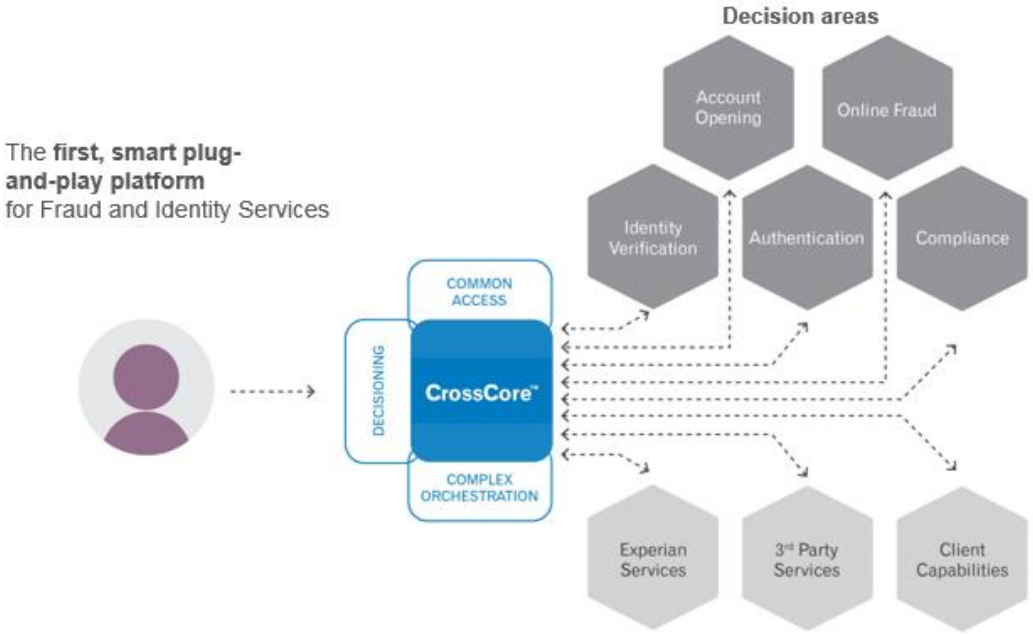
Our senior staff consists of our government sales and pre-sales teams, our customer support team and our implementation teams. The team can then avail themselves of the extraordinary resources in our Experian Advisory Services (EAS) organization for strategic and best practices guidance. The team also has at its disposal the considerable resources available in our product management and development organization. Lastly, but not at all least, our analytics team can help our clients review and assess the solution's performance statistics over time to optimize performance with respect to either technical performance or mitigation performance.

Our prospective clients also benefit from the wealth of knowledge and experience in our implementation team. This team continually assesses the best practices in place with existing installations. The team also maintains broad metrics which can be drawn upon to provide baseline input for configuration options.

Experian's solutions are implemented via our single API platform called CrossCore™. With this single, open platform, you can connect, access and orchestrate decisions across multiple systems efficiently and effectively. The flexible and scalable application program interface (API) combines powerful workflow and decisioning functions for your fraud and identity systems.

Figure 1. The first, smart plug-and-play platform for Fraud and Identity Services.

CrossCore™ helps to easily integrate with the fraud and ID products available from Experian, along with third-party and your capabilities. Rather than requiring individual setup for each application, CrossCore provides a single access and integration point for you.



Through a REST API, you can interact with multiple fraud and ID services available from Experian.

Listed below is a high-level illustration of the integration capabilities.

CrossCore™

Experian offers clients access to identity resolution, identity verification, account verification, robust behavioral analytics and document verification capabilities through our CrossCore platform.

In addition to providing a gateway to Experian owned data and proprietary analytical solutions, CrossCore incorporates optional partner vendor services to augment and future-proof the program. CrossCore's JSON API supports a RESTful web service integration that enables agency-specific workflow scenarios, a combination of data/service calls and decision management.

Experian's CrossCore platform was awarded by Javelin 'best overall identity proofing platform' for 2017 as measured across a field of 23 providers, and with specific focus on functionality, innovation, and flexibility.

Through CrossCore, services can be accessed independently, in tandem, or sequentially (when the results of one dictates a predetermined next step). In addition, CrossCore offers service and strategy monitoring, tuning, and flexibility to manage and respond to agency/program risks and constituent impacts.

Precise ID®

Experian's Precise ID® and FraudNet solutions maximize government agencies' ability to monitor identities over multiple dimensions such as time, geolocation, pattern of use, and attribute changes for indicators of potential fraud and provide that back to the agency as risk indicators.

This approach to Fraud Detection and Identification combines both identity and device centric evaluation of risk, and delivers actionable scores and supporting detail to ensure positive recognition of the vast user populations while isolating only those with substantive risk above an agreed upon threshold for further treatment.

We leverage Precise ID – our proprietary search and match engine leveraging billions of identity records across 20+ categorical data assets to derive:

- Identity element validation results across name, address, Social Security number, date of birth, phone number, email;
- Identity element verification to provide detailed levels of match between identity elements and categorical data assets;
- High risk conditional checks (e.g.: user victim statement on file, deceased or high risk address type conditions);
- Known fraud checks against aggregated records in Experian's National Fraud Database and searchable at the identity element level;
- Watch list screening (e.g. OFAC, PEP);
- Appended user's additional or associated addresses, phone numbers, dates of birth, Social Security numbers and household members.

Precise ID offers distinct fraud risk scores (each ranging from 1-999) along with supporting details in the form of score factor codes and attributes used to derive the scores. Score based decisions to approve or further treat or investigate identities are

transparently tuned to balance fraud detection with constituent impact and agency costs to handle potential fraud cases.

FraudNet

FraudNet provides a digital risk assessment to protect against user devices infected with malware, scripted attacks from botnets, man-in-the-middle attacks, and industrialized identity theft fraud. It determines level of risk for a device (mobile, desktop, tablet, etc.) being used to access an agency application during first-time registration and during login/authentication of existing users.

FraudNet uses a proprietary and patented process to capture and assess dozens of internal device characteristics that help identify the device as unique and assess the level of risk or trust based on the device's true geographic location, language preferences and other flags. FraudNet also captures consumer identity data asserted via the device along with the device-based information. A robust rules engine and user workstation allows agency fraud investigators to perform link analysis across their registered users and their associated device or devices.

Identity Element Network™

Experian's Identity Element Network™ (IEN) evaluates the use of the individual identity data elements presented upon input to determine where that same combination of identity elements is seen across the millions of inquiries processed daily by Experian. Experian processes over three million verification and credit inquiries each day from a variety of customers across the financial, automotive, telecom, retail, credit card and loan processing industries. This unique insight allows Experian to determine how the individual identity elements have been used previously, how often and across what timeframe, to generate an identity risk score and flags that will notify clients of the risk of identity theft and possible fraudulent use of the applicants' identity.

Digital Risk Score (DRS)

FraudNet invokes device printing, device attribute collection and risk assessment and identity associations that enable real-time risk assessment for online and mobile onboarding and authentication.

When fraud is detected, FraudNet enables the investigator to quickly identify other user registrations and access attempts linked to the fraudulently used device and/or identity. Experian provides agency specific decisions and strategies based on score and attribute (presence or absence) thresholds in combination or individually. This approach provides government agencies with the ability to standardize the tools and strategic approach while providing the flexibility to meet the needs of their programs and constituents.

BizID[SM]

Experian's BizID[SM] helps identify application anomalies that may indicate the presence of commercial fraud during client acquisition and account management phases of the client life cycle. BizID simplifies business and principal verification through superior data, analytics, and technology.

BizID leverages the following data sources:

- Business credit and demographic data with over 25 million active companies - all business data 3rd party verified and validated.
- Consumer demographic data (for business principal) with over 330 million records (including credit and non-credit sources, and proprietary databases) covering over 148 million households.

Specifically, these data sources form strong anti-fraud analytics such as:

- Greater breadth of data provides more accurate picture of applicant, leading to more predictive business, business principal, and combination fraud scores;
- Score-based analytics helps clients improve operational efficiency by prioritizing riskiest applicants for review and balance approval rates with fraud rates;

- Dedicated fraud analytics team with insight into best practices and strategy optimization.

b. A specific point-by-point response, in the order listed, to each requirement in the *Section 8 of the RFP*. Offerors should not provide links to a website as part of its response.

Offeror's should focus their proposals on the technical qualifications and capabilities described in the RFP. Offerors should not include sales brochures as part of their response.

Our technical response contains a complete narrative of our assessment of Cloud Solutions and a point-by-point response of RFP Section 8. Please see our response on the following pages.

8.0 Technical requirements

8.1 (M)(E) Technical requirements

8.1.1 For the purposes of the RFP, meeting the NIST essential characteristics is a primary concern. As such, describe how your proposed solution(s) meet the characteristics defined in NIST Special Publication 800-145.

The products and services we've proposed are pursuant to this RFP and meet all essential characteristics of NIST Special Publication 800-145 including:

- On-demand self-service – Experian services can be delivered completely on demand after an account is established and requisite contracts are signed related to contract participation, compliance onboarding and membership review processing.
- Broad network access – The complete complement of SaaS offerings are accessed through network services broadly in use throughout the Public Sector. They reside completely in the cloud and require no on premise hardware or software.
- Resource pooling – Resource pooling is an inherent quality of the solutions provided.
- Rapid elasticity – Solutions scale to virtually unlimited volume. The solutions use this elastic quality to accommodate client desires for flexible transaction processing.
- Measured service – Each service offered under this agreement is measured based on usage, typically on a per transaction basis.

- These characteristics are delivered to clients utilizing a SaaS model where the tools are accessed over the web, through batch processing, or via a single easily used API.

The Experian cloud infrastructure is predominately a Public Cloud where services across multiple clients access the same cloud based software. Each instance for client usage is custom configured to the client's own uses. Inquiry data and transactions across instances are isolated.

8.1.2 As applicable to an Offeror's proposal, Offeror must describe its willingness to comply with, the requirements of Attachments C & D.

The products and services (and related optional subcomponents) offered pursuant to this RFP are described at a high level in the following table and in complete detail in the Cost Proposal (not included here).

Product name	Options available	Modality	Service model
CrossCore	Yes	API	SaaS
Precise ID	Yes	Web UI, Batch or API	SaaS
FraudNet	Yes	Web UI, API	SaaS
Digital Risk Score	Yes	API	SaaS
BizID	Yes	Web UI, Batch or API	SaaS
Identity Element Network	Yes	Batch or API	SaaS

Each of these services meets the requirements (where applicable) described in Attachments C and D. We further recognize that the scope of this agreement unless modified in writing is always applicable, and commits to offering products and services that comply with these requirements going forward.

8.1.3 As applicable to an Offeror's proposal, Offeror must describe how its offerings adhere to the services, definitions, and deployment models identified in the Scope of Services, in Attachment D.

Experian meets the definition of a Cloud Based Service provider; we acquire and manage the computing infrastructure required for providing our services, run the cloud software that provides the services, and deliver the cloud services to cloud consumers through network access.

Further, the section of the Attachment D, related to Categorization of Risk is Low Data Risk.

Services and Models are discussed completely in our response to 8.1.1 related to NIST Special Publication 800-145.

8.2 (E) Subcontractors

8.2.1 Offerors must explain whether they intend to provide all cloud solutions directly or through the use of Subcontractors. Higher points may be earned by providing all services directly or by providing details of highly qualified Subcontractors; lower scores may be earned for failure to provide detailed plans for providing services or failure to provide detail regarding specific Subcontractors.

Any Subcontractor that an Offeror chooses to use in fulfilling the requirements of the RFP must also meet all Administrative, Business and Technical Requirements of the RFP, as applicable to the Solutions provided. Subcontractors do not need to comply with Section 6.3.

Experian intends to deliver all products and services under this contract directly to end user customers and does not intend to use subcontractor in the fulfillment of its contractual obligations.

Experian will use, based on requirements, some available third party data products to support this agreement. These providers are existing data partners of Experian and already provide data pursuant to agreements in existence before this solicitation was released. Clients will not be able to differentiate the experience when contracting for third party data products because they are all accessed through the same API.

These third-party data providers offer data in support of Identity and Fraud prevention beyond the core services provided by Experian. The combination of our quality data and additional data sources make this capability one of the premiere offerings in the marketplace.

8.2.2 Offeror must describe the extent to which it intends to use subcontractors to perform contract requirements. Include each position providing service and provide a

detailed description of how the subcontractors are anticipated to be involved under the Master Agreement.

Experian intends to complete all work required under this contract directly and does not intend to use subcontractors in the fulfillment of its contractual obligations. Sourcing some additional third party partner data products is used to improve the performance of our solutions. Contracts for this sourcing are already in existence as a part of Experian's partner business and the solution(s) provided is simply the data they offer to the Experian SaaS platforms.

8.2.3 If the subcontractor is known, provide the qualifications of the subcontractor to provide the services; if not, describe how you will guarantee selection of a subcontractor that meets the experience requirements of the RFP. Include a description of how the Offeror will ensure that all subcontractors and their employees will meet all Statement of Work requirements.

This section is not applicable based on our delivery method under this contract.

8.3 (E) Working with purchasing entities

8.3.1 Offeror must describe how it will work with Purchasing Entities before, during, and after a Data Breach, as defined in the Attachments and Exhibits. Include information such as:

- **Personnel who will be involved at various stages, include detail on how the Contract Manager in Section 7 will be involved;**
- **Response times;**
- **Processes and timelines;**
- **Methods of communication and assistance; and**
- **Other information vital to understanding the service you provide.**

The proposed Experian solutions will not use the inquiry input data for updating the Experian housed files. We will address the question from the standpoint of an unlikely breach of the Experian housed data.

Experian will, within 24 hours and to the extent permitted by law or law enforcement authorities, notify of any actual security intrusion or violation that will or could affect the Confidential Information.

In such notification, the notification will report on the nature of the incident, the estimated impact and investigative action taken or planned. To the extent permitted by law or law enforcement authorities, within 3 business days of the initial incident report, Experian will provide a written updated report that summarizes the results of the action and corrective or remedial action taken. Upon completion of the investigation and to the extent permitted by law or the law enforcement authorities a final written report will be provided, that gives a full accounting of the extent of the security intrusion or violation, a description of the confidential information affected, specific corrective or remedial action taken, and the information security impact.

8.3.2 Offeror must describe how it will not engage in nor permit its agents to push adware, software, or marketing not explicitly authorized by the Participating Entity or the Master Agreement.

Experian controls the entire ecosystem being proposed. Even when the source data, such as phone or email address data, is being provided by partner sources there is no relationship between the end customer and any partner data provider. As such there is no opportunity for the delivery of adware, software, or marketing that would be unwanted. Simply, there is no method in our products or services by which a third party could attempt to market inappropriately to an end user under this agreement. Experian does not use any adware, software or marketing material in the delivery of the services proposed.

8.3.3 Offeror must describe whether its application-hosting environments support a user test/staging environment that is identical to production.

Experian provides a complete test environment that is fully capable of ensuring that services are configured and tested before being used in a live environment. This is true regardless of whether services are accessed through a Web interface, a Batch Process or an integrated API.

8.3.4 Offeror must describe whether or not its computer applications and Web sites are accessible to people with disabilities, and must comply with Participating Entity accessibility policies and the Americans with Disability Act, as applicable.

To support the government’s commitment to meet accessibility requirements based on Section 508 of the Rehabilitation Act of 1973 (29 U.S.C. 794d), Experian works with government agencies to ensure that the delivery of our tools and services are performed and delivered in a manner that does not reduce the accessibility features and functionality of agency portals. Since

most application requests to Experian are Web services API calls, or call center calls from within the existing agency applications with no visibility by the citizen to an Experian's website, the Section 508 requirements for Web content and communications are typically met.

8.3.5 Offeror must describe whether or not its applications and content delivered through Web browsers are be accessible using current released versions of multiple browser platforms (such as Internet Explorer, Firefox, Chrome, and Safari) at a minimum.

Experian's Fraud & Identity applications are SaaS based solutions. The user interface, where applicable, supports current Web browsers that support TLS 1.2 and above encryption standards.

8.3.6 Offeror must describe how it will, prior to the execution of a Service Level Agreement, meet with the Purchasing Entity and cooperate and hold a meeting to determine whether any sensitive or personal information will be stored or used by the Offeror that is subject to any law, rule or regulation providing for specific compliance obligations.

Experian brings decades of experience in data compliance. As a highly regulated entity we have strict procedures for ensuring that data is used appropriately and that it is always protected. We will certainly be agreeable to a required meeting with each participating entity to insure they understand the compliance requirements before engagement with any of our products and services.

As part of our onboarding process, we process a Client Membership application to ensure we provide services to a legitimate business entity, to determine the applicable law and permissible use of the solution within the context of that law. Listed below is a sample of the on-boarding checklist.

- Review client roles and responsibilities
- Client Membership form submitted to membership for review
- Schedule solution and technical review
- Conduct solution review
- Technical solution review and project prep

- Conduct security and EWACS training

8.3.7 Offeror must describe any project schedule plans or work plans that Offerors use in implementing their Solutions with customers. Offerors should include timelines for developing, testing, and implementing Solutions for customers.

Each project is specific to client needs; deliverables and plans are updated with an estimated timeframe for completion of each task following exploratory discussions. Typical implementation timeframes for projects of a similar scope are 2-4 months. Our project delivery method consists of six phases, which typically begin within two weeks following contract signature. Where applicable the implementation will follow these phases below:

- Kick-off and analysis
- System Design
- Development and integration
- Testing and QA
- Implementation
- Production certification

Our typical project plan is as follows:

- Phase 1: Requirements and design
  - > Project kick-off
  - > Product demo
  - > Review proposed schedule
  - > Data requirements review
  - > Technical discussions on deploying the JSC and creating JSON messages Assemble Business
  - > Requirements Document (BRD) BRD Approval

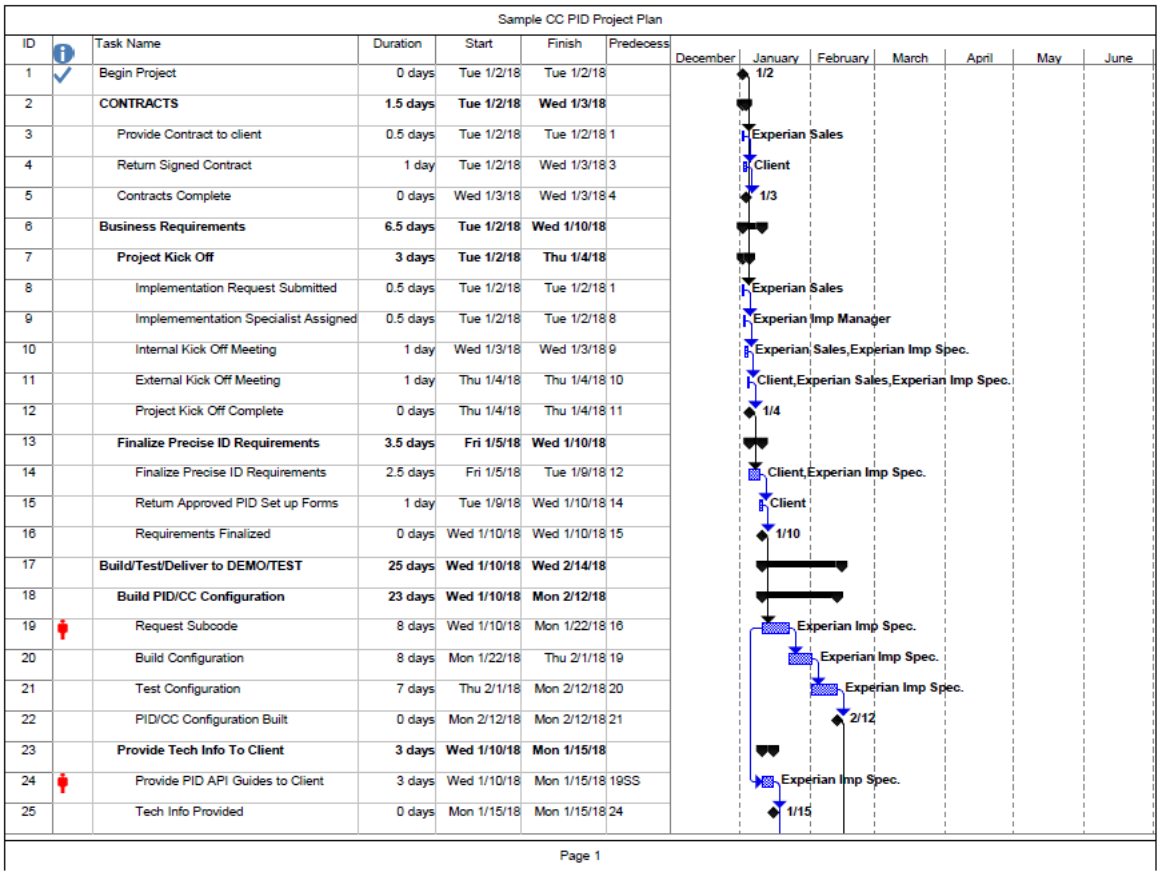
> Business/project stakeholders -Involves Project Manager, technical resources, etc., Developer who will create JSON messages and Web services process

- Phase 2: Configure and build
  > Environment provisioning and setup
  > Configuration per BRD
  > System integration
  > Input messages
  > Output messages
  > Chargeback file
  > Data transfer/Web services setup
  > Involves Project Manager, developer who will create JSON messages and Web services process
- Phase 3: Testing
  > Creation of test plan
  > SIT/user acceptance testing
  > Data transfer/Web services validation
  > Final testing certification
  > Involves Project Manager, testing team, technical resources, etc., Developer who will create JSON messages and Web services process
- Phase 4: Training fraud operations team
  > Provide onsite training
  > Provide shadowing (remote or onsite to be defined) of the clients team upon launch
  > Involves Project Manager, Fraud team
- Phase 5: Project launch and certification

- > Launch Product
- > Control and monitoring
- > Two to three-week certification period (where applicable)
- > Issue resolution
- > Business/project stakeholders
- > Involves Project Manager, Technical resources, etc. Developer who will create JSON messages and Web services process

- Phase 6: Project closure
  - > Project closure meeting
  - > Project acceptance Signoff
  - > Involves business/project stakeholders, Project Manager

Sample of CrossCore Precise ID Project Plan:



Sample CC PID Project Plan

ID	Task Name	Duration	Start	Finish	Predecess
1	Begin Project	0 days	Tue 1/2/18	Tue 1/2/18	
2	**CONTRACTS**	**1.5 days**	**Tue 1/2/18**	**Wed 1/3/18**	
3	Provide Contract to client	0.5 days	Tue 1/2/18	Tue 1/2/18	1
4	Return Signed Contract	1 day	Tue 1/2/18	Wed 1/3/18	3
5	Contracts Complete	0 days	Wed 1/3/18	Wed 1/3/18	4
6	**Business Requirements**	**6.5 days**	**Tue 1/2/18**	**Wed 1/10/18**	
7	**Project Kick Off**	**3 days**	**Tue 1/2/18**	**Thu 1/4/18**	
8	Implementation Request Submitted	0.5 days	Tue 1/2/18	Tue 1/2/18	1
9	Implemementation Specialist Assigned	0.5 days	Tue 1/2/18	Tue 1/2/18	8
10	Internal Kick Off Meeting	1 day	Wed 1/3/18	Wed 1/3/18	9
11	External Kick Off Meeting	1 day	Thu 1/4/18	Thu 1/4/18	10
12	Project Kick Off Complete	0 days	Thu 1/4/18	Thu 1/4/18	11
13	**Finalize Precise ID Requirements**	**3.5 days**	**Fri 1/5/18**	**Wed 1/10/18**	
14	Finalize Precise ID Requirements	2.5 days	Fri 1/5/18	Tue 1/9/18	12
15	Return Approved PID Set up Forms	1 day	Tue 1/9/18	Wed 1/10/18	14
16	Requirements Finalized	0 days	Wed 1/10/18	Wed 1/10/18	15
17	**Build/Test/Deliver to DEMO/TEST**	**25 days**	**Wed 1/10/18**	**Wed 2/14/18**	
18	**Build PID/CC Configuration**	**23 days**	**Wed 1/10/18**	**Mon 2/12/18**	
19	Request Subcode	8 days	Wed 1/10/18	Mon 1/22/18	16
20	Build Configuration	8 days	Mon 1/22/18	Thu 2/1/18	19
21	Test Configuration	7 days	Thu 2/1/18	Mon 2/12/18	20
22	PID/CC Configuration Built	0 days	Mon 2/12/18	Mon 2/12/18	21
23	**Provide Tech Info To Client**	**3 days**	**Wed 1/10/18**	**Mon 1/15/18**	
24	Provide PID API Guides to Client	3 days	Wed 1/10/18	Mon 1/15/18	19SS
25	Tech Info Provided	0 days	Mon 1/15/18	Mon 1/15/18	24

Page 1

8.3.8 The State of Utah expects Offeror to update the services periodically as technology changes. Offer must describe:

- **How Offeror's services during Service Line Additions and Updates pursuant to section 2.12 will continue to meet the requirements outlined therein.**
- **How Offeror will maintain discounts at the levels set forth in the contract.**
- **How Offeror will report to the Purchasing Entities, as needed, regarding changes in technology and make recommendations for service updates.**
- **How Offeror will provide transition support to any Purchasing Entity whose operations may be negatively impacted by the service change.**

In 2018, Forbes placed Experian on its top 100 most innovative company globally for the 5th consecutive year. While the products and services offered are among the best available, Experian is constantly innovated and expects to bring further value and innovation to this

important contract. Recent innovations based on client feedback, market conditions and R&D include our Synthetic ID suite, our version upgrade to the Precise Match functions and our CrossCore solution.

Experian has a long and significant history of performance on government contracts and we recognize that products and services we add to this contract through the process outlined in 2.12 must be fully compliant with mandatory minimums. We will have our contract management team review all additions for this compliance and through the annual recertification, ensure that all solutions remain consistent with stated mandatory minimums.

Pricing schedules and pricing tools are all maintained by Experian contract managers and will stay at the contracted levels. Our pricing tools have the requisite controls to ensure that quotes and orders are priced correctly and that pricing schedules are maintained as commercial pricing is modified over time.

Experian’s assigned contract manager will, from time to time, recommend updates or modifications to the scope of products and services so that the state purchasing entities can be assured the contract is always representative of the most recent products available in the market. Experian’s support organization will periodically issue client bulletin’s which outline changes or enhancements to offerings. Typically, our enhancements are made in a configurable manner to allow clients to select the timing of their use of a newer capability. There are cases where a change is made universally for all clients, for example infrastructure may be updated to further enhance our security protocols. Recently, Experian updated the security protocol used in our services to TLS 1.2. This change was made with significant notice and guidance to our clients along with testing recommendations and technical support in making the change.

In the unlikely event that a purchasing entity would be forced to migrate from one product to another, Experian would assign an implementation manager to insure the smooth migration and transition to the new product or service. This is rare, but should it happen these migrations have not proven difficult for our clients.

8.4 (E) Customer service

8.4.1 Offeror must describe how it will ensure excellent customer service is provided to Purchasing Entities. Include:

The staff assigned to our government focused organization are extremely experienced in working with clients and prospective clients is assessing their identity management requirements and evaluating the best methods to address those requirements. The team will then work with clients to develop the combination of our proposed services, help with advice on configuration options and test these configurations. The average seniority of our client facing team is more than 15 years of government market experience. As a company, we have decades of experience in applying analytic techniques to business challenges. Our analytic expertise ranges from model development and governance to data management.

Our government team is committed to your success. We work tirelessly and diligently to ensure that our client had access to all the best resources within the company. The company itself has a plethora of analytic, data management and identity management best practices, lessons learned and empirical information. We have been able to harness all this information and experience to our government client's benefit over many years of working with government agencies and programs.

Our senior staff consists of our government sales and pre-sales teams, our customer support team and our implementation teams. The team can then avail themselves of the extraordinary resources in our Experian Advisory Services (EAS) organization for strategic and best practices guidance. The team also has at its disposal the considerable resources available in our product management and development organization. Lastly, but not at all least, our analytics team can help our clients review and assess the solution's performance statistics over time to optimize performance with respect to either technical performance or mitigation performance.

Our prospective clients also benefit from the wealth of knowledge and experience in our implementation team. This team continually assesses the best practices in place with existing installations. The team also maintains broad metrics which can be drawn upon to provide baseline input for configuration options.

Described below are the customer service processes we have in place. These processes are supported with focused team members and a management staff focused on your complete satisfaction.

- **Quality assurance measures;**

  Experian has a well-designed quality assurance methodology the delivers specific benefits to the clients, such as an implementation that delivers business value rapidly as projects are delivered on time and on budget. To achieve these results, we perform the following quality control activities as part of every implementation project:

  - Unit testing ─ Tests the minimal software component or module. Each unit (basic component) of the software is tested to verify that the detailed design for the unit has been correctly implemented.
  - Integration testing ─ Exposes defects in the interfaces and interaction between integrated components (modules).
  - Functional testing ─ Tests a completely integrated system to verify that it meets its requirements.
  - System integration (end to end) testing ─ Verifies that a system is integrated to any external or third-party systems defined in the system requirements.
  - Stress testing ─ Deals with the quality of the application in the environment. The idea is to create an environment more demanding of the application than the application would experience under normal workloads.
  - User acceptance testing (UAT) ─ The objective of client's acceptance testing is to enable the client's authorized signatory to sign off the various Experian components being developed, as well as being delivered to the clients per the agreed specification documents.

  This process begins early in the project lifecycle as the planning for the quality assurance activities being in the analysis and design phase of the project. Our quality assurance

analysts build the quality assurance testing plan which will ensure that the system is fully tested to meet the functional requirements.

- **Escalation plan for addressing problems and/or complaints; and**

Escalation

Escalation of a support request can occur for many reasons, including, but not limited to:

- Timing
- Resources
- System constraints
- Client request

Following are the escalation steps within the Fraud & Identity Solutions team Level 2 support team:

Escalation step	Escalation contact
First	FS Support FSSupport@experian.com 877 863 2029
Second	Fraud & Identity Solutions Director of Client Services Shawna Dye shawna.dye@experian.com 714 830 5202
Third	Fraud & Identity Solutions General Manager

In the event a client wishes to escalate an unresolved problem, they can call FS Support and ask for the Client Services Director, who can escalate the priority of the ticket/problem accordingly.

Request closeout

Fraud & Identity Solutions Client Services will follow up with the client after a response has been provided. The request ticket will not be closed until the client expresses satisfaction with the results.

Fraud Solutions Bulletins

Fraud & Identity Solutions Client Services provides notification to fraud clients regarding various product and/or client support topics, including:

- Scheduled product releases
- Scheduled system/application maintenance
- Root Cause Analysis for major incidents
- Technical Documentation (API) updates
- Business continuity
- Emergency Problem Notification (EPN)

Clients may provide their email contact information to FS Support and be added to Fraud Solutions Bulletin distribution list.

- **Service Level Agreement (SLA).**

Experian warrants at least 99.5% System Availability for FraudNet, Digital Risk Score, Precise ID, IEN, BizID and CrossCore during each calendar month (e.g., the Hosted Service will not be unavailable to Customer more than 1 hour per month, excluding the Scheduled Maintenance and Emergency Maintenance).

8.4.2 Offeror must describe its ability to comply with the following customer service requirements:

a. You must have one lead representative for each entity that executes a Participating Addendum. Contact information shall be kept current.

b. Customer Service Representative(s) must be available by phone or email at a minimum, from 7AM to 6PM on Monday through Sunday for the applicable time zones.

c. Customer Service Representative will respond to inquiries within one business day.

d. You must provide design services for the applicable categories.

e. You must provide Installation Services for the applicable categories.

Experian will provide services consistent with each item listed above in section 8.4.2 a-e. In most cases, design services, should they be required, are offered as a part of a consulting arrangement and priced according the specific line items of the cost proposal. Installation / Implementation varies by product, is always available and these fees are outlined in the Cost Proposal. We will support the contract with a contract manager as described in our response to Section 7.0 of the RFP. During negotiations and prior to the go-live, our clients and prospective clients are supported by a sales and pre-sales organization to assist with understanding the offering's capabilities, design considerations and the onboarding process. This sales team covers a named geography and each individual sales person and will act as the lead representative for each respective entity. The coverage will be kept current and the Contract Manager will have the current list available.

The Fraud & Identity Solutions Client Services Team (FS Support) is a central, managed point of contact for post-production client accounts aiding with specific Fraud product-related questions, issues and incident management. The team is accountable for the resolution of requests and for meeting the needs of our clients on a timely basis, while maintaining the highest level of accuracy, integrity and professionalism.

The objectives of our team are to:

- Eliminate the need for clients to make multiple calls to find the right resource
- Provide answers to routine questions quickly
- Route issues as necessary to the appropriate support group(s), quickly and accurately
- Provide a point person to track and monitor the progress of the client issue
- Maintain a knowledge-base of Fraud product information for dissemination to clients

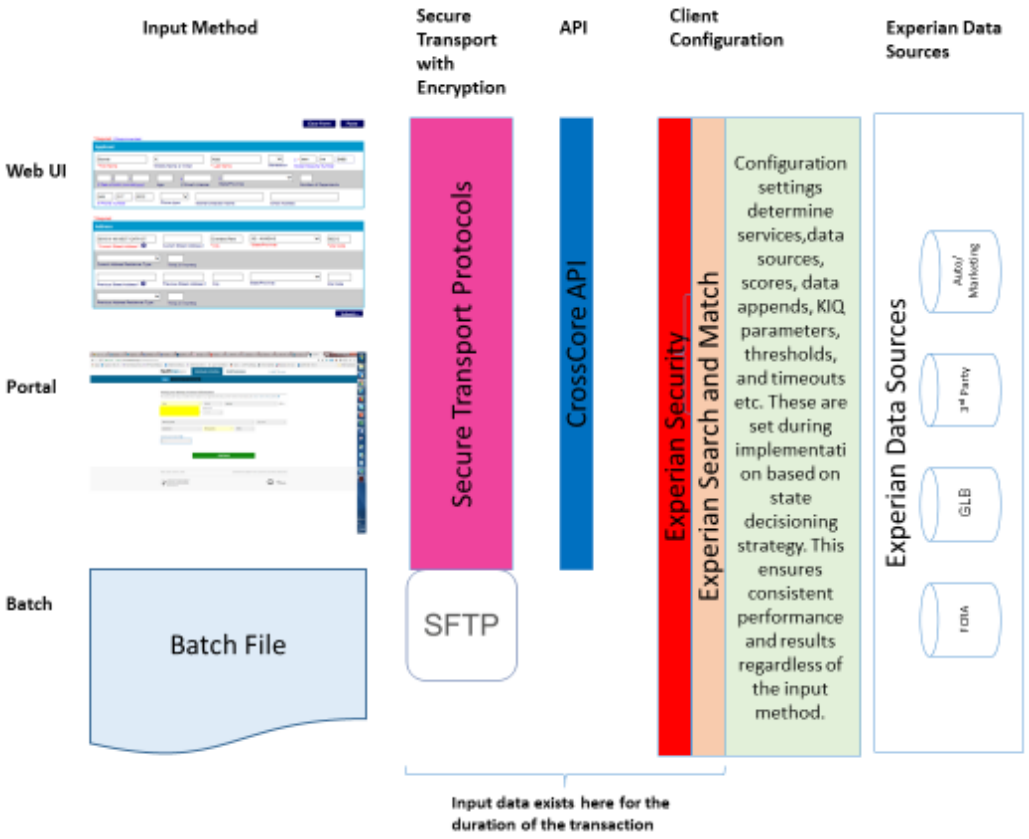
Our government clients are also supported by our team of account managers who are part of the sales team but focused on the operational performance of our existing clients. Our account managers have extensive government experience and act as a liaison between clients and our product or advisory services teams. Much of this work is focused on optimization potential based on historic performance metrics. However, this team will also act as an advocate for our clients in the event there are technical incidents which need additional attention.

In addition to the contract manager and lead representative, our clients are supported by a field support organization after the go-live for the specific implementation. During implementation, the client is supported by both the sales team and the implementation team. The implementation process is fully described above in section 8.3.7.

8.5 (E) Security of information

8.5.1 Offeror must describe the measures it takes to protect data. Include a description of the method by which you will hold, protect, and dispose of data following completion of any contract services.

Experian is providing solutions to NASPO under this agreement in the SaaS category and our products or services do not store any client data. As such, when services are terminated the instance of client tools are deleted, but there is not stored data to be removed. We use enterprise class encryption (see technical aspects of CAIQ) for any data in transit.



Input data is encrypted as it is transmitted to the Experian service. Input data is not persistent and exists only for the duration of the API session (for real-time) or returned to the client in the same secure manner (batch). Input data is used only for search/match purposes and is never stored by Experian.

Search/match functions use the provided input data to locate the appropriate matching record in the Experian repositories. Once matched, the repository data is used for risk assessment, scoring and other configured capabilities based on the client configuration. Additional Experian data attributes may be returned based on the client configuration and is returned in the same secure and encrypted manner.

8.5.2 Offeror must describe how it intends to comply with all applicable laws and related to data privacy and security.

Experian is a highly regulated Consumer Reporting Agency. As such, our procedures are regularly audited and verified compliant with all laws related to data privacy and security. We are keenly aware of and focused on the need for compliance with applicable laws. Performance under this contract would be no different.

Experian maintains steps in our onboarding process by which we ensure that the client's intended use of our data and services meet the applicable federal requirements. The specific law is based on the data and use case. Below are some examples.

- Fair Credit Reporting Act (FCRA) – 15 U.S.C. 1681 et. seq., as amended
- Graham-Leach-Bliley Act (GLB) – 15 U.S.C., Section 6801 et seq. (2000)
- Driver's Privacy and Protection Act of 1994 (DPPA) – 18 U.S.C. 2721
- The Electronic Signatures in Global and National Commerce Act (ESIGN) – 15 U.S.C. 96
- Standards for Safeguarding Customer Information – 16 CFR 314.4

We believe that as a regulated business with a rigorous onboarding process, we provide our clients with the highest level of assurance for compliance with laws. Experian maintains monitoring procedures which will alert our audit staff to activity which warrants further investigation with respect to compliance with applicable laws.

8.5.3 Offeror must describe how it will not access a Purchasing Entity's user accounts or data, except in the course of data center operations, response to service or technical issues, as required by the express terms of the Master Agreement, the applicable Participating Addendum, and/or the applicable Service Level Agreement.

The architecture of our products and services, whether accessed via the web, in batch or through an API does not enable Experian to access a Purchasing Entity's user accounts or data. Again, our solution does not store client data, but uses the input data for search/match functions which in turn support the appropriate decisioning process defined in the client's configuration.

User accounts are managed by the client's own staff. The onboarding process requires the client to name 'Head Designate(s)' who are responsible for creating, maintaining and monitoring user accounts. This is accomplished via the Experian Web Access Control Systems (EWACS).

8.6 (E) Privacy and security

8.6.1 Offeror must describe its commitment for its Solutions to comply with NIST, as defined in NIST Special Publication 800-145, and any other relevant industry standards, as it relates to the Scope of Services described in Attachment D, including supporting the different types of data that you may receive.

The products and services proposed by Experian pursuant to this RFP meet all essential characteristics of NIST Special Publication 800-145 including:

- On-demand self-service – Experian services can be delivered completely on demand after an account is established and requisite contracts are signed related to contract participation, compliance onboarding and membership review processing.
- Broad network access – The complete complement of SaaS offerings is accessed through network services broadly in use throughout the Public Sector. They reside completely in the cloud and require no on premise hardware or software.
- Resource pooling – Resource pooling is an inherent quality of the solutions provided.
- Rapid elasticity – Solutions scale to virtually unlimited volume. The solutions utilize this elastic quality to accommodate client desires for flexible transaction processing.
- Measured service – Each service offered under this agreement is measured based on usage, typically on a per transaction basis.

These characteristics are delivered to clients using a SaaS model where the tools are accessed over the web, through batch processing, or via a single easily used API.

The Experian cloud infrastructure is predominately a Public Cloud where services across multiple clients access the same cloud based software. The configuration for every instance for client usage is custom to the clients own uses and data and transactions across instances are isolated.

8.6.2 Offeror must list all government or standards organization security certifications it currently holds that apply specifically to the Offeror's proposal, as well as those in process at time of response. Specifically include HIPAA, FERPA, CJIS Security Policy, PCI Data Security Standards (DSS), IRS Publication 1075, FISMA, NIST 800-53, NIST SP 800-171, and FIPS 200 if they apply.

Experian adheres to a documented Global Security Policy modeled after ISO27001.

A list of certification maintained by Experian is listed below:

- ISO 270001
- PCI Compliance
- SOC2 Type II Compliance
- FICAM LOA 3 Recognition

8.6.3 Offeror must describe its security practices in place to secure data and applications, including threats from outside the service center as well as other customers co-located within the same service center.

Experian is not offering data or application hosting under the terms of this agreement. Further, with the exception of our Arizona facility, our facilities are not co-location facilities. Our security practices are fully detailed in other responses and our Cloud Assessments Initiative Questionnaire (CAIQ) document. Please see the CAIQ document for more detail.

The Arizona facility has multiple physical and logical partitions which prevent the access from other tenants.

8.6.4 Offeror must describe its data confidentiality standards and practices that are in place to ensure data confidentiality. This must include not only prevention of exposure to unauthorized personnel, but also managing and reviewing access that administrators have to stored data. Include information on your hardware policies (laptops, mobile etc).

Experian has instituted a company-wide program call Security First. Security First is an extensive training and process review program which has a core message that information security is the core of everything we do. Each and every employee is tasked to examine their own operational processes and ensure that security is considered first and foremost in conducting day to day operations. For our development teams, this means ensuring all

development fits the Experian security guidelines for authentication and data access. For our sales teams, it means we must treat each client interaction with an eye toward security. It means that our facilities team will consider physical access security as well as the security and well-being of our employees in all they do. The Security First program is an ongoing effort and will continue to evolve over time. Outlined below are some of the aspects of Security First, which we believe are of interest and responsive to the question above:

Protecting data

As a trusted steward of data, at Experian it is our responsibility to use and protect data properly, respect all the relevant laws, help evolve industry guidelines and new legislation, and ensure a culture of compliance with the highest standards of integrity.

People

Our information risk management and protection organization is led by a global chief information security officer and a team of information protection specialists, information technology experts, program managers, and legal and compliance advisors who are among the leaders in their field. Together, they implement processes and technology that allow for cost-effective protection of information while balancing risk and expense.

Our internal training capabilities allow us to continually develop, educate, and train our staff. Where legally permitted, we perform background checks on all individuals who have access to sensitive information. These checks may include criminal background checks, financial checks, and reviews of previous employment references. Upon hiring, each Experian representative signs proprietary information, non-disclosure, and invention agreements.

Experian ensures that appropriate separation of duties exists among the staff, including access to systems and networks. Access is granted to only approved individuals based upon business need. Duties are assigned in such a manner that a person does not have the opportunity to conceal their errors or irregularities.

Data

The importance of protecting data is embedded within the Experian culture. Executive and senior management actively participate in setting goals and promoting the data protection

program throughout the company. All staff including employees, consultants, contractors, and temporary workers are trained in how to properly classify the data they are collecting, storing or exchanging with business partners, clients, third-party service providers, or employees. Data classified as confidential or restricted is protected in a variety of ways that meet all applicable regulatory and industry requirements.

We take a managed approach to security to ensure that data is protected through the entire life cycle. During creation, transformation and use, storage, and destruction we deploy the latest techniques and processes to provide the best possible protection. To protect our clients, consumers, stakeholders, and Experian's corporate reputation, we monitor our systems to ensure high standards of data protection.

Network security and intrusion detection

We monitor inbound and outbound connections for signs of known threats and anomalous activity, and act based on identification of improper traffic. Firewalls and intrusion detection devices protect entrance to Experian's network. The internal network is divided into security zones providing additional layers of protection. Access to the production systems is granted on an as-needed basis and is monitored for any possible abuse or unauthorized users.

We protect our telecommunications system and any computer system or network device that is used to reduce the risk of infiltration and access penetration. We maintain state-of-the-art firewalls and provide general maintenance and monitoring of firewalls. We strictly monitor and approve all firewall rule set changes and provide monitoring of firewalls to identify attempted security violations.

Virus protection

Experian deploys, implements, and maintains the most current commercially available computer virus detection/scanning program. Our virus prevention architecture protects against the infection and spread of computer viruses between parties that access or exchange data or files through network connectivity.

Vulnerability and threat management

Our security operations group continuously scans our network and systems for vulnerabilities. We have security standards for configuration of our system devices that are maintained by our professional system administration staff.

Access control

Experian implements the latest measures to restrict electronic access to our systems to only authorized personnel who are subject to non-disclosure agreements for the protection of sensitive information. We ensure that all personnel who access or submit material to our systems are uniquely identified and authenticated. We enforce the principle of least privilege so that authorized personnel only have the level of access to our systems required to perform their job functions in providing services to them.

In addition to application, database, or operating system level access controls, we encrypt data (as required by regulation, our client contracts, and our corporate data protection policies) using strong, industry-standard encryption technology when not under the strict controls of our host systems.

Data integrity

Experian safeguards the confidentiality and integrity of all data being transmitted over our network. We implement and maintain strong, industry-standard encryption techniques to protect clients' data when transmitted over open networks.

Physical security

Experian's data centers are protected by a 24x7 manned security operation. Security officers patrol the site, ensure that all appropriate and established security measures are followed, and monitor and record closed circuit cameras. The cameras provide surveillance of the interior, parking lots, and all perimeter areas. Building access is controlled through an electronically coded magnetic-striped badge system. There are specific access levels controlling restricted areas that are approved only through senior management. Access to secured areas within our facilities, such as data centers and telecommunications areas, is restricted to authorized personnel on an as-needed basis. These areas are protected with entry controls such as video

surveillance, locks, magnetic swipe cards, proximity card readers, and biometrics readers. An audit trail of access is maintained and regularly reviewed.

Building and work site security

Our facilities use access control systems to protect main entrances, computer rooms, print centers, tape libraries, and general offices. The systems use a completely distributed database. All card information, time zone information, relay control information, and alarm point monitoring information is loaded into system memory. The unit is standalone, with no dependence on any other equipment.

Guard stations and a card reader entry system are located at entry points. Cards are required to enter internal areas. Permanent badges are issued to all employees and must be worn when on the premises. Visitors are required to sign in and are issued temporary badges.

Data centers

Only authorized personnel with magnetically encoded card key badges can enter the data centers. Card key locks, which are installed on all doors to the data center, are electronically activated based on insertion of a correctly coded card key badge. All card key badges are inventoried and controlled by operations management. Lost or stolen cards are reported immediately and, if necessary, all locks are re-coded and new badges are issued. All locks are changed and badges are reissued at intermittent intervals to complete the card/code security cycle.

Employee remote access

Remote access is provided on a limited basis to employees whose job functions warrant such access using strong, multi-factor authentication, and only then connected to Experian’s internal network.

8.6.5 Offeror must provide a detailed list of the third-party attestations, reports, security credentials (e.g., FedRamp High, FedRamp Moderate, etc.), and certifications relating to data security, integrity, and other controls.

A detailed list of certification is listed below:

- ISO 270001

- PCI Compliance
- SOC2 Type II Compliance
- FICAM LOA 3 Recognition

8.6.6 Offeror must describe its logging process including the types of services and devices logged; the event types logged; and the information fields. You should include detailed response on how you plan to maintain security certifications.

Activities to be logged include the following:

- Successful and failed authentication attempts (user authentication, application to system, system to system, database authentication)
- Failed resource access attempts (for critical objects)
- Account management (account creation, deletion, modification, individual and group accounts)
- Privilege changes or escalations
- Policy changes
- Object creation or modification, if not impacting performance (e.g. new user account type created by application, menu created/modified, database schema changes, file creation, deletion, etc.)
- System related events such as start and stop of daemons or services, critical jobs, invalid inputs, resource exhaustion, threshold exceeds, or other form of system, application or database abuse
- Updates to live program libraries (e.g. deploy file integrity monitoring to alert personnel to unauthorized modification of critical system or content files and perform critical file comparisons at a frequency commensurable to the system, application or data stored within)
- All activities performed by administrators, or accounts with special privileges (e.g. application administrator, application super user, system, database, and network administrators); and/or

- Network equipment event logs for syslog severity level errors, alerts, critical and emergency

8.6.7 Offeror must describe whether it can restrict visibility of cloud hosted data and documents to specific users or groups.

Experian does not “host” data as a part of its solutions. As to restricted visibility, each client instance exists completely and securely in its own environment and cannot gain access to any aspect of other users or groups of users’ profile or configuration data or account information.

8.6.8 Offeror must describe its notification process in the event of a security incident, including relating to timing, incident levels. Offeror should take into consideration that Purchasing Entities may have different notification requirements based on applicable laws and the categorization type of the data being processed or stored.

Experian will, within 24 hours and to the extent permitted by law or law enforcement authorities, notify of any actual security intrusion or violation that will or could affect the Confidential Information.

In such notification, the notification will report on the nature of the incident, the estimated impact and investigative action taken or planned. To the extent permitted by law or law enforcement authorities, within 3 business days of the initial incident report, Experian will provide a written updated report that summarizes the results of the action and corrective or remedial action taken. Upon completion of the investigation and to the extent permitted by law or the law enforcement authorities a final written report will be provided, that gives a full accounting of the extent of the security intrusion or violation, a description of the confidential information affected, specific corrective or remedial action taken, and the information security impact.

8.6.9 Offeror must describe and identify whether or not it has any security controls, both physical and virtual Zones of Control Architectures (ZOCA), used to isolate hosted servers.

Experian has both physical and logical security controls in place to protect our solutions. Listed below is a summary of the security controls. Attached to the RFP is a copy of Experian’s Information Security Overview for reference.

Allen/McKinney

- Physical security perimeters including fences, berms and barriers, walls, and gates safeguard access to facilities housing sensitive data and information systems.
- All doors at the data centers are control by card-key access. The facility is fully gated in.
- Security Guards and patrols monitor electronic surveillance systems, Physical security physical authentication mechanisms, reception desks guarding access to facilities housing sensitive data and information systems 24x7.
- ISO27001 certificate covers Allen and McKinney data centers.
- Physical and environmental controls in Allen and McKinney are similar.
- The computer equipment is located within the computer room inside the secured data center. Access to the computer room is controlled by biometric readers and card key access (MFA). Only employees who are assigned to support the business function are granted access. Requests for access must be approved by the security manager. Entitlement review is done quarterly. There are CCTVs installed in all entrances, major hallways, and inside the computer room. The security officers monitor the CCTV system 24x7.

Scottsdale, AZ

- This is a collocated data center operated by Sunguard.
- Controls in place include: Fire detection and suppression, redundant power sources, HVAC, card key and biometric access is utilized, and CCTV monitoring and recording.

8.6.10 Provide Security Technical Reference Architectures that support Infrastructure as a Service (IaaS), Software as a Service (SaaS) & Platform as a Service (PaaS).

The Security Technical Reference Architecture for Software as a Service (SaaS) in Section 7 Experian Confidential and Proprietary. Further security related information is available in the CAIQ attachment to this RFP.

8.6.11 Describe security procedures (background checks, foot printing logging, etc.) which are in place regarding Offeror's employees who have access to sensitive data.

At Experian, we believe our people are our most valuable asset. All new staff members participate in information security training and recertify their knowledge and understanding by taking an annual mandatory security course. All new staff members also go through background checks that include criminal and drug screenings and we verify education credentials and Social Security numbers.

Our standard background investigation includes verification of employment eligibility, verification of social security number, verification of previous employment, education verification, reference checking, drug testing, and a detailed seven-year criminal background check. Our background check policy is reviewed annually and updated as required.

All staff (employees, contractors, temps) must complete comprehensive information security training and testing (must score 80% minimum) and recertify annually. The process is monitored and tracked by the Experian Global Security Office (GSO).

Experian ensures that adequate separation of duties exists among the staff including access to systems and networks. Access is granted only to appropriate and approved individuals based upon business need. Duties are assigned in such a manner that a person does not have the opportunity to conceal his or her errors or irregularities.

Experian implements the latest measures to restrict electronic access to our clients' systems only to authorized personnel who are subject to nondisclosure agreements for the protection of client information. We ensure that all personnel who access or submit material to our clients' systems are uniquely identified and authenticated. We enforce the principle of "least privilege," namely, that authorized personnel only have the level of access to our clients' systems required to perform their job functions in providing services to them. Our application environment uses a three-tier network model for subscriber-facing servers and uses a two- or three-tier system for our application servers with a layered and redundant approach of firewalls and intrusion detection systems (IDS).

Experian maintains extensive logging functions to monitor access. This logging applies to both our client's (the State's) access and our own internal staff access to our own Experian data assets. Logging records the time/date, the user and the type of transaction executed. In

addition, certain transactions and access to Experian data assets are subject to active monitoring and investigation by Experian staff. These measures are focused on compliance with applicable laws and regulations as well as good security practices.

Experian’s data centers are protected by a 24/7 manned security operation. Our security officers monitor and record closed-circuit cameras 24/7. The cameras provide surveillance of the interior, parking lots and all perimeter areas. Building access is controlled through layers of electronic physical access control systems. There are specific access levels controlling restricted areas that are approved only through senior management. Access to secured areas such as computer rooms and telecommunication areas is restricted to authorized personnel on a need-to-access basis. These areas are protected with additional entry controls such as video surveillance, magnetic swipe cards, proximity-card readers and in some cases, biometrics readers. An audit trail of access to these restricted areas are maintained and regularly reviewed.

8.6.12 Describe the security measures and standards (i.e. NIST) which the Offeror has in place to secure the confidentiality of data at rest and in transit.

All data in-transit is encrypted using Transport Layer Security (TLS) version 1.2, Secure Socket Layers (SSLs), hardened security appliances (HSAs), and key management services (KMSs). This solution is consistent with National Institute of Standards and Technology (NIST) 800-57 recommendations and uses cryptographic algorithms approved by Federal Information Processing Standards (FIPS) 140-2.

The Batch access channel uses Experian's Secure Transport Serve (STS). STS is a Secure FTP file transfer mechanism designed to facilitate the exchange of data transmissions with Experian clients. STS is compatible with the following standard internet-based protocols: SFTP (SSH) and FTPS (SSL/TLS).

As stated previously in the response we are not storing client data therefore there is no data at rest. Data provided via API or batch is used only for search and match purposes and is either returned (batch) or expires with the API session.

8.6.13 Describe policies and procedures regarding notification to both the State and the Cardholders of a data breach, as defined in this RFP, and the mitigation of such a breach.

Experian will, within 24 hours and to the extent permitted by law or law enforcement authorities, notify of any actual security intrusion or violation that will or could affect the Confidential Information.

In such notification, the notification will report on the nature of the incident, the estimated impact and investigative action taken or planned. To the extent permitted by law or law enforcement authorities, within 3 business days of the initial incident report, Experian will provide a written updated report that summarizes the results of the action and corrective or remedial action taken. Upon completion of the investigation and to the extent permitted by law or the law enforcement authorities a final written report will be provided, that gives a full accounting of the extent of the security intrusion or violation, a description of the confidential information affected, specific corrective or remedial action taken, and the information security impact.

8.7 (E) Migration and redeployment plan

8.7.1 Offeror must describe how it manages the end of life activities of closing down a service to a Purchasing Entity and safely deprovisioning it before the Offeror is no longer contractually obligated to maintain the service, include planned and unplanned activities. An Offeror's response should include detail on how an Offeror maintains security of the data during this phase of an SLA, if the Offeror provides for redundancy during migration, and how portable the data is during migration.

Migration and redeployment for our services is simplified because we are a SaaS solution that doesn't store client information. Clients access our tools and information is passed back to the client or another cloud provider on behalf of the client. As such, when services are no longer desired the client can simply notify Experian, consistent with the terms of our agreement. At that time, the configuration of the environment will be removed and access to the online tools will be terminated. No client data is ever stored so migration to another provider and issues of data protection are out of scope for this solution.

8.7.2 Offeror must describe how it intends to provide an orderly return of data back to the Purchasing Entity, include any description in your SLA that describes the return of data to a customer.

Experian's solutions do not store client data. We process data in real time or batch and return scores, decisions and additional attributes to the client's application or a web UI. As such there would not be any data to return after termination of services.

8.8 (E) Service or data recovery

8.8.1 Describe how you would respond to the following situations; include any contingency plan or policy.

a. **Extended downtime.**

b. **Suffers an unrecoverable loss of data.**

c. **Offeror experiences a system failure.**

d. **Ability to recover and restore data within 4 business hours in the event of a severe system outage.**

e. **Describe your Recovery Point Objective (RPO) and Recovery Time Objective (RTO).**

Business Continuity program summary

Experian's Business Continuity and Disaster Recovery program is focused on the protection and recovery of our people, data centers and corporate offices, and safeguarding the interests of our clients. The program is based on the NFPA 1600 Standard and DRII industry best practices. Experian's Global Business Continuity Policy is updated regularly to meet changes in the organization's strategy and objectives. It addresses the following areas:

- Organization and management
- Responsibilities and planning
- Work area recovery
- IT disaster recovery
- Crisis management
- Awareness, exercising, and testing

Each business unit is required to maintain a comprehensive business continuity plan for all products and services. Plans are required to be updated and exercised at least annually or as material changes are made to the computing environment and/or software programs. Plans are reviewed and approved by the business line.

Business continuity program office

Business Continuity is administered by Experian's Business Continuity Program Office (BCPO). The BCPO is directed by the Risk Management Committee (RMC), which is comprised of Experian's senior management. The BCPO is staffed by a dedicated team of certified business continuity professionals called coordinators. Coordinators work with the business units to develop, implement, and maintain plans that are current, exercised and audited. Plans are stored in a central repository with secured access.

General disaster recovery client communications plan

Experian Evaluation Response Team (ERT), Site Response Team (SRT) and Regional Response Team (RRT) are responsible for the declaration of a business disaster based on information provided by the damage assessment team, our recovery coordination team, and the

BCP coordinator. Once a disaster has been declared, a toll-free client information number will be activated. Clients will be able to obtain general information about the operational status of an impacted Experian site in the event of an extended business interruption. The recorded message will provide the status of the initial damage assessment and the next update message time.

The Experian Americas Global Operations Center will contact our clients in accordance with set escalation procedures. A disaster will be viewed as severity level one. The Experian Americas Global Operations Center will then re-verify the client's disaster recovery coordinator contact, technical contact, and business contact name for future updates and recovery coordination activities. Individual client communication action plans that are part of Experian's business continuity plans will be activated at this time.

The Marketing Services client delivery group is the primary contact point for Marketing Services clients.

Experian will activate the disaster recovery command center within one hour of disaster declaration. Depending upon the location of the disaster, the disaster recovery command center will be located at one of the following locations:

- Allen command center – 601 Experian Parkway, Allen, Texas, Building A
- Experian Global Operations Center – Americas – 3400 Stonebridge Drive, McKinney, Texas
- Schaumburg command center – 955 American Lane, Schaumburg, Illinois
- 41st Parameter Data Center Operations – Decision Analytics

Recovery levels for the SunGard data center in Scottsdale Arizona are based on level of failure and recovery ability. While we would initially try to recover functionality onsite at the Scottsdale data center, we maintain a fully functional hot site of our customer hosted data center environment at our Equinix data center in Virginia for a full failover. Data recovery to a production state at the Virginia hot site would be recovered in order of customer SLA and RTO.

8.8.2 Describe your methodologies for the following backup and restore services:

a. Method of data backups

Disk to Disk

b. Method of server image backups

Server and database images are backed up/replicated to disk.

c. Digital location of backup storage (secondary storage, tape, etc.)

In an Experian owned Disaster Recovery facility

d. Alternate data center strategies for primary data centers within the continental United States.

Experian operates several data centers which are geographically dispersed across North America.

The data centers are robustly designed and have the following capability:

- Dedicated backup sites
- Two tier-1-Internet Services Providers (ISPs)
- 24-7 operations and monitoring by onsite staff
- 24-7 security patrol and surveillance monitoring
- Uninterrupted Power Supply (UPS) systems
- Dual utility/telephone feeds from different sources
- Onsite diesel power generation

8.9 (E) Data protection

8.9.1 Specify standard encryption technologies and options to protect sensitive data, depending on the particular service model that you intend to provide under this Master Agreement, while in transit or at rest.

All data in-transit is encrypted using Transport Layer Security (TLS) version 1.2, Secure Socket Layers (SSLs), hardened security appliances (HSAs), and key management services (KMSs).

This solution is consistent with National Institute of Standards and Technology (NIST) 800-57 recommendations and uses cryptographic algorithms approved by Federal Information Processing Standards (FIPS) 140-2. For encrypting data transmissions, we use algorithms and key sizes that provide at least the equivalent strength of AES-256.

The batch access channel uses Experian's Secure Transport Serve (STS). STS is a Secure FTP file transfer mechanism designed to facilitate the exchange of data transmissions with Experian clients. STS is compatible with the following standard internet-based protocols: SFTP (SSH) and FTPS (SSL/TLS).

As stated previously in the response, we are not storing client data therefore there is no data at rest. Data provided via API or batch is used only for search and match purposes and is either returned (batch) or expires with the API session.

8.9.2 Describe whether or not it is willing to sign relevant and applicable Business Associate Agreement or any other agreement that may be necessary to protect data with a Purchasing Entity.

Experian will negotiate with any Purchasing Entity on documents necessary to ensure both parties are clear on the data protection aspects of our business and will gladly discuss and negotiate in good faith with clients who are in the scope of this agreement.

8.9.3 Offeror must describe how it will only use data for purposes defined in the Master Agreement, participating addendum, or related service level agreement. Offeror shall not use the government data or government related data for any other purpose including but not limited to data mining. Offeror or its subcontractors shall not resell nor otherwise redistribute information gained from its access to the data received as a result of this RFP.

Experian is a highly regulated organization with some of the worlds most trusted data. We became one of the most trusted data companies in the world by honoring our commitment to our clients and the consumer. We never use consumer data without a permissible use under the law. Performance under this agreement would be no different. Experian has a rigorous compliance process supported by an empowered compliance department that protects consumer data from improper use.

We believe that as a regulated business with a rigorous onboarding process, we provide our clients with the highest level of assurance for compliance with laws. Experian maintains monitoring procedures which will alert our audit staff to activity which warrants further investigation with respect to compliance with applicable laws.

Experian maintains steps in our onboarding process by which we ensure that the client's intended use of our data and services meet the applicable federal requirements. The specific law is based on the data and use case. Below are some examples.

- Fair Credit Reporting Act (FCRA) – 15 U.S.C. 1681 et. seq., as amended
- Graham-Leach-Bliley Act (GLB) – 15 U.S.C., Section 6801 et seq. (2000)
- Driver's Privacy and Protection Act of 1994 (DPPA) – 18 U.S.C. 2721
- The Electronic Signatures in Global and National Commerce Act (ESIGN) – 15 U.S.C. 96
- Standards for Safeguarding Customer Information – 16 CFR 314.4

We believe that as a regulated business with a rigorous onboarding process, we provide our clients with the highest level of assurance for compliance with laws.

8.10 (E) Service level agreements

8.10.1 Offeror must describe whether your sample Service Level Agreement is negotiable. If not describe how it benefits purchasing entity's not to negotiate your Service Level Agreement.

Experian warrants at least 99.5% System Availability for FraudNet, Digital Risk Score, Precise ID, IEN, BizID and CrossCore during each calendar month (e.g., the Hosted Service will not be unavailable to Customer more than 1 hour per month, excluding the Scheduled Maintenance and Emergency Maintenance).

It has been our experience that the 99.5% system availability metric above suffices for nearly all clients employing the services outlined in this technical response. In some cases, we would be willing to negotiate an SLA should a State's needs be dramatically outside the norm.

8.10.2 Offeror, as part of its proposal, must provide a sample of its Service Level Agreement, which should define the performance and other operating parameters within which the infrastructure must operate to meet IT System and Purchasing Entity's requirements.

Where SLAs exist, each SLA is State-specific and is provisioned in the Master Services Agreement. The State can apportion the level of support required for maintenance of the system. Our system availability is warranted at 99.5%.

It has been our experience that the 99.5% system availability metric above suffices for nearly all clients employing the services outlined in this technical response. In some cases, we would negotiate a State SLA should a State's needs be dramatically outside the norm.

8.11 (E) Data disposal

Specify your data disposal procedures and policies and destruction confirmation process.

Experian does not persistently store client data, so there is not a requirement to destroy client data or confirm its destruction. Input data does not persist beyond the API session established to pass the input data to the Experian service for search/match functions.

8.12 (E) Performance measures and reporting

8.12.1 Describe your ability to guarantee reliability and uptime greater than 99.5%. Additional points will be awarded for 99.9% or greater availability.

Experian warrants at least 99.5% System Availability for FraudNet, Digital Risk Score, Precise ID, IEN, BizID and CrossCore during each calendar month (e.g., the Hosted Service will not be unavailable to State for more than 1 hour per month, excluding the Scheduled Maintenance and Emergency Maintenance).

8.12.2 Provide your standard uptime service and related Service Level Agreement (SLA) criteria.

Experian warrants at least 99.5% System Availability for FraudNet, Digital Risk Score, Precise ID, IEN, BizID and CrossCore during each calendar month (e.g., the Hosted Service will not be unavailable to State for more than 1 hour per month, excluding the Scheduled Maintenance and Emergency Maintenance).

When negotiated with States, Service Level Agreements (SLAs) determine the level of service in uptime percentage and response times, maintenance windows, escalation procedures, State notification, problem tracking, root cause analysis and other procedures. Listed below is the standard uptime service and Service Level Agreement criteria:

"System Availability" means the percentage of total time during which the Hosted Service is available to the State, excluding the Scheduled Maintenance Window, Emergency Maintenance, or any Force Majeure Event. Also excluded are: (a) use of the Hosted Service outside the scope described in the Agreement and the Documentation; (b) State Equipment and/or third party software, hardware or network infrastructure outside of Experian's data center and not under the direct control of Experian; (c) failure of State to meet the configuration requirements for State Equipment set forth in the Documentation; (d) failure of the external internet beyond Experian's network; (e) electrical or internet access disruptions not covered by Experian's disaster recovery plan, as amended from time to time, as further described in Section 3 ("Disaster Recovery");(f) any actions or inactions of State or any other third party not under the direct control of Experian; or (g) attacks (i.e. hacks, denial of service attacks, malicious introduction of viruses and disabling devices) caused by third parties provided Experian has used commercially reasonable efforts to prevent such attacks by means including implementation of a current version of a leading anti-virus application.

"Emergency Maintenance" means downtime of the Hosted Service outside of the Scheduled Maintenance Window hours that is required to complete the application of urgent patches or fixes, or to undertake other urgent maintenance activities. If Emergency Maintenance is required, Experian immediately contacts the State and provides the expected start time of the

Emergency Maintenance, its planned duration, and whether Experian expects the Hosted Service to be unavailable during the Emergency Maintenance.

"Scheduled Maintenance Window" means the window during which scheduled maintenance of the Hosted Service may be performed. The Scheduled Maintenance Window occurs on the first, second, and fourth Wednesday of each month between 10:00 PM and 12:00 AM (Mountain Standard Time) and on the third Wednesday of each month between 8:00 PM and 12:00 AM (Mountain Standard Time). In the event Experian expects the Scheduled Maintenance Window activity to result in the Hosted Service being unavailable to the State, Experian provides the State with a minimum of four business days advance notification. The notification includes the expected start time and duration of the Scheduled Maintenance Window activity.

8.12.3 Specify and provide the process to be used for the participating entity to call/contact you for support, who will be providing the support, and describe the basis of availability.

Fraud & Fraud & Identity Solutions Client Services

The Fraud & Identity Solutions Client Services Team (FS Support) is a central, managed point of contact for post-production client accounts aiding with specific Fraud product-related questions, issues and incident management. The team is accountable for the resolution of requests and for meeting the needs of our clients on a timely basis, while maintaining the highest level of accuracy, integrity and professionalism.

The objectives of our team are to:

- Eliminate the need for clients to make multiple calls to find the right resource
- Provide answers to routine questions quickly
- Route issues as necessary to the appropriate support group(s), quickly and accurately
- Provide a point person to track and monitor the progress of the client issue
- Maintain a knowledge-base of Fraud product information for dissemination to clients
- Provide feedback to the Fraud Solutions Team about problem areas and improvement opportunities

In meeting these objectives, the Fraud Solutions Client Services Team helps to minimize the time-to-resolution and maximize the productivity of our client.

Contact Information

Requests to the Fraud & Identity Solutions Client Services team can be made via telephone or email. Please note that high priority requests should be made by telephone to help ensure the timeliest response.

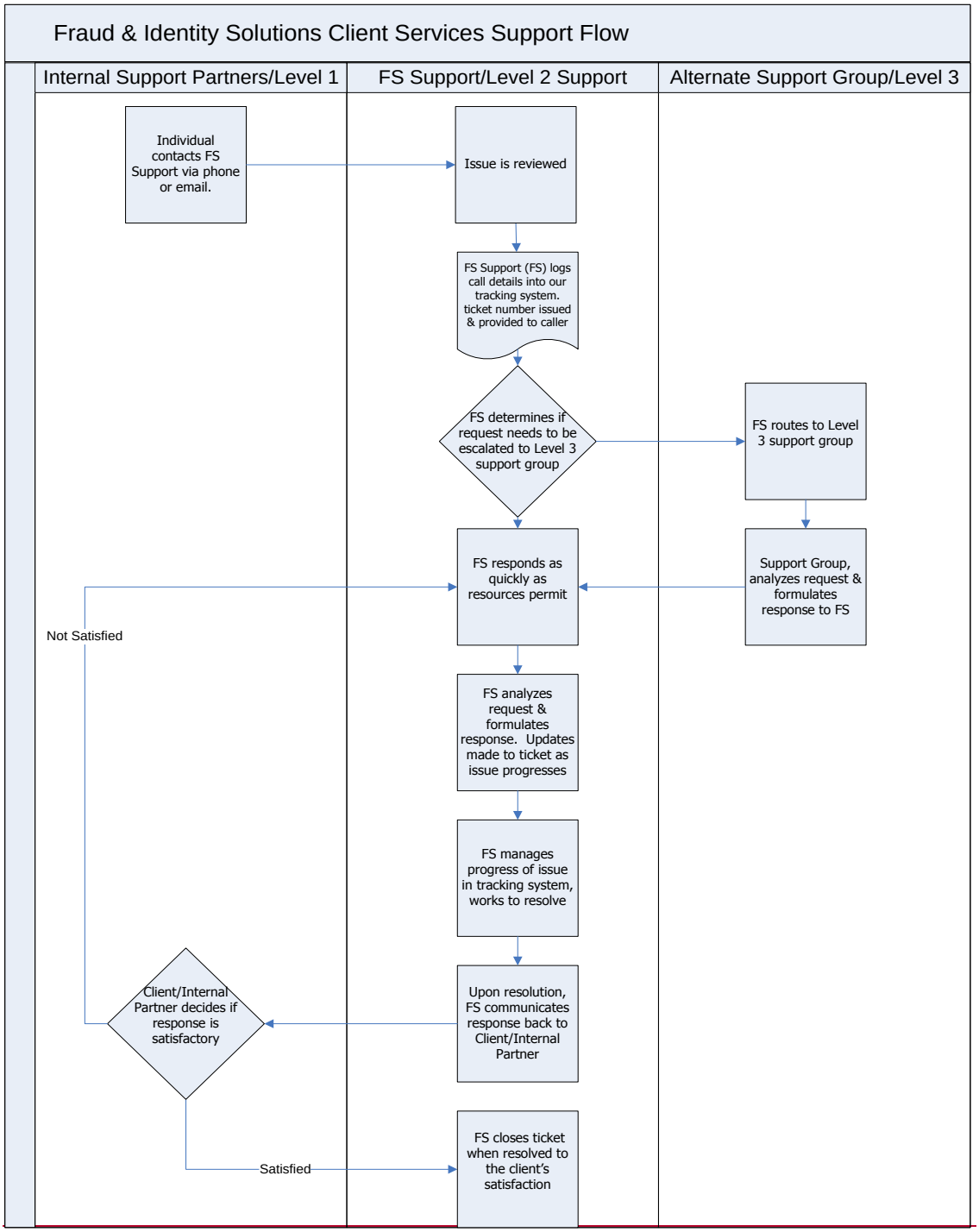
By email:

- To reach Fraud & Identity Solutions Client Services by email, send an email to **FSSupport@experian.com**, 24 hours a day. Please include any known information on the, “Initiating a Request”. Emails will be responded to during normal working hours, 6:00 AM PST – 5:00 PM PST, Monday through Friday, except national and company holidays. Emails received after hours will be responded to the following business day.

By phone:

- To reach Fraud & Identity Solutions Client Services by phone, please call toll free 877 863 2029, 24 hours a day.
- You may also call our direct number, 714 830 5262, to reach FS Support.
- Phones are answered by a Fraud & Identity Solutions Client Services support representative during normal working hours, 6:00 AM PST – 5:00 PM PST, Monday through Friday, except national and company holidays.
- During off hours, the calls roll over to our Experian Global Operations Center in Allen, Texas. The Experian Global Operations Center staff answers the calls and provides the necessary support.

The Experian Fraud Support Client Services Flow diagram in Section 7 Experian Confidential and Proprietary.


Fraud & Identity Solutions Client Services Support Flow
Internal Support Partners/Level 1
FS Support/Level 2 Support
Alternate Support Group/Level 3
Individual contacts FS Support via phone or email.
Issue is reviewed
FS Support (FS) logs call details into our tracking system. ticket number issued & provided to caller
FS determines if request needs to be escalated to Level 3 support group
FS routes to Level 3 support group
FS responds as quickly as resources permit
Support Group, analyzes request & formulates response to FS
Not Satisfied
FS analyzes request & formulates response. Updates made to ticket as issue progresses
FS manages progress of issue in tracking system, works to resolve
Client/Internal Partner decides if response is satisfactory
Upon resolution, FS communicates response back to Client/Internal Partner
Satisfied
FS closes ticket when resolved to the client's satisfaction

Problem Tracking and Management

Request tracking software and related tools are used for all request tickets. All incoming requests are logged and assigned a ticket number when the first contact with Fraud & Identity Solutions Client Services is initiated. The caller should record the ticket number as a reference for future calls on the same problem or for escalation of the problem. Once the ticket has been recorded, all subsequent progress on the request is recorded and tracked, including information gathering, forwarding to other support groups, escalation, and resolution, as applicable. All requests are tracked until resolved. Fraud & Identity Solutions Client Services maintains contact with the client until a request has been resolved to the client's satisfaction.

The ticket tracking system will be the system of record for all Fraud & Identity Solutions Client Services requests.

Support Groups

Level 1 support groups include:

- Technical Support Center, 800 854 7201
- Sales Support, 888 400 8989
- Field Support Reps
- Experian Global Operations Center (for after-hours support), 800 553 4785

Level 2 support group:

- Fraud & Identity Solutions Client Services (FS Support) 877 863 2029

Level 3 support groups include: (internal escalation from Level 2)

- Technical Sales Support Reps. (TSSRs)
- Product Managers (PMs)
- Technology team

Types of Requests

Types of Level 1 support requests include, but are not limited to:

- Desktop hardware/software inquiries
- Technical support issues
- PC related issues
- Login, ID & password issues/resets
- Connectivity issues

Types of Level 2 Support requests include, but are not limited to:

- Product functionality & use
- Product specific questions
- Product results & interpretation
- Ad hoc management reports
- System incident reports (SRRs)
- Research
- Root Cause Analysis
- Product documentation (APIs)
- Product Analysis

Types of Level 3 support requests include, but are not limited to:

- Issues that have not been resolved by Level 2 support
- Product enhancement requests
- Issues that require Development review
- Special client requests requiring TSSR engagement

Service Level Objectives for Level 2 support

Requests can vary significantly by type and level of severity. Requests are assigned a priority from 1 - 4 based on the extent of client impact:

Priority 1

- A business-critical functionality is down or there is a critical impact to the client's business operation. *Service Level Objective: Immediate to One hour*

Priority 2

- Operation of existing functionality is severely degraded or significant aspects of the client's business operation are negatively impacted. *Service Level Objective: One to Three hours*

Priority 3

- Operational performance of the product is degraded and/or there is a work around available. An issue exists, however, the cause, at this time is unknown. (Note that the priority may be adjusted as additional information becomes available.) *Service Level Objective: Within Twenty-four hours*

Priority 4

- Customer requires information or assistance on product capabilities, access and/or setup; however, there is little or no impact to the client's business operation. *Service Level Objective: One to Three days*

Initiating a Request

All requests for Level 2 support should include the following information, as applicable, whenever possible:

- Requester (User) name
- Client (Company) name
- Client Sub Code (for Precise ID and Biz ID)
- Which interface is the client using to access the product (*Web/access or XML via Net Connect*)

- What URL is the client using to access the product
- Audit Number
- Demo/Staging environment, Production environment, or a Pilot
- Is this an active implementation?
- Request summary, including symptoms, operating conditions, recent changes to client environment, etc.
- Date and time problem occurred
- Client impact, if known
- Troubleshooting already attempted / individuals' client has been working with
- Sample records/screen shots

Depending on the product involved, please include as much product-specific information as possible.

Escalation

Escalation of a support request can occur for many reasons, including, but not limited to:

- Timing
- Resources
- System constraints
- Client request

Following are the escalation steps within the Fraud & Identity Solutions team Level 2 support team:

Escalation step	Escalation contact
First	FS Support FSSupport@experian.com 877 863 2029
Second	Fraud & Identity Solutions Director of Client Services Shawna Dye shawna.dye@experian.com 714 830 5202
Third	Fraud & Identity Solutions General Manager

In the event a State wishes to escalate an unresolved problem, they can call FS Support and ask for the Client Services Director, who can escalate the priority of the ticket/problem accordingly.

Request closeout

Fraud & Identity Solutions Client Services follows up with the State after a response has been provided. The request ticket is not closed until the State expresses satisfaction with the results.

Fraud Solutions Bulletins

Fraud & Identity Solutions Client Services provides notification to the State regarding various product and/or client support topics, including:

- Scheduled product releases
- Scheduled system/application maintenance
- Root Cause Analysis for major incidents
- Technical Documentation (API) updates
- Business continuity
- Emergency Problem Notification (EPN)

The State may provide their email contact information to FS Support and be added to Fraud Solutions Bulletin distribution list.

8.12.4 Describe the consequences/SLA remedies if the Respondent fails to meet incident response time and incident fix time.

If an SLA is negotiated, Experian uses its' best efforts to meet or exceed its' SLA performance obligations. In all incident responses, we provide a Root Cause Analysis (RCA) of the problem which caused the incident. The nature of the services we offer and their delivery methods make them subject to impact by many possible factors. The RCA identifies the cause and the responsible party. Where Experian is the responsible party, we make commercially reasonable efforts to correct the cause of the issue and prevent its recurrence.

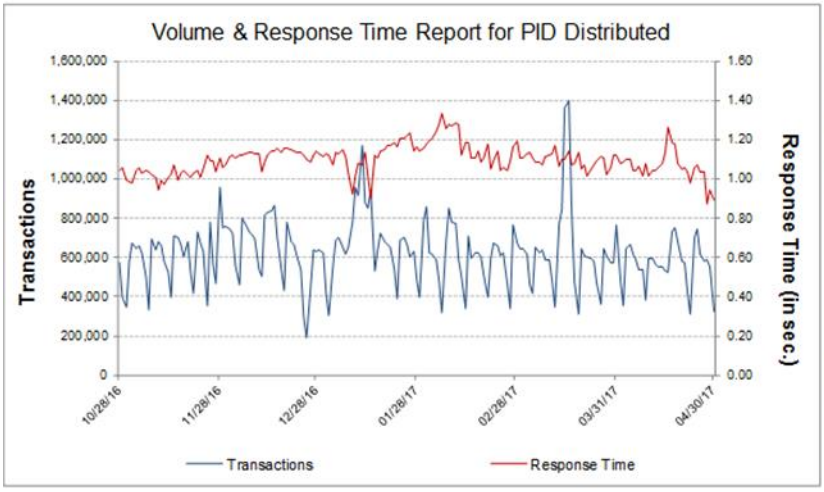
8.12.5 Describe the firm's procedures and schedules for any planned downtime.

Fraud & Identity Solutions Client Services provides notification to the State regarding various product and/or client support topics, including scheduled system/application maintenance. For planned downtime 30-day notice is provided, unless the downtime is for an emergency update in which case we provide as much notice as possible. The State may provide their email contact information to FS Support and be added to Fraud Solutions Bulletin distribution list.

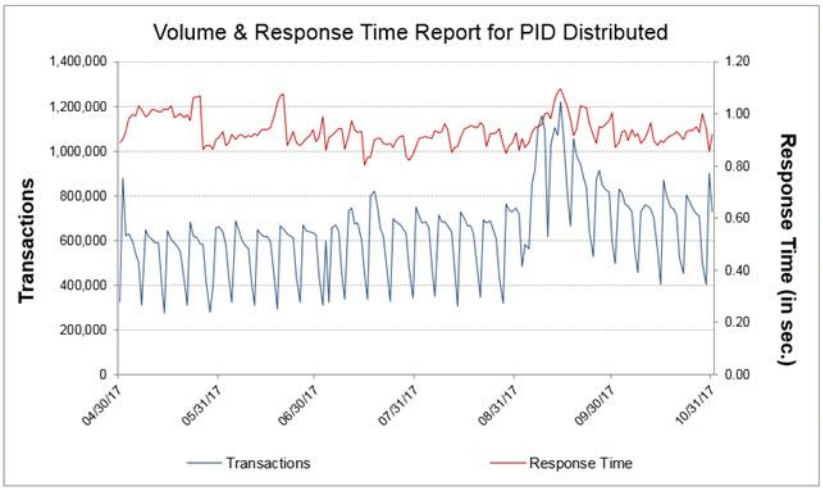
8.12.6 Describe the consequences/SLA remedies if disaster recovery metrics are not met.

Experian will negotiate specific SLAs with set goals for System Availability and Response times. Experian commits to Recovery Time Objectives (RTO) in the event of a disaster. However, it should be noted that all SLA remedies are for business as usual, we do not agree to remedies for disaster recovery.

8.12.7 Provide a sample of performance reports and specify if they are available over the Web and if they are real-time statistics or batch statistics.



Statistics for	April-2017
Total Transaction	16,890,793
Avg. Trans. per day	563,026
Avg. Resp. Time per day	1.057
Total Outage (in min.):	0
Total Outage (in %):	0.000%
Availability (in %):	100.000%



Statistics for	October-2017
Total Transaction	21,167,140
Avg. Trans. per day	682,811
Avg. Resp. Time per day	0.918
Total Outage (in min.):	15
Total Outage (in %):	0.034%
Availability (in %):	99.966%

All reports discussed in this response are available online in an ad-hoc manner and are real time when pulled. Standard reporting can also be scheduled for delivery to designated recipients at designated intervals.

Precise ID offers several types of real-time reporting. We offer a Web user interface for accessing reports/individual transactions submitted through Precise ID. Usage reports allow clients to immediately recall the results of any transactions submitted over the last six months for review of the transactions details. Citizens can search the transactions within the usage reports by several criteria of the consumer or submitter. Precise ID also offers periodic reporting

of basic result code counts and score distribution. The periodic reporting is delivered to the State via encrypted email on a weekly or monthly basis. Finally, a transaction level detail report is available to States who are not storing data themselves or prefer to receive this information via periodic report. Precise ID Reports are stored online for six months and then archived for seven years.

Experian also offers Performance Monitoring, which helps States perform periodic checks of scorecards or knowledge-based authentication while helping monitor the State's portfolio for population stability and decision management. Typically, this reporting involves a quarterly consulting service that provides insight to performance and trending quarter over quarter. Experian accepts client outcome data or fraud identifiers to perform a more robust performance review.

BizID[SM]

BizID[SM] archive reporting is available online via the Web user interface for 6 months, then offline for 7 years by submitting a request to the Fraud Support Team. Monthly BizID management reports are also available via e-mail to track and manage product usage. Each BizID product option provides management reports at the client level or the subcode level. Reports may be requested by administrative users and includes summary user ID usage, summary score distributions, and transactional details.

FraudNet

The FraudNet solution contains six standard reports including:

- System Level Hit Rate
- Out sort Summary
- Feedback by Payment Type
- Feedback by Reason Code
- Investigator Productivity Reference
- Rule Level Hit Rate

The FraudNet Solution offers the ability to create Custom Reports with flexibility to extract information from FraudNet that caters to your specific business needs.

8.12.8 Ability to print historical, statistical, and usage reports locally.

Experian provides a variety of summary reports that can be delivered by email or downloaded from a web portal as well as detail reports that are available as delimited files by either email or download. Reports are scheduled to run daily, weekly or monthly and can be run on an ad hoc basis by State's citizens from the web portal. Experian also offers custom reports, if required.

Precise ID

Precise ID offers several types of reporting. The usage reporting within the citizen interface allows States to immediately recall the results of any transactions submitted over the last six months for review of the transactions details. Users can search the transactions by several criteria of the consumer or submitter. Precise ID also offers periodic reporting of basic result code counts and score distribution, delivered via encrypted email on a weekly or monthly basis. Finally, a transaction level detail report is available to States who are not storing data themselves or prefer to receive this information via periodic report.

Precise ID/Knowledge IQ Performance Monitoring provides regular analysis and insight to your fraud risk management strategy. Our Knowledge-Based Authentication expert will conduct custom analysis on your portfolio with a consultative approach, offering the latest in best practice recommendations. While customization is available, standard areas of review include analyses in the areas of Volume Summary, Decision Matrix, Question Performance, Identity Verification, Shared Application Rules, Fraud Shield, and more. The Question Performance portion includes analysis of question selection, ordering, and weighting.

Clients are encouraged to prepare regular extracts of fraud performance data about these performance monitoring reports. This allows us to compare overall performance to that of the known fraud cases in each of the areas above, and is a valuable means of both evaluating the tool's performance and fine-tuning the configuration or overall risk strategy.

Whether or not fraud performance data are provided, regular reviews of the reports also allow for trending analysis and comparison to prior reporting periods. This allows for a bird's eye view of the tool's stability and performance over time. Periodic consulting also provides insights into

how recent product developments and functionalities can fit into your fraud prevention strategy to best meet your business needs.

For examples of our Precise ID reports please see attachment.

FraudNet

FraudNet offers standard reporting that allows users to analyze the efficacy of FraudNet, the risk models and the State's investigators. FraudNet standard reports are accessible via the FraudNet citizen Interface and can be executed and exported to a comma-separated value (CSV) file.

- Feedback by Payment Type – This report presents fraud information at the system level. The data can be filtered by organization, model, date range, payment type and reason code. The information is displayed in a table, and in graphic representations that make it easier to interpret the data. By using the Feedback by Payment Type report, Fraud Managers can gain an understanding of the current fraud levels and the potential risk of multiple parameters.
- Feedback by Reason Code – Using the confirmed fraud feature, investigators can record feedback on historical events using different reason codes. The Feedback by Reason Code report allows managers to look at Feedback by reason code to understand patterns and follow-up actions.
- Investigator Productivity – This report shows a wide range of investigator activity within FraudNet. The data can be filtered by organization, model, and amount by currency, and action date. It is used to review investigators' activities and performances, which lists count and amount information by action for each investigator. The report will list stats of each investigator side by side for easy comparison.
- Outsort Summary – This report is a summary of out sorted events based on action reason codes, models, and orgs as percent of count and amount compared to all out sorts and total events.

- Rule Level Hit Rate – This report is a measure of the individual performance of each rule within the risk engine. The data can be filtered by organization, model, model version, amount by currency and rule code.
- System Level Summary – This report shows hit rate information at the system level. The data can be filtered by organization, model, model version, amount by currency, event date and date range.

FraudNet offers custom reporting which provides the flexibility to extract information from FraudNet that caters to specific business needs. With more than 100 fields to include in criteria and the ability to use filters, States can create many different types of reports. FraudNet custom reports are accessible via the FraudNet user interface and can be executed and exported to a comma-separated value (CSV) file. Reports can be executed based on a defined schedule. Finally, Experian offers custom ad hoc reporting when standard reports, custom reports or a State's own in-house reports do not meet their FraudNet reporting needs. Our Customer Experience Manager can assist with the request, made through our ticketing system.

For examples of our FraudNet reports please see attachment.

BizID

BizID archive reporting is available online via the Web user interface for 6 months, then offline for 7 years by submitting a request to the Fraud Support Team. Monthly BizID management reports are also available via e-mail to track and manage product usage. Each BizID product option provides management reports at the State level or the subcode level. Reports may be requested by administrative users and includes summary user ID usage, summary score distributions, and transactional details.

For examples of our BizID reports please see attachment.

8.12.9 Offeror must describe whether or not its on-demand deployment is supported 24x365.

"On Demand Deployment" is available for all existing Client-States. New States will need to complete the on boarding process which will include any contract requirements by the Purchasing Entity as well as any contractual or compliance agreements that need to be

completed as a part of the desired products and services. For example, if a Purchasing Entity requires the use of data that is governed by the Fair Credit Reporting Act (FCRA) the entity must complete the appropriate onboarding documents. Once this is done and the services are made available then the deployment and access for citizens can scale up or down as the State desires. Once the State is onboarded, user administration functions are available through the EWACS environment at any time.

8.12.10 Offeror must describe its scale-up and scale-down, and whether it is available 24x365.

Our solution architecture is built to address varying volumes. As our configurable SaaS solutions are built to address a wide range of industries, we have taken an approach which allows for the environment to scale quickly and seamlessly without client intervention. Each industry or market segment has its own ‘seasonality’. We understand it is therefore imperative that the architecture be capable of this scaling flexibility to accommodate this factor. Our product and infrastructure teams meet on an ongoing basis to review the detailed monitoring metrics. The design is also managed with insight and knowledge of new clients coming on board that could drive large transaction volumes. All efforts are geared toward keeping the environment with extensive flexibility over time. The environment is available 24 X 365 excluding planned downtime.

On -Demand Deployment is available for all existing Client-States. New States will need to complete the on boarding process which will include any contract requirements by the Purchasing Entity as well as any contractual or compliance agreements that need to be completed as a part of the desired products and services. For example, if a Purchasing Entity requires the use of data that is governed by the Fair Credit Reporting Act (FCRA) the entity must complete the appropriate onboarding documents. Once this is done and the services are made available then the deployment can scale up or down as the State desires.

8.13 (E) Cloud security alliance

Describe and provide your level of disclosure with CSA Star Registry for each Solution offered.

a. Completion of a CSA STAR Self-Assessment. (3 points)

Experian has completed a CAIQ self-assessment including the submission of our CAIQ to the CSA STAR Registry and, as such we anticipate we have completed all necessary requirements for the maximum 3 points available.

b. Completion of Exhibits 1 and 2 to Attachment B. (3 points)

Experian has completed and provided the CAIQ Self-Assessment as a part of this RFP response, as such we anticipate receiving the 3 available points for this item.

c. Completion of a CSA STAR Attestation, Certification, or Assessment. (4 points)

d. Completion CSA STAR Continuous Monitoring. (5 points)

In addition, Experian is a Cloud Security Alliance (CSA) Corporate Member Add EDQ content from c. d. here and add first.

8.14 (E) Service provisioning

8.14. 1 Describe in detail how your firm processes emergency or rush services implementation requests by a Purchasing Entity.

We recognize that there are times when a Purchasing Entity may need accelerated onboarding to meet specific project deadlines or in support of important State initiatives. Each order of services is unique in complexity, size and scope. As such we can't make specific guarantees about rush services, but would, of course, work to make any implementation satisfactory for our client purchasing entities. We have worked with large and small clients to speed implementation and are happy to discuss and negotiate on an as needed basis.

The Experian field sales team (lead representative) works with the State to identify the emergency nature of the situation. The team alerts the implementation team and the onboarding team to the urgency of the situation. As needed, field sales management escalates the request. It is important to recognize that there are steps in the onboarding process entirely outside Experian's control and entirely within the State's control. We are therefore very dependent on the timely action on the client's part.

8.14.2 Describe in detail the standard lead-time for provisioning your Solutions.

Each project is specific to client needs; deliverables and plans are updated with an estimated timeframe for completion of each task following exploratory discussions. Typical implementation timeframes for projects of a similar scope are 2-4 months. Our project delivery method consists of six phases, which typically begin within two weeks following contract signature. Where applicable the implementation will follow these phases below:

- Kick-off and analysis
- System Design
- Development and integration
- Testing and QA
- Implementation
- Production certification

8.15 (E) Back up and disaster plan

8.15.1 Ability to apply legal retention periods and disposition by agency per purchasing entity policy and/or legal requirements.

Experian information is retained based on a master record retention schedule which is based on needs of business unit retention, legal and regulatory requirements. The master record retention schedule is approved and maintained by the applicable Regional Information Security Officer (RISO) and Information Steward.

8.15.2 Describe any known inherent disaster recovery risks and provide potential mitigation strategies.

Our Business Continuity Plan (BCP) office conducts annual business impact analysis reviews. The business impact analysis (BIA) review requires the business unit to consider factors such as permanent or long-term loss of a building, medium and short-term outages, loss of high-risk applications, external and internal dependencies, etc. in the recovery strategy to support the business unit BCP plans. Each BIA must be reviewed, approved and signed-off by the business unit management. Plans are updated at least every 12 months, but may be updated more

frequently as changes in environments/systems or applications occur. An overview of Business Continuity Program is being provided with this email/questionnaire.

8.15.3 Describe the infrastructure that supports multiple data centers within the United States, each of which supports redundancy, failover capability, and the ability to run large scale applications independently in case one data center is lost.

Data center operations in Texas are comprised of two sites: a primary site in McKinney, Texas, and secondary site in Allen, Texas. Experian owns and operates both these data center facilities. They are located away from potential earthquake faults, hurricanes, tidal waves and flood plains. These data centers have been designed to eliminate single points of failure while providing clients with both resilience and disaster recovery. There is private fiber-optic connectivity between the Allen and McKinney data centers to enable remote vaulting, database mirroring and disk file backups.

The McKinney facility was built to withstand winds of 175 mph, ice storms and other severe weather conditions. The building is below grade level, providing a bunker effect and has two roofs which provide continuous protection for the facility if the primary roof were to fail.

The McKinney data center has an independent, self-contained power plant. The site has its own diesel emergency generators and dual Uninterruptible Power Systems (UPS) to provide uninterrupted power.

The backup Command Center is in McKinney and is periodically tested by Command Center personnel. The primary and secondary data centers each have multiple routes of entry so that telecommunications carrier services can be brought into each building from diverse exchanges. In addition, cross-site bandwidth provides the ability for both sites to act as one routed network, providing continuous availability. Both the primary and secondary data centers have main carrier services from multiple providers. The primary and secondary data centers are connected by a resilient dark fiber network. This provides very high capacity between the two sites to allow the deployment of cross-site services.

The Allen data center facility can support and back up the McKinney data center facility, including power, air conditioning and floor space. Reliability —The Allen facility houses the Command Center, which supports both the McKinney and the Allen data centers

8.16 (E) Hosting and provisioning

8.16.1 Documented cloud hosting provisioning processes, and your defined/standard cloud provisioning stack.

Experian will not be offering “hosting” as a part of its products and services under this RFP. Our solutions fall into SaaS category and are specifically in Fraud Detection and Prevention as well as Remote Identity Proofing and Risk Analysis and Scoring.

8.16.2 Provide tool sets at minimum for:

1. **Deploying new servers (determining configuration for both stand alone or part of an existing server farm, etc.)**
2. **Creating and storing server images for future multiple deployments**
3. **Securing additional storage space**
4. **Monitoring tools for use by each jurisdiction’s authorized personnel – and this should ideally cover components of a public (respondent hosted) or hybrid cloud (including Participating entity resources).**

Experian’s SaaS solutions do not involve server deployment. This means that creating and storing server images is out of scope for our offerings. Lastly, all aspects of our SaaS offerings include the requisite storage and there would not be a need to secure additional storage.

As to 8.16.2 point 4, Experian provides a web portal for certain aspects of account management and provisioning through the EWACS capability described above. All clients who execute a contract for services will have access to the appropriate portal for management of their specific product and services set.

8.17 (E) Trial and testing periods (pre- and post-purchase)

8.17.1 Describe your testing and training periods that your offer for your service offerings.

Through a RESTful API and a single sign-on (SSO) portal interface, clients can interact with multiple fraud and ID services available from Experian. CrossCore provides a single point of connection for the numerous fraud and ID products within Experian and is data agnostic. With fraud strategies continually changing, a prompt response is difficult. CrossCore’s flexible JSON

API allows you to connect and adjust your fraud and identity services quickly through a single source. This open approach can help:

• Reduce time to market for new and enhanced strategies

• Easily test and trial new services

• Quickly adapt and respond to changing conditions

• Address new risks with the built-in strategy design and workflow capabilities

The objectives of the Experian solution are: - A frictionless customer experience - Improve risk assessment and reduce losses - Streamline processes and increase operational efficiency - Reduce drop-off rates and acquire more good customers

Project Plan

We have a highly disciplined and structured project and risk management approach to all implementations. We have a well-established methodology to define, document, monitor and manage all phases of the implementation.

Our first step in the project plan is an initial kick off conference call (usually 60 to 90 minutes in length) in which both sides do introductions, summarize the objectives, and then discuss and agree to the possible product configurations. Once agreed upon and signed off, we setup the product configuration per your specifications. Once the coding is complete, the IT staff on both sides will perform appropriate testing. Once completed and approved by you, the solution is ready for production.

Testing

Experian has a well-designed quality assurance methodology the delivers specific benefits to our clients, such as an implementation that delivers business value rapidly as projects are delivered on time and on budget. To achieve these results, we perform the following quality control activities as part of every implementation project:

- Unit testing - Tests the minimal software component or module. Each unit (basic component) of the software is tested to verify that the detailed design for the unit has been correctly implemented.
- Integration testing - Exposes defects in the interfaces and interaction between integrated components (modules).
- Functional testing - Tests a completely integrated system to verify that it meets its requirements.
- System integration (end to end) testing - Verifies that a system is integrated to any external or third-party systems defined in the system requirements.
- Stress testing - Deals with the quality of the application in the environment. The idea is to create an environment more demanding of the application than the application would experience under normal workloads.
- User acceptance testing (UAT) - The objective of the client's acceptance testing is to enable the client's authorized signatory to sign off the various Experian components being developed, as well as being delivered to the client per the agreed specification documents.

This process begins early in the project lifecycle as the planning for the quality assurance activities being in the analysis and design phase of the project. Our quality assurance analysts build the quality assurance testing plan which will ensure that the system is fully tested to meet the functional requirements.

Throughout the process, Experian proposes ongoing project status reviews at intervals agreed upon mutually. This will ensure key stakeholders and task owners have an opportunity to track to the Master Project Schedule. Additionally, this will assist in addressing any risks or issues and provide ongoing status. Milestones/key deliverables are documented and tracked throughout the process.

The approximate time frame for implementation of these services is 2-4 months. Implementation times vary based on expertise, resources and testing requirements from the client.

Training

Experian's representatives work with you on pre-and post-implementation and help support all ongoing training. They assist in helping develop "train the trainer" type programs so that you can provide internal training resources to new employees or refresher courses for existing employees. If formal onsite or Web trainings are required, Experian works directly with our clients to determine the most effective method given the audience, time constraints and locations.

8.17.2 Describe how you intend to provide a test and/or proof of concept environment for evaluation that verifies your ability to meet mandatory requirements.

Connectivity and integration testing is available for all the proposed Experian solutions. In addition and specific to Precise ID and BizID, Experian's Quality Assurance Analyst will provide Experian's STAR Test cases for the QA testing. The QA analyst is also responsible for smoke testing the solution when it is moved to UAT and production to ensure that the solution is performing to the requirements.

Experian's STAR Test Database was designed to provide a test facility that simulates the regulated Experian File One online production environment. We invested heavily in this testing facility to allow customers, vendors, and employees to test system access and verify software handling in an environment that is a replica of production. Experian's STAR Test Database includes:

- Over 200,000 dynamic test cases that perform as real consumers would in our production system.
- Over 20,000 tri-bureau test cases with the same identification data at each of the three bureaus.
- The ability to test virtually all Experian online products.
- Test data that meets virtually all data conditions that clients and vendors want to test. Experian can locate or create test data to meet a client's specific requirements.

STAR is available nearly 24/7 with a short downtime each night at 1:30 CST to refresh STAR’s Customer Master File.

8.17.3 Offeror must describe what training and support it provides at no additional cost.

Training

Experian's representatives work with you on pre-and post-implementation and help support all ongoing training. They assist in helping develop "train the trainer" type programs so that you can provide internal training resources to new employees or refresher courses for existing employees. If formal onsite or Web trainings are required, Experian works directly with the you to determine the most effective method given the audience, time constraints and locations. Training costs are included. Support

Please refer to Section 8.12.3 for a full description of Support Processes.

8.18 (E) Integration and customization

8.18.1 Describe how the Solutions you provide can be integrated to other complementary applications, and if you offer standard-based interface to enable additional integrations.

The Experian solutions proposed here are available via a well-documented Application Programming Interface (API). Experian's solutions are implemented via this single API platform called CrossCore. With this single, open platform, you can connect, access and orchestrate decisions across multiple systems efficiently and effectively. The flexible and scalable application program interface (API) combines powerful workflow and decisioning functions for your fraud and identity systems. Our approach will also let agencies and programs integrate their own data stores with the Experian IDLM solutions. The benefit of our integration approach is that the data remains at rest with the originating agency and does not have to be moved or replicated.

CrossCore helps to easily integrate with the Fraud and ID products available from Experian, along with third-party and your capabilities. Rather than requiring individual setup for each application, CrossCore provides a single access and integration point for you. Through a REST API, you can interact with multiple fraud and ID services available from Experian.

Listed below is a high-level illustration of the integration capabilities.

CrossCore

Experian offers clients access to identity resolution, identity verification, account verification, robust behavioral analytics and document verification capabilities through our CrossCore platform.

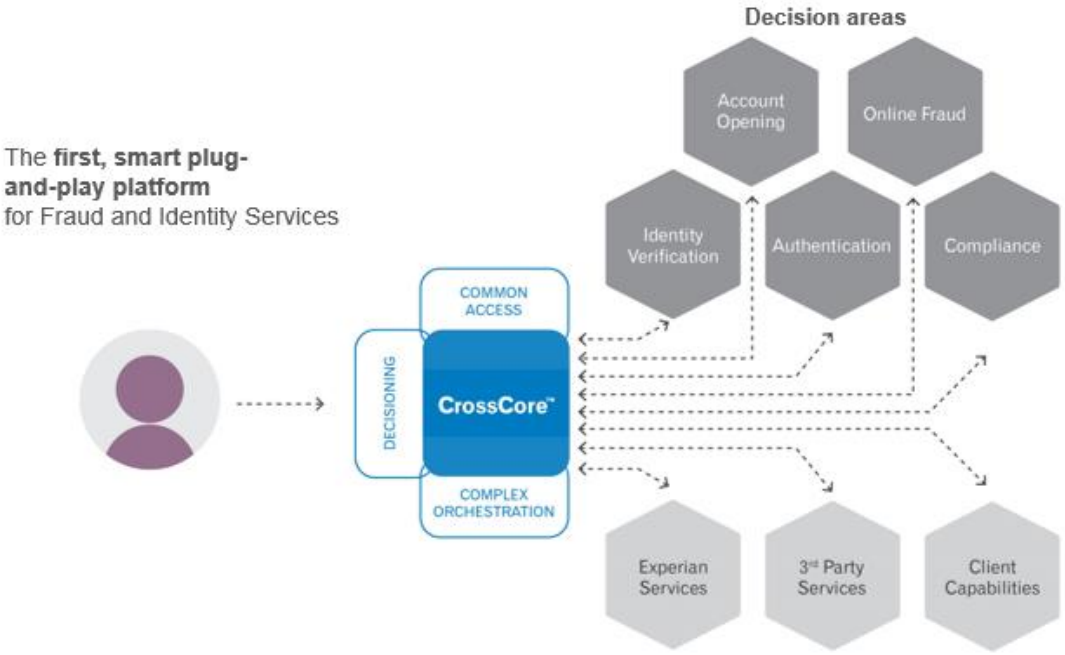


Figure X. The first, smart plug-and-play platform for Fraud and Identity Services.

In addition to providing a gateway to Experian owned data and proprietary analytical solutions, CrossCore incorporates optional partner vendor services to augment and future-proof the program. CrossCore's JSON API supports a RESTful web service integration that enables agency-specific workflow scenarios, a combination of data/service calls and decision management.

Experian's CrossCore platform was awarded by Javelin 'best overall identity proofing platform' for 2018 as measured across a field of 23 providers, and with focus on functionality, innovation, and flexibility.

Through CrossCore, these services can be accessed independently, in tandem, or sequentially (when the results of one dictates a predetermined next step). In addition, CrossCore offers

service and strategy monitoring, tuning, and flexibility to manage and respond to agency/program risks and constituent impacts.

8.18.2 Describe the ways to customize and personalize the Solutions you provide to meet the needs of specific Purchasing Entities.

Experian's Fraud Team offers the full breath of fraud and identity focused solutions across the entire customer life cycle. Using knowledge gained with over two decades of service to the private and public sector, we provide operational and thought leadership in data, analytics and technology. In turn, you can depend on our consultative approach to design, implement and support fraud detection analytics, authentication and device identity services. The key to our success is the depth and breadth of our data assets, with unmatched scalability of any other international company, as well as our commitment to continual evolution of tools to stay ahead of fraudsters.

Experian's solutions are highly configurable and customizable; we start by initiating a Kick Off call to understand the scope of the requirements and walk thru the set-up process. For example, Experian's Knowledge IQ verification process leverages the Precise ID score and a combination of the number and type of questions answered successfully to pass or refer citizens. Questions are developed to present five (5) available answers in multiple-choice format. We also employ several question-sequencing methods that randomize the question presentation to the citizen. You can also group questions into customized categories (e.g. demographic, employment, vehicle, etc.) and present them in category sequence or by random category delivery, allowing you the flexibility of configuring question presentation without requiring custom coding. In addition, you can also choose to use progressive questioning where pass/fail is determined by additive weighted value only vs. weighted percent correct. Use limits and global exclusion for each Q&A session can be set up. As part of our knowledge-based authentication practice, we engage in regular performance reviews of all questions in the active question set.

For customizations and personalized solutions, we work with our Decision Scientist to perform an analytical review of the data you provide. We engage our Expert Consultants to provide best practices and customization recommendations that fit the needs of each specific purchasing entities. We begin with understanding your needs, and engage with our Data Scientist to review and model the data and use case. We work closely with you and our Expert Consultants to determine the best model fit for your needs.

8.19 (E) Marketing plan

Describe your how you intend to market your Solutions to NASPO ValuePoint and Participating Entities.

Should Experian be successful in obtaining an award under this solicitation we intend to aggressively market our capabilities to Participating Entities and NASPO. In doing so we will develop a complete marketing plan that will include target agencies within each state. Our services are highly sought after in areas of Tax and Revenue, Unemployment Insurance, Health and Social Services among others. Each use case has an Experian developed value proposition and recommended tools and deployment methods that states can easily adopt by the nature of their availability on a broad procurement vehicle such as a NASPO ValuePoint contract.

Tactically we use a significant number of electronic marketing methods to reach prospective clients. Webinars, targeted email campaigns and follow up voice communication are typically employed. We do, however, recognize and respect the mission of State agencies and sub-agencies and do NOT engage in any marketing activity that would reflect poorly on Experian or its contract partners such as NASPO.

In addition to electronic medium, we attend many Association events annually where NASPO would become a core element. For example, we attend events hosted by the National Association of State Workforce Administrators, Federation of Tax Administrators and the National Association of State Treasurers. There are many others, and they do change over time, but we would anticipate our position as a NASPO contract holder to become a part of these types of events.

Our overall goal is to reach as many States and Participating Entities as possible, so there will be an initial focus on contacting state procurement offices to address contract usage and make these valuable services available as quickly as possible.

We are also willing to participate in events or activities that NASPO sponsors or encourages to support the overall mission of NASPO.

8.20 (E) Related value-added services to cloud solutions

Describe the valued-added services that you can provide as part of an awarded contract, e.g. consulting services pre- and post- implementation. Offerors may detail professional services in the RFP limited to assisting offering activities with initial setup, training and access to the services.

The Experian Advisory Services (EAS)Practice is dedicated to creating measurable and sustainable value for organizations around the globe. This group, comprising 40 industry business leaders, has deep knowledge of data, analytics and software and a full understanding of credit management principles and practices to best address governments' needs. Our consultants specialize in analytics-based decision strategies, data-driven problem solving, regulatory compliance and fraud risk-management programs to better solve complex business challenges and enhance agencies' constituent services. Experian uniquely understands the local markets we serve. We draw upon our global network of business consultants to bring a vast amount of market, industry, product and operational expertise to meet our clients' needs locally. Regardless of size or type of agency, we have developed a reputation of confidence and trust among clients, and our global consultants are versed at working with all functional levels of an organization — from agency directors striving to meet stakeholder expectations to business line management focused on implementing process change that directly impacts governments' success.

Experian's consultants are former business leaders and tenured advisers with years of operational experience and industry expertise. Having overcome many of the same challenges facing clients today, these consultants have practical, real-world experience combined with the global best practices, business acumen and competencies for deep problem-solving and communication.

This experience allows our consultants to:

- Holistically assess a challenge or an opportunity
- Identify the root cause or drivers
- Recommend a fact-based approach to improving strategies

8.21 (E) Supporting infrastructure

8.21.1 Describe what infrastructure is required by the Purchasing Entity to support your Solutions or deployment models.

The proposed Experian identity management solutions are designed to seamlessly integrate with existing client infrastructure such as applications or portals. To access our services through the Experian provided API, the client would need to have programming logic with which to integrate and call the Experian service API. The API is designed to handle expected input parameters and provide back to the client environment defined and expected returns via the API. The client would then be responsible for handling the returned information whether that is a score, decision or data attribute. All of this is contemplated in the API design. Experian staff will work with our clients to assist with understanding and leveraging the API fully.

Clients are responsible for maintaining their citizen facing systems and infrastructure. We provide an API and batch process that can be integrated into these systems. Once these interfaces are active, Identity and Fraud inquiries can flow to and from Experian. The entire service is owned and maintained by Experian with data elements, scores and other components returned via the API or in Batch. So, in short, to deploy our entire stack of products and services clients need the ability to integrate an RESTful API into existing Purchasing Entity tools.

Due to the nature of the solution, no requirements are imposed on our clients to install any hardware or software to use the solutions except for:

- FraudNet (Device Evaluation) - Installation of a Java Script Collector (JSC) or Software Development Kit (SDK) of which both technologies are provided to you by Experian.
- Outside of above exceptions, you will not be required to install any software.

8.21.2 If required, who will be responsible for installation of new infrastructure and who will incur those costs?

Generally, Experian does not anticipate the installation of any new infrastructure in the performance of any subsequent award under this RFP. Experian assumes the responsibility for enhancing, maintaining and documenting the applicable APIs. We ask the State to assume the responsibility to stay current with the API with the assistance of the Experian support staff.

It should be noted that in the situation where the proposed identity management services are used via the Experian provided Web UI in a call center environment, call recording capabilities will be needed to obtain and record the citizen’s consent as required for the FCRA compliant identity management service. In the event, there is no call recording available, it will need to be instituted to use this product option and would be provided at the State’s expense.

Contact information

Should you have any questions please contact:

Bradley Uhlenhoff

Solutions Consultant - Decision Analytics

Experian Information Solutions, Inc.

Phone: 208 249 2288

Email: bradley.uhlenhoff@experian.com

Attachment E – Service Offering EULAs, SLAs

EXPERIAN
STANDARD TERMS AND CONDITIONS

This Standard Terms and Conditions ("STAC") is made on the Effective Date set forth below between **Experian Information Solutions, Inc.** ("Experian") and **[INSERT CLIENT NAME]** ("Client").

1. Agreement. The STAC contain the standard terms and conditions applicable to Experian's provision of products and services (collectively, the "Services") to Client. Terms and conditions specific to the Services ordered by Client are set forth in individual schedules signed by Client and the applicable Experian entity offering the Services (each, a "Schedule"). The STAC, together with the Schedules, and any other documents incorporated or referenced in a Schedule, constitute the "Agreement." In the event of any conflicting or inconsistent terms, the following order of precedence applies with respect to the Services offered pursuant to a Schedule: (a) the terms and conditions in a Schedule solely with respect to the Service offered pursuant to such Schedule, and (b) the STAC. The use of the term "days" shall mean "calendar days" unless otherwise specified.

2. Fees and Payment. Client shall pay Experian for the Services in the amounts agreed upon in writing and set forth in the applicable Schedule or other mutually agreed pricing document. Unless otherwise provided in the applicable Schedule or pricing document, Experian shall have the right to revise or amend the pricing by providing thirty (30) days' prior written notice to Client before such revision or amendment becomes effective. If Client requests a change to any business requirements relative to, or cancels, a Service, or any portion thereof, after Experian has commenced work, Client agrees to pay Experian for its costs incurred for such work in process. If the Services are substantially completed at the time of such change or cancellation, Client agrees to pay Experian the full price for such Services. Experian's invoices will be deemed to be correct and acceptable to Client unless Client advises Experian of disputed items within ten (10) days of their receipt. Payments shall be made to Experian within thirty (30) days of invoice date. If Client fails to pay any invoice in accordance with the foregoing terms, Experian reserves the right to suspend the Services and Client also shall pay interest on the unpaid amount at the lesser of one and one-half percent (1.5%) per month or the maximum amount allowed by law. The prices and rates for the Services do not include either shipping costs or applicable federal, state, local, or foreign sales or use taxes, and Client will pay or reimburse Experian for such shipping costs and taxes.

3. Data; Confidential Information.

A. Experian Data. The parties acknowledge and agree that the Services may include the delivery, access or use of (i) personal data or information that does or could be used to identify a consumer, (ii) credit data or data that is a consumer report as defined under the Fair Credit Reporting Act, as may be amended, (iii) data that has been furnished or otherwise provided by or on behalf of Client to Experian and is included in Experian databases, and (iv) any other data or information related to consumers and/or businesses, in each case provided or made available by or on behalf of Experian to Client (including, without limitation, business credit data and marketing data); and (v) any copies or derivatives of such data or information, whether or not such data or information is or could be linked back to an individual consumer (collectively, "Experian Data"). Client represents and warrants that it shall not resell the Experian Data, and that it shall only access, receive and use the Experian Data in the manner explicitly permitted in a Schedule.

(i) Safeguards. Client agrees to treat such data responsibly and take reasonable steps to maintain appropriate confidentiality and to prevent unlawful dissemination or misuse by its employees, officers, or any other person with access to such data. Client shall implement and maintain a comprehensive information security program written in one or more readily accessible parts and that contains administrative, technical, and physical safeguards that are appropriate to Client's size and complexity, the nature and scope of its activities, and the sensitivity of the information provided to Client by Experian. Such safeguards shall, at minimum, include the elements set forth in 16 C.F.R. § 314.4 and shall be reasonably designed to (i) ensure the security and confidentiality of Experian Data, and other information provided by Experian, (ii) protect against any anticipated threats or hazards to the security or integrity of such information, and (iii) protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any consumer. Client shall, at a minimum, comply with Experian's standard security requirements with respect to Experian Data, and to the extent applicable to Client's access and use of the Services. Client shall provide a copy of its written security program to Experian upon request and shall adopt any safeguard that Experian may reasonably request. Client shall promptly notify Experian of any unauthorized access, use or disclosure of Experian Data. Client agrees to defend and indemnify and hold Experian and its affiliates harmless from and against all damages, liabilities, claims, losses, costs and expenses that Experian may incur, suffer, become liable for or which may be asserted or claimed against Experian as a result of Client's non-performance of any obligation with respect to Experian Data.

B. Client Data. Any non-public data or information provided by or on behalf of Client to Experian in connection with Client's request for the Services and which does not constitute Experian Data ("Client Data") is and shall continue to be the exclusive property of Client. Except as otherwise permitted in a Schedule, Experian agrees to (i) use Client Data only for purposes of providing the Services to Client, and (ii) take reasonable steps to maintain the confidentiality of Client Data and prevent unauthorized access, use or disclosure of Client Data.

C. Confidential Information. Client and Experian agree not disclose, and shall strictly maintain the confidentiality of, all Confidential Information of the other party. Client and Experian each agree to use at least the same degree of care to safeguard and to prevent disclosing to third parties the Confidential Information of the other as it employs to avoid unauthorized disclosure, publication, dissemination, destruction, loss, theft, or alteration of its own information of a similar nature, but not less than reasonable care. The term "Confidential Information" means in any form: (a) all information marked confidential, restricted or proprietary; or (b) any other information that is treated as confidential by the disclosing party and would reasonably be understood to be confidential, whether or not so marked or disclosed orally. The parties agree that Confidential Information does not include Experian Data or Client Data. Without limiting the generality of the foregoing, the parties agree that Experian's Confidential Information includes the confidential, proprietary, and trade secret information of Experian, its affiliates and their respective licensors and suppliers, which information includes, but is not limited to: (i) models, attributes, weights, data structures, Experian PINs, pricing structures, and application programming interfaces, (ii) the Agreement, and (iii) any other types of information applicable to the Services as maybe identified in a Schedule; and (iv) any copies or derivatives of such data or information.

4. Retained Rights; Access and Use.

A. Retained Rights. Client acknowledges that Experian has expended substantial time, effort and funds to develop, create, compile, provide and deliver the Services, Experian Data, Experian Confidential Information and various databases, improvements, technologies, inventions, developments, ideas, and discoveries associated therewith; all of which, when used in connection with the provision of, or access to, the Services shall be deemed part of the Services. Client agrees that the Services, all data in Experian's databases and any other intellectual property that are part of the Services or related to the Services are owned by Experian (or its licensors or providers, as applicable). Nothing contained in the Agreement shall be deemed to convey to Client or to any other party any ownership interest in or to any intellectual property or data provided in connection with the Services, Experian Data or Experian Confidential Information. Client shall not acquire any license to use the Services, Experian Data or any Experian Confidential Information in excess of the scope and/or duration described in the Agreement.

B. Access and Use. Client represents and warrants to Experian that it shall only access and use the Services and Experian Data for Client's own internal business and solely in the manner explicitly permitted in the Agreement. Client further agrees that it shall not, and shall not permit others (including but not limited to any affiliate or related companies and users) to, (i) change, modify, add code or otherwise alter the Services in any manner, (ii) reverse engineer, disassemble, decompile, in any way attempt to derive the source code of, or translate the Services, or (iii) use, transform, modify, or adapt the Services for use for any other purpose, including but not limited to use to assist in the development or functioning of any product or service that is competitive, in part or in whole, with any existing or reasonably anticipate product or service of Experian.

5. Compliance. Experian shall comply with all federal, state and local laws, rules and regulations applicable to Experian as a provider of the

Services. Client shall comply with all federal, state and local laws, rules and regulations applicable to Client's access, collection, use, storage, transmission and provision to Experian of Client Data, and Client's access, receipt and use of the Services and Experian Data. Experian reserves the right to revise, amend or supplement the terms or conditions or pricing under the Agreement and/or the Services (including without limitation the right to withdraw or restrict affected data) to meet any requirement imposed by federal, state, or local law, rule or regulation, a third party supplier, or to address matters concerning privacy, confidentiality or security, upon reasonable notice to Client.

6. Domestic Access and Use. Client shall not access, transfer, or use the Services, Experian Confidential Information or Experian Data outside the United States or its territories. Any direct or indirect access to, transfer, or use of the Services, Experian Confidential Information or Experian Data outside the United States or its territories shall require the prior written approval of Experian.

7. Term; Termination. The term of the Agreement shall begin upon the Effective Date set forth below and shall continue in effect until the termination or expiration of all Schedules. Upon any termination of the Agreement or a Schedule, Client shall immediately cease using the applicable Services, Experian Data and Experian Confidential Information in its possession. If either party is in material breach of the Agreement or any individual Schedule, the other party may terminate the individual Schedule and/or the Agreement, as applicable, provided such breach is not cured within thirty (30) days following written notice of such breach, unless such breach is the failure to pay for the Services under the terms of the Agreement, in which case Client shall have ten (10) days to cure such breach following notice. Notwithstanding the foregoing, the Agreement or any Schedule may be terminated by Experian immediately upon written notice to Client if in Experian's reasonable good faith judgment any Services, Experian Confidential Information and/or Experian Data provided to Client are being used or disclosed contrary to the Agreement and/or any Schedule. In the event that the Agreement or a Schedule is terminated as a result of a breach, the other party shall, in addition to its rights of termination, be entitled to pursue all other remedies against the breaching party. Termination of the Agreement or any Schedule shall not relieve Client of its obligation to pay for any Services performed or provided by Experian under the Agreement or any Schedule.

8. Limited Warranty; Disclaimers. Experian warrants to Client that Experian will use commercially reasonable efforts to deliver the Services in a timely manner. THE WARRANTY IN THE FIRST SENTENCE OF THIS PARAGRAPH IS THE ONLY WARRANTY EXPERIAN HAS GIVEN CLIENT WITH RESPECT TO THE SERVICES OR EXPERIAN DATA. BECAUSE THE SERVICES INVOLVE CONVEYING INFORMATION PROVIDED TO EXPERIAN BY OTHER SOURCES, EXPERIAN CANNOT AND WILL NOT, FOR THE FEE CHARGED FOR THE SERVICES, BE AN INSURER OR GUARANTOR OF THE ACCURACY OR RELIABILITY OF THE SERVICES, EXPERIAN DATA OR THE DATA CONTAINED IN ITS VARIOUS DATABASES. IN ADDITION, EXPERIAN MAKES NO REPRESENTATION OR WARRANTIES, EXPRESS OR IMPLIED, WITH RESPECT TO THE EXPERIAN SERVICES, ANY EXPERIAN DATA, OR ANY OTHER MATERIALS (TANGIBLE OR INTANGIBLE) SUPPLIED BY EXPERIAN HEREUNDER, AND EXPERIAN HEREBY EXPRESSLY DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTIES WITH RESPECT THERETO, INCLUDING WITHOUT LIMITATION, ANY WARRANTIES AS TO THE ACCURACY, COMPLETENESS OR CURRENTNESS OF ANY DATA OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY, OR NON-INFRINGEMENT, OR FITNESS FOR A PARTICULAR PURPOSE. EXPERIAN DOES NOT WARRANT, REPRESENT OR UNDERTAKE THE OPERATION OF THE EXPERIAN SERVICES TO BE UNINTERRUPTED OR ERROR-FREE, NOR DOES EXPERIAN MAKE ANY WARRANTY OR REPRESENTATION REGARDING THE USE OR OUTPUT OF THE SERVICES IN TERMS OF CORRECTNESS, ACCURACY, COMPLETENESS, TIMELINESS, RELIABILITY OR OTHERWISE, OR THAT THE SERVICES WILL MEET CLIENT'S REQUIREMENTS.

9. Acceptance. Client acknowledges that the prices Experian charges for the Services are based upon Experian's expectation that the risk of any loss or injury that may be incurred by use of the Services will be borne by Client and not Experian. Client agrees that it is responsible for determining that the Services are in accordance with Experian's obligations under the Agreement. If Client reasonably determines that the Services do not meet Experian's obligations under the Agreement, Client shall so notify Experian in writing within ten (10) days after access to or receipt of the Services in question. Client's failure to so notify Experian shall mean that Client accepts the Services or the performance of the Services as is. If Client so notifies Experian within ten (10) days after access to or receipt of the Services, then, unless Experian reasonably disputes Client's claim, Experian shall, at its option, either re-perform the Services in question or issue Client a credit for the amount Client paid to Experian for the nonconforming Services. EXPERIAN'S REPERFORMANCE OF THE SERVICES OR THE REFUND OF ANY FEES CLIENT HAS PAID FOR SUCH SERVICES SHALL CONSTITUTE CLIENT'S SOLE REMEDY AND EXPERIAN'S MAXIMUM LIABILITY UNDER THE AGREEMENT REGARDING THE SERVICES.

10. Limitation of Liability.

CLIENT AGREES THAT EXPERIAN'S TOTAL AGGREGATE LIABILITY UNDER THE AGREEMENT, REGARDLESS OF THE NATURE OF THE LEGAL OR EQUITABLE RIGHT CLAIMED TO HAVE BEEN VIOLATED, IS LIMITED TO DIRECT DAMAGES WHICH SHALL NOT EXCEED THE AMOUNT PAID BY CLIENT TO EXPERIAN UNDER THE AGREEMENT FOR THE PARTICULAR SERVICES THAT ARE THE SUBJECT OF THE ALLEGED LOSSES OR INJURIES DURING THE SIX-MONTH PERIOD PRECEDING THE DATE ON WHICH THE ALLEGED LOSSES OR INJURIES BY EXPERIAN FIRST ACCRUED. CLIENT COVENANTS THAT IT WILL NOT SUE EXPERIAN FOR ANY AMOUNT GREATER THAN SUCH AMOUNT. CLIENT FURTHER ACKNOWLEDGES THAT SECTIONS 8 AND 9 APPLY TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, REPRESENT A FAIR ALLOCATION OF THE RISK BASED ON THE PRICES EXPERIAN CHARGES FOR THE SERVICES AND APPLY EVEN IF AN EXCLUSIVE OR LIMITED REMEDY STATED HEREIN FAILS OF ITS ESSENTIAL PURPOSE.

NOTWITHSTANDING ANY OTHER PROVISION OF THE AGREEMENT, IN NO EVENT SHALL EITHER PARTY BE LIABLE TO THE OTHER PARTY FOR ANY INCIDENTAL, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCREASED DAMAGES, OR DAMAGES TO BUSINESS REPUTATION, DAMAGES ARISING FROM LOSS OF BUSINESS WITH THIRD PARTIES, OR LOSS OF PROFITS FROM TRANSACTIONS WITH THIRD PARTIES, WILLFUL INFRINGMENT BY THE OTHER PARTY, WHETHER ANY OF THE FOREGOING ARE FORESEEABLE OR NOT, AND HOWEVER CAUSED, EVEN IF SUCH PARTY IS ADVISED OF THE POSSIBILITY THAT SUCH DAMAGES OR LOST PROFITS MIGHT ARISE.

11. Waiver; Severability. Either party may waive compliance by the other party with any covenants or conditions contained in the Agreement or any Schedule, but only by written instrument signed by the party waiving such compliance. No such waiver, however, shall be deemed to waive any other circumstance or any other covenant or condition not expressly stated in the written waiver. The provisions of the Agreement shall be deemed severable, and the invalidity or unenforceability of any one or more of its provisions shall not affect the validity and enforceability of its other provisions. If any such provision is held to be invalid, void, or unenforceable, the remaining provisions shall nevertheless continue in full force. In lieu of any invalid provision, a substitute provision shall apply retroactively which comes as close as legally and commercially possible to that intent which the parties had or would have had, according to the spirit and purpose of the Agreement.

12. Audit. Client agrees that Experian will have the right to audit Client's and any of its agent's compliance with the terms of the Agreement, including its access, receipt and use of the Services, Experian Confidential Information and Experian Data. Client will be responsible for assuring full cooperation with Experian in connection with such audits and will provide Experian or obtain for Experian access to such properties, records and personnel as Experian may reasonably require for such purpose.

13. Successors and Assigns; No Third-Party Beneficiaries. Client shall not assign, delegate, or otherwise transfer the Agreement or any of its rights or obligations under it, or purport to do any of these things, or any interest relating to the Agreement without the prior written approval of Experian. Any attempted assignment, delegation or transfer by Client without such approval shall be null and void *ab initio*. The dissolution, merger, consolidation, reorganization, assumption, sale or other transfer of assets, properties, or controlling interest of Client constitutes an

assignment of the Agreement. Without the prior written consent of Client being required, Experian may use subcontractors to perform any of its obligations under the Agreement, and may assign or subcontract the Agreement or any of its rights under it to its affiliates or a subsequent owner. The Agreement is binding upon and inures to the benefit of the parties and their permitted successors and assigns. Persons or entities who are not a party to the Agreement (other than Experian and its affiliates, and their respective successors and assigns) shall not have any rights under the Agreement and the parties hereby agree that nothing in the Agreement shall be construed as creating a right that is enforceable by any person or entity that is not a party to the Agreement (or an Experian affiliate) or a permitted successor assignee of such party.

14. Excusable Delays. Experian shall not be responsible for any delay, failure to perform, or alteration of the Services due to any act, omission or failure to perform by Client, and Client may be responsible to Experian for additional fees and costs associated therewith. Neither party shall be liable for any delay or failure in its performance under the Agreement (except for the payment of money) if and to the extent such delay or failure is caused by events beyond the reasonable control of the affected party including, without limitation, acts of God, public enemies, or terrorists, labor disputes, equipment malfunctions, material or component shortages, supplier failures, embargoes, rationing, acts of local, state or national governments or public agencies, utility or communication failures or delays, fire, earthquakes, flood, epidemics, riots and strikes. If a party becomes aware that such an event is likely to delay or prevent punctual performance of its own obligations, the party will promptly notify the other party and use its reasonable effort to avoid or remove such causes of nonperformance and to complete delayed performance whenever such causes are removed.

15. Choice of Law. The Agreement is governed by and construed in accordance with the internal substantive laws of the state of California, without giving effect to any choice of law or other provision that would result in the application of the laws of any other jurisdiction. Any legal action, suit, proceeding brought by a party in any way arising out of or relating to the Agreement shall be brought in the federal or state courts located in Orange County, California.

16. Notices. All notices, requests and other communications hereunder shall be in writing and shall be deemed delivered at the time of receipt if delivered by hand or communicated by electronic transmission, or, if mailed, three (3) days after mailing by first class mail with postage prepaid. Notices to Experian and Client shall be addressed to the addresses provided below each party's signature, or to such other address as either party shall designate in writing to the other from time to time.

17. Complete Agreement. The Agreement, as supplemented or amended by any Schedules, sets forth the entire understanding of Client and Experian with respect to the subject matter hereof, and the terms of the Agreement shall be superior to, control, and supersede all terms in any prior letters of intent, agreements, covenants, arrangements, communications, representations, or warranties, whether oral or written, by any officer employee, or representative of either party relating thereto.

18. Amendments. The Agreement may only be amended in writing signed by authorized representatives of both parties.

19. Survival. The provisions of Sections 3, 4, 5, 7, 9, 10, 11, 12, 14, 15, 16, 18 and 20, in addition to any other provisions of the Agreement that would normally survive termination, shall survive termination of the Agreement for any reason.

20. Authority to Sign. Each party represents that (i) the person signing the Agreement or any Schedule has all right, power and authority to sign the Agreement on behalf of such party; (ii) it has full power and authority and all necessary authorizations to comply with the terms of the Agreement and to perform its obligations hereunder; and (iii) if it signs the Agreement with an electronic signature, it (a) shall comply with all applicable electronic records and signatures laws, including but not limited to the Electronic Signatures in Global and National Commerce Act; (b) hereby acknowledges its electronic signature is effective and will not dispute the legally binding nature, validity or enforceability of the Agreement based on the fact that the terms were accepted with an electronic signature; and (c) shall ensure that its electronic signature vendor shall comply with the confidentiality obligations of the Agreement.

IN WITNESS WHEREOF, Client and Experian sign and deliver the STAC as of the Effective Date set forth below.

Experian Information Solutions, Inc.

By: _____
Signature (Duly Authorized Representative Only)

Name: _____
Print

Title: _____

Effective Date: _____

Address for Notice: Experian, 475 Anton Boulevard, Costa Mesa, CA 92626, Attn: General Counsel, Law Department

_____
Print or Type Legal Name of Client

By: _____
Signature (Duly Authorized Representative Only)

Name: _____
Print

Title: _____

Physical Address for Notice:
Attn:

EXPERIAN
DEATH MASTER FILE ADDENDUM

This Death Master File Addendum ("Addendum") supplements the Experian Standard Terms and Conditions, dated ("Agreement"), currently in place between Experian and Client.

Client and Experian agree as follows:

1. "Experian Services" as used herein shall mean services provided to Client by Experian Information Solutions, Inc.

2. Client acknowledges many Experian Services contain information from the Death Master File as issued by the Social Security Administration ("DMF"). Pursuant to Section 203 of the Bipartisan Budget Act of 2013 and 15 C.F.R. § 1110.102, Client certifies that consistent with its applicable FCRA or GLB use of Experian Services, Client's use of deceased flags or other indicia within the Experian Services is restricted to legitimate fraud prevention or business purposes in compliance with applicable laws, rules regulations, or fiduciary duty, as such business purposes are interpreted under 15 C.F.R. § 1110.102(a)(1).

3. Client further certifies it will not take any adverse action against any consumer without further investigation to verify the information from the deceased flags or other indicia within the Experian Services.

4. Capitalized terms not otherwise defined herein shall have the meaning set forth in the Agreement. In the event of a conflict between this Addendum, Schedules, Supplements, pricing document(s) and the Agreement, the terms and conditions of this Addendum shall prevail.

This Addendum, together with the applicable Schedules, Supplements, pricing document(s) and the Agreement as amended herein constitute the entire agreement between the parties with respect to the Experian Services provided hereunder and supersedes all prior proposals and agreements, both written and oral, and all other written and oral communications between the parties.

Experian Information Solutions, Inc.		_____ Print or Type Full Legal Name of Client
By: _____ Signature (Duly Authorized Representative Only)	By:	_____ Signature (Duly Authorized Representative Only)
Name: _____ Print	Name:	_____ Print
Title: _____	Title:	_____
Addendum Effective Date: _____		

EXPERIAN
CONSUMER SERVICES SCHEDULE

This Consumer Services Schedule ("Schedule") supplements the Experian Standard Terms and Conditions, dated ("Agreement"), currently in place between Experian and Client.

1. Application. For the purposes of this Schedule, the term "Services" shall mean Experian's provision of services to Client which includes the supply of consumer credit information, account review services, identification information, generic scoring services, and other data services from information stored in one of Experian's consumer databases. Experian will provide Services to Client for the fees set forth in a pricing document signed by both parties that identifies the Services being ordered by Client and which incorporates this Schedule and the Agreement by reference.

2. Term. This Schedule shall commence on the Schedule Effective Date and continue in force without any fixed date of termination and either Client or Experian may terminate this Schedule upon thirty (30) days prior written notice to the other party. Notwithstanding the foregoing, if a term is designated in a pricing document signed by both parties, such term will apply to this Schedule and Client shall have no right to terminate this Schedule upon thirty (30) days prior written notice with regards to the applicable Services.

3. FCRA Use. Client will request and use the Services strictly in accordance with the federal Fair Credit Reporting Act, 15 U.S.C. 1681 *et. seq*., as amended (the "FCRA"). Without limiting the foregoing, Client certifies that Client will request and use the Services solely in connection with (i) a single credit transaction with a consumer, or, if applicable, for another "permissible purpose" as defined by the FCRA; and (ii) transactions involving the consumer as to whom such information is sought and will not request or use such Services for purposes prohibited by law. Permissible purpose does not include the collection of debts not voluntarily incurred by the consumer unless those debts are judicially established by a court order or judgment. Client further certifies that it will comply with all requirements of the FCRA applicable to it. If Client has purchased a consumer report from Experian in connection with a consumer's application for credit, and the consumer makes a timely request of Client, Client may share the contents of that report with the consumer as long as it does so without charge and only after authenticating the consumer's identity.

4. Data Use Restrictions. Client agrees that it will not, either directly or indirectly, itself or through any agent or third party, without the prior written consent of Experian, request, compile, store, maintain, resell or use the Services (including any of the information contained in the Services) to build its own credit reporting database. Client shall be solely responsible for assuring the secure and confidential manner in which it stores, delivers and transmits Services to its authorized employee users. Client shall, at a minimum, comply with Experian's standard access security requirements.

5. Inquiries. When accessing Services, Client certifies it will use reasonable measures to identify consumers and will accurately provide Experian with complete identifying information about the consumer inquired upon in the form specified by Experian. Client will enter all requested Client and type code information when requesting Services. Experian may use Client's inquiry data for any purpose consistent with applicable federal, state and local laws, rules, and regulations. Client will be responsible for installing the necessary equipment, software and security codes to prevent unauthorized access to an Experian database.

6. Data Contribution. If Client contributes information on its credit experience with consumers, including updates thereof, (collectively "Client Records") to Experian, Client agrees to make Client Records available to Experian at mutually agreeable times and format, in accordance with Section 623 of the FCRA. Client shall provide Client Records which are accurate to the best of its knowledge and shall promptly update and correct all known inaccurate information. Client shall provide Experian with written notice (i) if any information is disputed by a consumer, (ii) if the consumer closes the account; and (iii) not later than 90 days after furnishing the information, of the date of the commencement of the delinquency of an account which is placed for collection. Client shall bear the expense of preparing and delivering Client's Records to Experian. Experian may incorporate, at Experian's expense, Client Records into its credit reporting system. Information, once incorporated and merged with other contributed data, will be Experian's exclusive property. Client shall retain ownership in information used to compile its Client Records. At Experian's request, Client will promptly reinvestigate and verify the accuracy of Client Records. Experian may use Client Records for any purpose consistent with applicable federal, state and local laws, rules, and regulations; provided, however, that Experian will use reasonable commercial efforts not to release a list that specifically identifies individuals as Client's customers. Where applicable, Experian and the credit reporting industry expect all data contributors to report collection accounts as "paid collection" transactions when they are paid. This information should not be deleted unless required by law. Although this may seem like a valuable consumer service and helps Client collect on debt, it is a disservice to credit grantors for Experian to allow the deletion of this valuable collection information. For these reasons, if Client is deleting valid collection information, or charging fees to delete information, or both, Experian reserves the right to terminate this Agreement immediately and remove Client Records from Experian's credit reporting system.

7. Third Party Processors. In the event Client chooses to use a third party to perform certain data processing or model building services, the parties understand and acknowledge that the third party shall be acting on behalf of Client. Client will cause the third party to (i) handle, process, and possess all Experian provided data in accordance with this Agreement, and (ii) sign a Third Party Processor Undertaking form. Client shall provide Experian with the appropriate mailing instructions at least ten (10) days prior to the requested shipment date.

ALL CLIENTS MUST COMPLETE THIS SECTION

8. Point of Sale Certification. In compliance with Section 1785.14(a) of the California Civil Code, Client certifies to Experian that (i) Client ☐ ***IS*** ☐ ***IS NOT*** a retail seller, as defined in Section 1802.3 of the California Civil Code ("Retail Seller") and issues credit to consumers who appear in person on the basis of applications for credit submitted in person ("Point of Sale); (ii) if Client is a Retail Seller who issues Point of Sale credit, Client will instruct its employees and agents to inspect a photo identification of the consumer at the time an application is submitted in person; and (iii) it will only use the appropriate subscriber code number designated by Experian for accessing consumer reports for California Point of Sale credit transactions conducted by Retail Seller. Client shall notify Experian within 24 hours of any change in Client's status as a Retail Seller.

EXPERIAN
CONSUMER SERVICES SCHEDULE

This Schedule, together with the applicable pricing document(s) and the Agreement as amended herein constitutes the entire agreement between the parties with respect to the Services provided hereunder and supersedes all prior proposals and agreements, both written and oral, and all other written and oral communications between the parties.

Experian Information Solutions, Inc.		_____
		Print or Type Full Legal Name of Client
By: _____	By:	_____
Signature (Duly Authorized Representative Only)		Signature (Duly Authorized Representative Only)
Name: _____	Name:	_____
Print		Print
Title: _____	Title:	_____
Schedule Effective Date: _____		

EXPERIAN CROSSCORE SCHEDULE
(UNITED STATES)

This Experian CrossCore™ Schedule (**"CrossCore Schedule"**) is entered into effective , 20 (**"CrossCore Schedule Effective Date"**) by and between Experian Information Solutions, Inc., a Ohio corporation, with a place of business at 475 Anton Boulevard, Costa Mesa, CA 92626 (**"Experian"**) and , having an address at (**"Client"**). This CrossCore Schedule incorporates and is made a part of the Experian Standard Terms and Conditions between Experian and Client dated (**"Agreement"**). Experian and Client may be referred to individually as a **"Party"** and collectively as the **"Parties."** Capitalized terms not defined herein or in the Attachments shall have the meaning set forth in the Agreement.

In consideration of the foregoing, the covenants contained herein, and other good and valuable consideration, the Parties hereby agree:

1. Definitions.

"Attachments" means the terms for the Experian Services attached to this CrossCore Schedule and incorporated herein by reference. The Attachments, Services Addenda, and the CrossCore Schedule, may collectively be referred to as the Schedule.

"Ancillary Service" means a third-party Service, including software, product, hardware, tool, service, or material, developed, purchased, or licensed by Client that Client uses to connect to, access or otherwise use with CrossCore and the Experian Services. Where Client's access to an Ancillary Service is provided by Experian, such Ancillary Service shall be considered a Service subject to the terms of the Agreement, this CrossCore Schedule, and a Service Addendum hereto.

"Claim" means any claim, demand, action, damage, loss, liability, cost or expense, including reasonable attorney fees.

"**Client Data**" means data elements submitted by Client to Experian through CrossCore for processing, including Customer Data.

"Client Equipment" means any hardware, software and network infrastructure needed to connect to, access or otherwise use CrossCore and the Experian Services.

"CrossCore" means Experian's on-demand, web-based platform and decisioning tool for fraud and identity verification assessment, transaction viewing, workflows and reporting, which incorporates, as applicable, the Experian Services selected by Client and any Ancillary Services.

"**CC Use Case**" means the scope of use for which Client is authorized to use CrossCore as specified in the Pricing Exhibit.

"**Customer Data**" means any of the following data elements collected by Client from its customer or entered by Client's customer on Client's website: name, billing address, shipping address, phone number, email, date of birth, credit card number (PAN), Employer Identification Number (EIN), Social Security Number (SSN), password, or any other security code.

"**Delivery Plan**" means a document that describes Experian's implementation services to Client, which will be subject to this Schedule and the Agreement, and to be effective, must be signed by both Parties. Any deviation from the Delivery Plan, as well as any additional services requested by Client, will be billable at Experian's standard service rate then in effect; provided, however, that Experian must obtain Client's advance written approval prior to performing any services deemed billable.

"Documentation" means information, instructions, and materials made available or provided by Experian to Client, which Experian may amend from time to time, regarding the access and use of CrossCore, the Experian Services, and/or the configuration requirements for the Client Equipment and/or any applicable Ancillary Services.

"Experian Service" means any Experian fraud and identity Service, including but not limited to Precise ID and FraudNet, Services for delivery through CrossCore, in accordance with the terms of this CrossCore Schedule, the applicable Attachments, and the Agreement.

"Fees" mean the fees and amounts payable by Client during the applicable Term for CrossCore and the Experian Services, as set forth in a pricing exhibit hereto ("Pricing Exhibit").

"Output" means the response data, reports, or other deliverables generated by Experian and provided to Client through CrossCore during Client's use of the Experian Services and/or Ancillary Services.

"**Service Addendum"** means a contract supplementing this CrossCore Schedule signed by the Parties, setting forth supplemental terms and conditions for Client's use of an Ancillary Service, access to which is provided by Experian.

"Term" means the period during which Client is authorized to use CrossCore, the Experian Services, and any Ancillary Services, pursuant to the terms and conditions set forth in this CrossCore Schedule, the Attachments, the Agreement, and Service Addenda, unless earlier terminated as set forth in Section 5 of this CrossCore Schedule**.**

"Updates" means new versions, derivative works, modifications, additions or improvements to CrossCore or an Experian Service, including possible changes to security, technical configurations, application features, patches, and hotfixes.

"Users" means those Client employees, agents, and contractors authorized to use CrossCore, Experian Services, and/or Ancillary Services on behalf of Client in accordance with the terms of this CrossCore Schedule, the Attachments, the Agreement, and the Service Addenda.

2. Provision and Use of CrossCore.

A. Authorization to Use CrossCore. Subject to Client's compliance with the terms and conditions of this CrossCore Schedule and the Agreement, Experian grants Client a nonexclusive and non-transferable right to use CrossCore during the Term for the CC Use Case selected in the Pricing Exhibit.

Experian will provide Client with User logins for Users to access CrossCore. Each unique User must use a unique login, provided by Experian, to access CrossCore. Experian reserves the right to terminate, suspend or limit any User's access to CrossCore.

B. Product Enhancements and Improvements. Client hereby grants Experian the right to use Client Data sent to Experian for storage and/or processing through CrossCore in accordance with this CrossCore Schedule and the Attachments. Subject to Experian's confidentiality obligations with respect to Client Data under the Agreement, Experian may disclose the Client Data (i) to vendors, consultants, and subprocessors for Experian's internal business purposes, (ii) to enforce this CrossCore Schedule, the Agreement, the Attachments, or any Service Addendum, and (iii) to respond to law enforcement or governmental requests.

Client further agrees to provide Experian confirmed fraud feedback monthly during the Term based on its use of the Experian Services (**"Outcome Reporting"**) in the format specified by Experian, or as otherwise agreed by the Parties in writing. However, Client is not required to provide Outcome Reporting for Clients use of Experian Services consisting of Precise ID for Compliance Services (as described on the applicable Attachment). After extraction of information identifying Client and consumers, Client grants Experian the right to use Client Data and Outcome Reporting for validation, deployment, measurement, improvement, research, development, and optimization (**"Improvements"**) of CrossCore and the Experian Services. Client acknowledges that Experian may incorporate these Improvements into and for use within CrossCore and the Experian Services generally, and agrees that this is an additional permitted use of the Client Data.

C. Experian Responsibilities. To the extent reasonably possible, before Client begins using CrossCore to access any Experian Service, as specified in a Delivery Plan signed by the Parties, Experian will assist Client in (i) integrating CrossCore with the Experian Services, Client Equipment, and any applicable Ancillary Services, and (ii) training Client's employees around the use and functionality of CrossCore and the Experian Services. Client will be billed for integration services, maintenance and support, and training assistance, as applicable, at Experian's then-current rates.

D. Client Responsibilities. In addition to the confidentiality obligations in Section 3 of the Agreement, Client is responsible for (i) maintaining the confidentiality of login information, preventing unauthorized access or use of CrossCore and the Experian Services, monitoring activities conducted under its User logins, and notifying Experian of any unauthorized access or use; (ii) immediately notifying Experian of any compromise of User logins and assisting in any investigation or remedial action in the event of a compromise; (iii) obtaining and maintaining the Client Equipment; (iv) ensuring that the Client Equipment and any Ancillary Service not subject to a Services Addendum comply with the requirements applicable to CrossCore, the Experian Services, and the Documentation; (v) ensuring the accuracy, quality, integrity, legality, reliability, and appropriateness of all Client Data; and (vi) maintaining reasonable anti-virus and data security controls. Client is responsible for all activities of its Users with respect to CrossCore.

E. Restrictions on Client's Use of CrossCore. Client will use CrossCore and the Experian Services solely for its internal business purposes in accordance with the terms, scope, and use limitations of the Agreement, the Attachments, and this CrossCore Schedule. Client will not, and will ensure that its Users do not: (i) resell, sublicense, lease, rent, time-share or otherwise make CrossCore, the Experian Services, the Output available to any third-party, including third-party consultants of Client; (ii) use CrossCore or the Experian Services to send or store infringing, obscene, threatening, libelous, or otherwise unlawful or tortious material, including material harmful to children, or violate third-party privacy rights; (iii) gain or attempt to gain unauthorized access to, disrupt the integrity or performance of, or damage, disable, overburden or impair the operation of CrossCore, the Experian Services or the data contained therein; (iv) upload to CrossCore or the Experian Services or use CrossCore or the Experian Services to send or store viruses, worms, time bombs, Trojan horses or other harmful or malicious code, files, scripts, agents or programs; (v) modify or copy CrossCore or the Experian Services or create derivative works based on any aspect of CrossCore or the Experian Services; (vi) reverse engineer, disassemble, decompile or otherwise attempt to recreate, obtain or perceive the underlying code for CrossCore or the Experian Services; (vii) access CrossCore or the Experian Services for the purpose of building a competitive product or service or copying its features or user interface; (viii) use or permit the use of CrossCore or the Experian Services for purposes of product evaluation, benchmarking or other comparative analysis without Experian's prior written consent, or (ix) permit access to CrossCore or the Experian Services by a direct competitor of Experian.

F. Updates. Experian may release Updates to the CrossCore Services or the Experian Services from time-to-time. When reasonably possible, Experian will provide reasonable notice of such Updates. Experian agrees that such Updates will not result in a material reduction in the level of performance, availability or functionality of CrossCore or the latest version of Experian Services. Updates will be subject to the terms and conditions of the Agreement, the Attachments, and this CrossCore Schedule.

If Client is using a non-current version of an Experian Service or Ancillary Service, and Experian is aware that an Update will result in a material reduction in or unavailability of such service, Experian will make commercially reasonable efforts to notify Client ninety (90) days before the release of the Update. Client and Experian agree to cooperate in transitioning Client to the current version of the Experian Service or Ancillary Service to allow for proper access to such service through CrossCore following release of the Update, subject to applicable and reasonable professional services fees at Experian's then-current rates. If such transition is not possible or practicable, Experian will not be required to continue to facilitate delivery of the non-current version of such service through CrossCore following the release of the Update and may terminate Client's use of CrossCore, the Experian Service, and/or Ancillary Service in its discretion.

3. Consumer and Data Privacy Obligations.

A. Regulatory Compliance. Client is solely responsible for its regulatory compliance in its use of CrossCore, the Output, and the Experian Services. Client must make Experian aware of any technical requirements that result from its regulatory obligations before signing this CrossCore Schedule or any applicable Service Addendum, and of any subsequent changes to such technical or regulatory requirements.

B. Data Transmission. Before transmission of Customer Data to Experian, Client must hash, at a minimum, Personally Identifiable Information, as defined by the Gramm-Leach-Bliley Act, 15 USC 6801 et. seq., including but not limited to Date of Birth, PAN, EIN, SSN, and PIN (whether a password or other security code).

4. Intellectual Property Ownership Rights. Experian owns, reserves, and retains all rights, title and interest in and to CrossCore and the Experian Services, as well as the Documentation, any Updates, and the Output. Neither Client nor any User acquires any right or interest of any kind in CrossCore and the Experian Services, the Documentation, any Updates, or the Output because of the access provided in this CrossCore Schedule. All rights and interest to derivative works, modifications, additions or improvements to CrossCore or the Experian Services, the underlying software, and the Documentation will remain with and are hereby assigned to Experian, by Client for itself and on behalf of its Users, regardless of inventorship or authorship, and regardless of the Party suggesting or making the derivative work, modification, addition or improvement. Further, Experian owns all rights, title and interest in and to any suggestions, ideas, enhancement requests, feedback, recommendations or other information provided by Client or its Users relating to the features, functionality or operation of CrossCore or the Experian Services.

5. Term and Termination. Unless terminated earlier pursuant to this CrossCore Schedule, this CrossCore Schedule will commence on the CrossCore Schedule Effective Date and continue for the period set forth on the applicable Pricing Exhibit, (the **"Initial Term"**). Thereafter, this CrossCore Schedule will automatically renew for additional successive one (1) year terms (each a **"Renewal Term"**) until either Party provides the other Party with sixty (60) days' written notice of non-renewal before the end of the Initial Term or the then-current Renewal Term. The Initial Term and the Renewal Terms(s) are collectively the Term.

The Experian Services will commence on the applicable Effective Date specified on page one of this CrossCore Schedule and continue until the termination of this CrossCore Schedule. Notwithstanding the foregoing, Experian may terminate this CrossCore Schedule, any Experian Service, and/or the applicable Service Addenda in accordance with the terms of Section 2.F. In the event Client terminates an Experian Service without cause before the end of the CrossCore Schedule Term, then Client agrees to pay Experian the sum of all fees due for such Experian Service for the remainder of the then-current CrossCore Schedule Term.

Upon expiration or termination of this CrossCore Schedule, (i) Client's and its Users' right to access and use CrossCore and the Experian Services will immediately terminate, (ii) Client and its Users will immediately cease all use of CrossCore and the Experian Services, and (iii) each Party will return to the other Party and make no further use of any confidential information, materials, or other items (and all copies thereof) belonging to the other Party. In its discretion, Experian may destroy or otherwise securely dispose of any Client Data in its possession. In addition, upon any termination of this CrossCore Schedule, Client will immediately pay to Experian all Fees outstanding as of the date of, and any amounts outstanding resulting from, such termination.

Termination of this CrossCore Schedule or an Attachment does not relieve Client of its obligations under this CrossCore Schedule or an applicable Attachment that calls for performance after the termination date.

6. Indemnification.

A. Experian Indemnification Responsibilities. Subject to the limitations of Section 10 of the Agreement, Experian will indemnify, defend and hold harmless Client from and against any and all third party Claims to the extent caused by any: (i) direct infringement by Experian of any United States patent, copyright, trade secret, or other intellectual property right resulting from Experian's provision of or Client's or its Users' use of CrossCore or the Experian Services in accordance with this CrossCore Schedule and the Agreement; or (ii) Experian's violation of any applicable federal, state or local law, regulation, rule or judicial or

administrative order in connection with Experian's provision of CrossCore. Notwithstanding the foregoing, in no event will Experian be liable for any Claim caused or alleged to be caused by information, products or services supplied by or through Client. Experian will have no liability for any Claim of infringement to the extent such Claim is based upon or caused in whole or in part by: (i) Client's alteration or modification of CrossCore or the Experian Service; (ii) Client's use of CrossCore or the Experian Service in combination with any hardware, software or other products or services without Experian's express authorization; or (iii) Client's breach or violation of any term or condition of this CrossCore Schedule or the Agreement.

B. Client Indemnification Responsibilities. Subject to the limitations of Section 10 of the Agreement, Client will indemnify, defend and hold harmless Experian, its affiliates, and their respective officers, directors, employees, and contractors from and against any and all Claims to the extent caused by (i) Client's or its Users access to or use of CrossCore, the Experian Services, or the Output in violation of any applicable federal, state or local law, regulation, rule or judicial or administrative order; (ii) Client's failure to perform any of the Client responsibilities set forth in Section 2.D.; (iii) Client's breach of this CrossCore Schedule, the Attachments, any Service Addendum, or the Agreement; or (iv) infringement by Client of any patent, copyright, trade secret, or other intellectual property right in connection with Client's provision of any Client Data.

7. Disclaimer of Warranties. EXPERIAN DOES NOT WARRANT THAT THE ACCESS TO AND OPERATION OF CROSSCORE, THE EXPERIAN SERVICES, THE ANCILLARY SERVICES, AND ANY OUTPUT, WILL BE UNINTERRUPTED OR ERROR-FREE, OR THAT ALL PROGRAMMING ERRORS WILL BE CORRECTED. EXCEPT AS OTHERWISE EXPRESSLY PROVIDED IN THIS CROSSCORE SCHEDULE, CROSSCORE, THE EXPERIAN SERVICES, AND ANCILLARY SERVICES ARE PROVIDED "AS IS" AND "AS AVAILABLE" WITHOUT ANY WARRANTY, INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF TITLE, QUIET ENJOYMENT, DATA ACCURACY, NON-INFRINGEMENT, SYSTEM INTEGRATION, MERCHANTABILITY, OR FITNESS FOR A PARTICULAR PURPOSE, OR ANY WARRANTY AS TO PERFORMANCE, ACCURACY, COMPLETENESS, TIMELINESS, RELIABILITY OR FREEDOM FROM ERROR, OR AS TO ANY RESULTS GENERATED THROUGH THEIR USE.

CLIENT ACKNOWLEDGES AND AGREES THAT WHERE EXPERIAN IS DELIVERING ANCILLARY SERVICES THROUGH CROSSCORE, EXPERIAN IS OPERATING AS A RESELLER OF SUCH ANCILLARY SERVICES AND THAT EXPERIAN CANNOT AND WILL NOT BE A GUARANTOR OF THE ACCURACY OR RELIABILITY OF SUCH ANCILLARY SERVICES. EXPERIAN MAKES NO REPRESENTATION OR WARRANTIES, EXPRESS OR IMPLIED, WITH RESPECT TO ANY ANCILLARY SERVICES DELIVERED BY EXPERIAN HEREUNDER, AND EXPERIAN HEREBY EXPRESSLY DISCLAIMS ANY LIABILITY WITH RESPECT THERETO, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, OR FITNESS FOR A PARTICULAR PURPOSE. EXPERIAN DOES NOT WARRANT, REPRESENT OR UNDERTAKE THE SECURITY OF THE ANCILLARY SERVICES.

EXPERIAN MAKES NO WARRANTIES AS TO CLIENT EQUIPMENT, INCLUDING THE COMPATIBILITY OF CLIENT EQUIPMENT WITH CROSSCORE OR THE EXPERIAN SERVICES.

8. Marketing. Client agrees that, during the Term, Experian may list Client as a client in Experian's marketing collateral, including on its websites, and that Experian may use Client's name, logo and statements in its promotional material. In addition, Client agrees to make reasonable efforts to act as a customer, press, and analyst reference, and to participate in additional marketing activities such as a customer case study and digital press release, which activities will be mutually agreed to by both Parties. Client will also discuss with and furnish to Experian details and case studies on its use of CrossCore in conjunction with Experian Services. Experian may use Client details, case studies, and results achieved in Experian's public relations and marketing material. Experian retains all intellectual property rights to such information. Client may revoke the rights granted to Experian in this paragraph at any time and for any reason by sending at least thirty (30) days' prior written notice of such revocation to Experian.

This CrossCore Schedule, together with the applicable Attachments, the Pricing Exhibit, the Agreement, and if applicable any Exhibits or Sign-Up Form, constitute the entire agreement between the Parties with respect to CrossCore and the Experian Services, and supersede all prior proposals and agreements, both written and oral, and all other written and oral communications between the Parties.

If any express terms of this CrossCore Schedule directly conflict with the terms of the Agreement, the provisions of this CrossCore Schedule will be controlling and will govern with respect to the subject matter of this CrossCore Schedule. If any express terms of an Attachment directly conflict with the terms of the Agreement, Consumer Services Schedule (if applicable), or the CrossCore Schedule, the provisions of such Attachment will be controlling and will govern with respect to the subject matter of the that Attachment. This CrossCore Schedule may be executed in two or more counterparts, each of which will be deemed an original for all purposes, and together will constitute the same document.

Experian Information Solutions, Inc.

By: _____
Signature (Duly Authorized Representative Only)

Name: _____
Print

Title: _____

_____
Print or Type Full Legal Name of Client

By: _____
Signature (Duly Authorized Representative Only)

Name: _____
Print

Title: _____

EXPERIAN
ADDENDUM TO THE CROSSCORE SCHEDULE
FOR EMAILAGE SERVICES

This Addendum to the CrossCore Schedule for Emailage Services ("Addendum") supplements the CrossCore Schedule dated ("CrossCore Schedule") and the Experian Standard Terms and Conditions dated (together with the CrossCore Schedule, the "Agreements"), currently in place between Experian and Client. All capitalized terms not otherwise defined herein will have the meanings ascribed to such terms in the Agreement.

1. Emailage Services. This Addendum applies to Experian's provision of Emailage services, whether through CrossCore or a standalone alone batch process, to assist Client with vetting email addresses associated with consumers (the "Emailage Services"). Experian will provide the Emailage Services to Client for the fees set forth in the attached pricing exhibit.

2. Term. This Addendum will commence on the Addendum Effective Date set forth below and expire upon the termination or expiration of the CrossCore Schedule; provided that, in addition to the termination rights set forth in the Agreements, Experian may terminate this Addendum upon ninety (90) days' written notice to Client, in the event that Experian anticipates that it will not have the right to continue to deliver the Emailage Services.

3. Data Transmittal. Client authorizes Experian to provide Client's data and information to Emailage Corporation ("Emailage"), either, as necessary, through CrossCore or a standalone batch process. Client agrees that Emailage may use such data and information solely to provide Emailage Services to Client and for Emailage's internal business purposes.

4. Outcome Reporting. Client agrees to provide Emailage, either directly or through Experian, fraud feedback during the Term based on its use of the Emailage Services ("Outcome Reporting") in the format specified by Experian or Emailage, or as otherwise agreed by the parties in writing. Client agrees Emailage may use Outcome Reporting to provide the Emailage Services and for general product improvement, tuning, and development after extraction of information identifying Client.

5. Restrictions on Use. In addition to the use restrictions set forth in the CrossCore Schedule and elsewhere in the Agreements, Client will not use the Emailage Services in whole or in part (a) for any purposes enumerated in the Fair Credit Reporting Act, 15 U.S.C. § 1681, *et seq*. ("FCRA") in lieu of obtaining a consumer report as defined in the FCRA ("Consumer Report"); (b) for the purpose of serving as a factor in establishing an individual's eligibility for personal credit, insurance, or employment, or determining an individual's eligibility for a license or other benefit that depends on an applicant's financial responsibility or status, or for any other purpose under the FCRA; or (c) in the preparation of a Consumer Report or in such manner that may cause the Emailage Services to be characterized as a Consumer Report. Client further agrees that no adverse action (as defined in the FCRA), which is based in whole or in part on information obtained from the Emailage Services, may be taken against any consumer.

This Addendum, together with the Agreements, as amended, constitutes the entire agreement between the parties with respect to the Emailage Services provided hereunder and supersedes all prior proposals and agreements, both written and oral, and all other written and oral communications between the parties, with respect to the Emailage Services provided hereunder. In the event that any of the terms set forth in this Addendum conflict with the terms set forth in the Agreements, the terms set forth in this Addendum will control.

Experian Information Solutions, Inc.

By: _____
Signature (Duly Authorized Representative Only)

Name: _____
Print

Title: _____

Addendum Effective Date: _____

_____
Print or Type Full Legal Name of Client

By: _____
Signature (Duly Authorized Representative Only)

Name: _____
Print

Title: _____

ADDENDUM FOR NEUSTAR MPIC SERVICES
TO
ATTACHMENT FOR PRECISE ID TERMS
TO
EXPERIAN CROSSCORE SCHEDULE

Client will abide by and Experian will provide the Services to Client in accordance with the terms and conditions contained in this Addendum for Neustar Services that supplements the Attachment for Precise ID Terms to the Experian CrossCore Schedule ("Addendum").

1. Services. This Addendum sets forth the additional terms and conditions for use of Services under the Supplement enhanced with data licensed from Neustar Information Services, Inc. ("NIS") for both email and phone verification, in the manner set forth herein ("Neustar MPIC Services"), which terms supplement the terms and conditions set forth in the Supplement. If a request for Precise ID Services by Client yields a "no match" response based on Experian's files, such request will be routed to NIS. NIS will then return result codes to Experian, and Experian will deliver the result codes to Client in conjunction with the Precise ID Services, which results codes may also be used to deliver as part of a Precise ID Services score (if Client has contracted to receive such score under the Supplement), for the fees set forth in the Pricing Exhibit to this Addendum.

2. Term. Unless otherwise set forth on the applicable pricing document, this Addendum shall commence on the Addendum Effective Date and expire upon the termination or expiration of the Supplement; provided that, in addition to the termination rights set forth in the Agreement, Client or Experian may terminate this Addendum for any or no reason upon thirty days prior written notice to the other party. Experian may immediately terminate this Addendum in the event that the Neustar MPIC Services are no longer available.

3. Client Certifications. Client certifies that Client is the end user for the Neustar MPIC Services and will not resell or provide the Neustar MPIC Services to any third party. Each request for Neustar MPIC Services shall be for a single use only. All telephone numbers provided by Client in connection with the Neustar MPIC Services shall have been obtained by Client in compliance with all applicable law, and the same is transmitted to Experian and/or NIS in compliance with all applicable laws. Client shall promptly notify Experian of any unauthorized access, disclosure or use of the Neustar MPIC Services.

4. **Data; Data Use Restrictions.**

a. Client acknowledges that: (i) the data contained in the Neustar MPIC Services will be inserted into and leveraged by the Precise ID Services platform in order for Experian to deliver a score to Client for use in accordance with the terms of this Exhibit and the Supplement; and (ii) the Neustar MPIC Services leverages information solely from telephone numbers within the fifty (50) U.S. states and the District of Columbia.

b. Client certifies that it will not use Neustar MPIC Services (or any data contained therein), in whole or in part, as a factor in establishing a consumer's eligibility for credit, insurance, employment or for any other "permissible purpose" as defined in the Fair Credit Reporting Act. Client may not deny any consumer access to any of Client's online or other services based on the Neustar MPIC Services and/or Experian's Precise ID Services delivered in conjunction or integrated with the Neustar MPIC Services. The Neustar MPIC Services may only be used to permit access to or to refer a consumer to Client's additional authentication processes, and any denial of access must be based solely on such additional authentication processes.

c. Client shall not (i) disassemble, deconstruct, decompile or otherwise reverse engineer the Neustar MPIC Services or use the Neustar MPIC Services with computer-generated or random information; (ii) use database manipulation or any other method to reverse engineer the Neustar MPIC Services or any information contained therein to produce an unlisted or unpublished telephone number that Client is not licensed to receive under this Exhibit; (iii) use the information from the Neustar MPIC Services to build a database for resale or for access to such built database by a third party in competition with the Neustar MPIC Services; (iv) allow information from the Neustar MPIC Services to be used in a way to verify information from a third party that resells data in competition with NIS; (v) use the Neustar MPIC Services independent of or on a standalone basis from the Precise ID Services; (vi) use the Neustar MPIC Services for outbound collection and/or any Telephone Consumer Protection Act ("TCPA") risk mitigation applications; (vii) use the Neustar MPIC Services for any telemarketing or direct marketing purposes; or (viii) use the Neustar MPIC Services to enhance, verify, confirm, audit or update third party data.

d. Client understands and acknowledges that Neustar MPIC Services (and/or the data contained therein) being provided under this Addendum may not be used for the following purposes as listed below:

(i) Routing Related Applications which shall include providing location-based services during a transaction with an end customer, e.g., routing a telephone call to a geographically selected location, specking back information about nearby locations via the telecommunication network, or providing a dealer locator program over the Web/Internet.

(ii) Screen Pop Applications which shall mean the display of address or name information in real-time on the CRT or screen of a live operator during an inbound telephone call.

(iii) Interactive Voice Response (IVR) Applications which shall mean the printing or speaking via a voice response unit or utilizing voice recognition for the purpose of verifying address or name information with a consumer or business in real-time for data enhancement purposes.

(iv) Retail Point-of-Sale Applications which shall mean appending name and address information in real-time to a phone number captured at the Point-of-Sale for data enhancement purposes.

(v) Caller Name Services which shall mean providing a calling party name for display on a consumer device during a communication session initiated by the calling party.

(vi) Lead Verification Services which shall mean a service using quality attributes associated with a name, address, and telephone number to verify or otherwise validate a consumer prospect.

This Addendum with Pricing Exhibit, Pricing Attachment for Neustar MPIC Services, collectively with the Supplement, its applicable Consumer Service Schedule and the Agreement as amended herein, constitutes the entire agreement between the parties with respect to the subject matter hereof and supersedes all prior proposals and agreements, both written and oral, and all other written and oral communications between the parties with respect thereto.

Experian Information Solutions, Inc.		_____
		Print or Type Name of Client
By: _____	**By:**	_____
Signature (Duly Authorized Representative Only)		Signature (Duly Authorized Representative Only)
Name: _____	**Name:**	_____
Print		Print
Title: _____	**Title:**	_____
Addendum Effective Date: _____		

PRICING EXHIBIT
TO
ADDENDUM FOR NEUSTAR MPIC SERVICES
TO
ATTACHMENT FOR PRECISE ID TERMS
TO
EXPERIAN CROSSCORE SCHEDULE

Experian will provide the Neustar MPIC Services to Client for the fees set forth in this Pricing Exhibit. The fees shall become effective on the Addendum Effective Date indicated below, and may be superseded by any conflicting fees agreed to by the parties in subsequently-executed Pricing Exhibits to the Addendum.

Product/Service	Unit Price (Per Inquiry)*
Neustar MPIC Email	$
Neustar MPIC Phone	$

* Prices do not include applicable Sales and Use Tax which will be added separately, if applicable.

ATTACHMENT FOR PRECISE ID TERMS
TO
EXPERIAN CROSSCORE SCHEDULE

This Attachment for Precise ID Terms (**"PID Attachment"**) incorporates by reference the Consumer Services Schedule ("**CSS**") to, and supplements the CrossCore Schedule to, the Agreement currently in place between Experian and Client. Collectively, the CSS, CrossCore Schedule and the Agreement are referred to herein as the "**Agreement**." All capitalized terms not otherwise defined herein shall have the meanings ascribed to such terms in the Agreement.

1. Services. For the purposes of this PID Attachment, the terms "**Services**" and "**Experian Services**" include, as selected by Client on the applicable Sign-Up Form, the Precise ID for ID Screening Services, Precise ID for Identity Element Network Services, Precise ID for Compliance Services, Precise ID for Account Opening Services, and Knowledge IQ through Precise ID Services (collectively, the **"Precise ID Services").** Services also include validations and analytics projects (**"Validations"**) described in a criteria letter, and may utilize Depersonalized Data as defined below in Section 5. A criteria letter may include pricing and may be transmitted and approved by the Parties via electronic mail.

A. The **Precise ID for ID Screening Services, Precise ID for Identity Element Network Services, and the Precise ID for Compliance Services** mean the comparison of Client-supplied consumer-identifying information against identifying information contained in multiple Experian databases.

B. The **Precise ID Account Opening Services** means the comparison of Client-supplied consumer information against consumer-identifying and credit information contained in multiple Experian databases.

C. The **Knowledge IQ through Precise ID Services** means the question and response session providing identity verification in either FCRA or GLB regulated modes.

D. For **Validations**, Client shall specify in writing to Experian any information field that can be used by Client to link directly or indirectly to the personally identifiable information of any consumer in the Client data file it provides to Experian for the Services. Client represents to Experian that Client has the authority to provide the data to Experian required for performance of the Services at the time Client provides such data, and agrees that Experian may use Client's consumer data for general product research and development after extraction of information identifying Client and the consumer whose records are utilized. Where a third party is specified in a criteria letter as performing validations and/or analytics projects in connection with the Services delivered to Client, Client acknowledges and agrees that (i) it has sufficient rights, title, and interest in any data it provides to Experian for such specified third party to use the data in performing validations and/or analytics for Client, (ii) Experian may provide the Client-supplied data to such third party for such purpose, and (iii) such third party may use and process Client-supplied data for such purpose.

E. Client may request detailed Output for the Services in addition to the fraud risk score, classification type, or final decision.

F. Except to the extent set forth herein the terms and conditions in the Agreement and CrossCore Schedule relating to Services will apply to the Precise ID Services and Validations described herein.

2. Client's Certification of Use

NOTE: For regulatory purposes, and to ensure that the appropriate certifications are in place throughout the duration of Client's use of the Services, the certifications in A through F below are contained within this PID Attachment. Only those certifications herein that are applicable to Client's use of the Services at any given time will apply.

A. **GLB Certification.** Client certifies to Experian that Client will use the Services to protect against or prevent actual or potential fraud, unauthorized transactions, claims or other liability under the Gramm-Leach-Bliley Act, 15 U.S.C.A. Sec. 6801, *et seq*. (**"GLB"**). Client will not use the Precise ID for ID Screening, Precise ID for Identity Element Network, Precise ID for Compliance, or Knowledge IQ through Precise ID Services for the granting or denial of credit or for the setting of credit terms or pricing.

B. **Credit Information Certification.** ***When Client chooses to use consumer credit data in the Services***, then Client certifies that it has a "permissible purpose" under the Fair Credit Reporting Act, 15 U.S.C. 1681 *et. seq*. (**"FCRA"**). If Client's "permissible purpose" is based upon the written instructions of the consumer via the Internet, then Client shall obtain the consumer's written instructions in a manner substantially similar to that provided for in Section 6A below, or if Client obtains the consumer's consent to access credit data over the telephone, Client shall do so as provided for in Section 6B below. If Client's permissible purpose is "a legitimate business need for the information in connection with a business transaction that is initiated by the consumer," then the written instructions provisions of this PID Attachment and Section 6 do not apply, but only where (i) the Client has a risk of financial loss in the transaction, or (ii) Client uses the information to detect or prevent actual or potential fraud, to verify the identity of a consumer paying by check, to verify the identity of a consumer opening a DDA Checking Account, or for tenant screening. Client acknowledges and agrees that unless the number of inquiries made with respect to a consumer report is among the top four factors adversely affecting the credit score provided as part of the Precise ID Services, Experian does not output the same as an adverse action factor. If Client is using the Precise ID Services for mortgage lending credit decisions, Client further acknowledges that it must obtain a credit score that will disclose such key factor in accordance with the requirements of Section 609(g) of the FCRA. In any case, Client certifies that it will request and use all data received from Experian solely for its internal purposes in connection with transactions involving the consumer as to whom such information is sought and that it will not provide the Services to any third party. If Client chooses to use custom Fraud Penetration Index (**"FPI"**) attributes within Precise ID for Account Opening Services, Client certifies that: (i) it will obtain and use the consumer's written instructions as Client's sole permissible purpose under the FCRA; (ii) Client understands that the custom FPI application has not been developed to be compliant with the Equal Credit Opportunity Act, 15 U.S.C. 1691 *et seq*.; and (iii) therefore, Client will not use the Precise ID for Account Opening Services for the granting or denial of credit or for the setting of credit terms or pricing.

C. **Use of OFAC Data.** Matching of names to the OFAC list is based on very limited identification information. A match does not necessarily indicate that the consumer about whom Client inquired is the same person referenced by OFAC. ***Accordingly, if Client receives an OFAC result code in the Services***, Client acknowledges that any action taken by Client regarding a consumer must be taken based on Client's complete investigation of the consumer and not based solely on the OFAC information.

D. **Certification for Use of Motor Vehicle and Property Data.** ***If Client chooses to use vehicle ownership data in the Services***, Client certifies that its use is in compliance with the Driver's Privacy Protection Act of 1994 (18 U.S.C. Sec. 2721(b)(3)). Further, motor vehicle department data and property information will be used solely for authentication purposes.

E. **Client's Use of Alternate Source Data**. Certain product options offer questions that use information from Experian's non-FCRA data sources (**"Alternate Source Data"**). ***When using FCRA regulated product options***, Client certifies that it will obtain the consumer's written instructions before accessing any questions based on Alternate Source Data.

When using Alternative Source Data, Client certifies that it will not use the Alternate Source Data with the FCRA or GLB regulated Services provided hereunder for the granting of or denial of credit or any other FCRA permissible purpose. ***Further, when using Alternate Source Data with FCRA regulated Services***, Client certifies that it will obtain and use the consumer's written instructions as Client's sole permissible purpose under the FCRA.

ATTACHMENT FOR PRECISE ID TERMS
TO
EXPERIAN CROSSCORE SCHEDULE

F. **Use of Services for Compliance.** ***In the event that Client uses the Services for compliance with any law, regulation or similar requirement applicable to Client***, including without limitation the Red Flags Rules under the Fair and Accurate Credit Transactions Act or the regulations pursuant to the Office of Foreign Assets Control (**"Applicable Law"**), Client shall be solely responsible for such compliance, including without limitation the sufficiency of the Services for such purpose and any and all selection of criteria or attributes used in the Services. In addition to all other disclaimers in the Agreement and/or this PID Attachment and other applicable schedules or supplements, Experian hereby expressly disclaims any express or implied warranty or other assurance that Client's use of the Services will be sufficient to comply with Applicable Law, whether or not Experian has been apprised of such use. Experian shall not be deemed to have rendered to Client any legal or other advice, including with respect to Client's selection of criteria or attributes. Client warrants that it will use the Services in compliance with Applicable Law. Client shall defend and indemnify Experian and/or its affiliates for any and all liabilities, costs and expenses and/or damages incurred by Experian and/or its affiliates resulting from any noncompliance with Applicable Law by Client.

3. System Implementation Approval. Experian will configure the Services pursuant to specifications provided by Client in the Sign-Up Form. Upon completion of the configuration, Client shall test and audit performance of the Services to ensure proper configuration. Client shall notify Experian if the Services fail to meet the configuration requirements, and Experian shall modify the configuration to meet Client's requirements set forth in the Sign-Up Form. Such modification constitutes Client's sole remedy for failure to configure the Services in accordance with the Sign-Up Form and Experian's maximum liability for any such failure.

4. Client Use Restrictions. Except as expressly contemplated by this PID Attachment, Client shall not (a) distribute, publish, transmit or disseminate, in any form or by any means (including, without limitation, any internet), any part of the Services or the Output, (b) allow any third party to access the Services or the Output (including evaluation results), or (c) use the Services or Output to identify or solicit potential customers for its products or services.

5. Depersonalized (Coded) Data/Historical Validation. Depersonalized Data means certain data about consumers possessed by Experian and retained for modeling and research purposes which has consumers' identifying information coded or masked. Upon Client's request, Experian will provide the Depersonalized Data that may also include a record identifier. Client certifies to Experian that Client has no known ability to, and will not seek to (a) link the Depersonalized Data or record identifier to the individual identity of the consumer, including but not limited to, name, address, social security number, or customer account number, whose credit data is contained in or used to prepare the Services, or (b) otherwise identify the individual identity of the consumer whose credit data is contained in or used to prepare the Depersonalized Data. Client agrees that it will not, either directly or indirectly, itself or through any agent or third party, without the prior written consent of Experian, request, compile, store, maintain, resell or use the Depersonalized Data to build its own credit reporting database. Client shall be solely responsible for assuring the secure and confidential manner in which it stores, delivers and transmits the Depersonalized Data to its authorized employee users.

6. Written Instructions. Subsections 6A and 6B below shall apply as described in Section 2B above.

A. **FCRA Compliance--Written Instructions.** Client shall substantially comply with the following web site requirements:
(1) Client will prominently display a message specifically informing the consumer that his or her credit profile will be consulted for the purpose for which it is to be used and no other purpose, and that clicking on the "I AGREE" button following such notice constitutes written instructions to the Client under the FCRA. Client agrees that the notice provided by Client will be substantially as follows:

> "You understand that by clicking on the I AGREE button immediately following this notice, you are providing 'written instructions' to (*Client*) under the Fair Credit Reporting Act authorizing (*Client*) to obtain information from your personal credit profile or other information from Experian. You authorize (*Client*) to obtain such information solely to _____ *(insert purpose e.g. to confirm your identity to avoid fraudulent transactions in your name.)*

(2) The "I AGREE" button must immediately follow the notice provided for above. The notice and "I AGREE" button must be separate from any other notice or message contained on the web site.
(3) The consumer must have the ability to fully review any of the terms to which he or she is agreeing immediately preceding the consensual click.
(4) The consumer must not be able to proceed in the process without affirmatively agreeing to the terms in the notice.
(5) The consumer must have the ability (should they choose) to print out the terms to which he or she is agreeing, including their consent.
(6) The record of the consumer's 'written instruction' by clicking "I AGREE" must be retained by Client in a form that is capable of being accurately reproduced for later reference by the Parties.

B. **Written Instructions by Telephone.** If Client is obtaining "written instructions" over the telephone, Client shall substantially comply with the following requirements which are designed to comply with the Electronic Records and Signatures in Commerce Act:
(1) Client will ask each consumer to confirm his or her consent to access such person's credit report for authentication purposes by asking the following: "In order to verify your identity, you need to authorize (Client) to access your credit report for authentication purposes. Please confirm your authorization to access your credit report for authentication purposes by pressing the # key now";
(2) The consumer must not be able to proceed in the process without affirmatively agreeing to allow access to his credit report as provided above; and
(3) The record of the consumer's 'written instruction' by pressing the # symbol must be retained by Client in a form that is capable of being accurately reproduced for later reference by the Parties.

This PID Attachment, together with the Agreement (and the applicable schedules, supplements and exhibits thereto), as amended, constitutes the entire agreement between the Parties with respect to Services provided hereunder and supersedes all prior proposals and agreements, both written and oral, and all other written and oral communications between the parties, with respect to the Services provided hereunder. In the event that any of the terms set forth in this PID Attachment conflict with the terms set forth in the Agreement, the terms set forth in this PID Attachment shall control.

Experian Information Solutions, Inc.			Print or Type Full Legal Name of Client
By:	Signature (Duly Authorized Representative Only)	**By:**	Signature (Duly Authorized Representative Only)
Name:	Print	**Name:**	Print
Title:		**Title:**	
PID Attachment Effective Date: _____			

ADDENDUM FOR KNOWLEDGE IQ SELECT
TO
ATTACHMENT FOR PRECISE ID TERMS TO EXPERIAN CROSSCORE SCHEDULE

This Addendum for Knowledge IQ Select ("Addendum") supplements the Attachment for Precise ID Terms ("PID Attachment") to the Experian CrossCore Schedule dated ("CrossCore Schedule") currently in place between Experian and Client. All capitalized terms not otherwise defined herein shall have the meanings ascribed to such terms in PID Attachment, the CrossCore Schedule, and the Agreement.

1. Services. This Addendum applies to Experian's provision of additional questions utilizing data licensed from a third-party provider (together with the information contained therein, the "Knowledge IQ Select"), which will be integrated with Experian's Knowledge IQ through Precise ID Services. The defined term "Precise ID Services" as used in PID Attachment shall include Knowledge IQ Select. Experian will provide Knowledge IQ Select to Client for the fees set forth in a Pricing Exhibit.

2. Term. This Addendum shall commence on the Addendum Effective Date set forth below and expire upon the termination or expiration of the CrossCore Schedule; provided that, in addition to the termination rights set forth in the CrossCore Schedule, Experian may terminate this Addendum by providing thirty (30) days' prior written notice to Client in the event that the third-party data utilized in Knowledge IQ Select is no longer provided to Experian.

3. Data Transmittal. Client authorizes Experian to provide Client's inquiry data to Acxiom Identity Solutions, Inc. ("Acxiom") as necessary for the provision of Knowledge IQ Select, which may be disclosed to Acxiom's affiliates or data providers solely in connection with compliance audits, investigations, or complaint responses.

4. DPPA Certification. Client acknowledges that Knowledge IQ Select may contain vehicle ownership data and other motor vehicle department data, and Client shall comply with all requirements in the CrossCore Schedule and PID Attachment applicable to such data. Client certifies to Experian that Client will use Knowledge IQ Select for the following purpose as set forth in the Driver's Privacy Protection Act of 1994 (18 U.S.C. Sec. 2721(b)(3)): for use in the normal course of business to verify the accuracy of information submitted by the consumer and, if such information is not correct, to obtain the correct information, but only for the purposes of preventing fraud by pursuing a legal remedy against, or recovering on a debt or security interest against, the individual.

5. Alternate Source Data. Client acknowledges that Knowledge IQ Select contains Alternate Source Data, and Client shall comply with all requirements in the CrossCore Schedule and PID Attachment applicable to Alternate Source Data. Without limiting the foregoing, Client shall not use Knowledge IQ Select in whole or in part (a) for any purposes enumerated in the FCRA in lieu of obtaining a consumer report as defined in the FCRA ("Consumer Report"); (b) for the purpose of serving as a factor in establishing an individual's eligibility for personal credit or insurance or assessing risks associated with existing credit obligations, evaluating an individual for employment purposes, determining an individual's eligibility for a license or other benefit that depends on an applicant's financial responsibility or status, or for any other purpose under the FCRA; or (c) in the preparation of a Consumer Report or in such manner that may cause Knowledge IQ Select to be characterized as a Consumer Report. Client further agrees that no adverse action (as defined in the FCRA), which is based in whole or in part on information obtained from Knowledge IQ Select, may be taken against any consumer.

6. Data Use Restrictions. In addition to the use restrictions set forth in the CrossCore Schedule, PID Attachment, or elsewhere in the Agreement:

a. Client shall not deny any consumer access to any of Client's online or other services based in whole or in part on Knowledge IQ Select. Knowledge IQ Select shall only be used to permit access to, or refer a consumer to, Client's additional authentication processes, and any denial of access must be based solely on such additional authentication processes.

b. Client shall only use Knowledge IQ Select for the permitted uses under the Driver's Privacy Protection Act of 1994 and the Gramm-Leach Bliley Act to which Client has certified in this Addendum and in the CrossCore Schedule and PID Attachment. Without limiting the foregoing, Knowledge IQ Select may not be used in any manner which could be considered marketing or a solicitation, or for any illegal purposes, including, without limitation, for the purpose of intimidating, stalking or harassing any person or entity.

c. Client acknowledges that the government has placed restrictions upon the use of cell phone numbers. Client agrees that any use of the cell phone numbers provided as part of Knowledge IQ Select will be used in strict accordance with all applicable laws, rules, and regulations.

d. Client shall hold Knowledge IQ Select in confidence, using no less than a reasonable degree of care. Client shall use information obtained from each individual request for Knowledge IQ Select only for the particular permitted uses and transaction for which Client made such request. Knowledge IQ Select shall only be used by Client's designated and authorized employees having a need to know and only to the extent necessary to enable Client to use Knowledge IQ Select in accordance with this Addendum and the Agreement. Such designated and authorized employees of Client shall only access Knowledge IQ Select in the exercise of their official duties.

e. Client shall remain responsible for protecting Knowledge IQ Select (and any log-in credentials used to access such questions) from unauthorized use or disclosure.

7. Domestic Access and Use. Client shall not access or use Knowledge IQ Select outside of the United States or its territories. Any access to or use of Knowledge IQ Select outside of the United States or its territories shall require the prior written approval of Experian, which approval shall be signed by Experian on or after the Addendum Effective Date and shall specifically reference access to Knowledge IQ Select.

8. Post-Termination Requirements. Upon termination of this Addendum for any reason, Client agrees to cease using any and all data or information contained in, or obtained from, Knowledge IQ Select, and to remove all such data or information from its systems, including any back-ups and all other means of storage, magnetic, electronic or otherwise, shall immediately be permanently erased

or destroyed; provided, however, that all data in Client's nonproduction back-up systems shall be removed after no more than seven (7) years in accordance with Client's retention policies. If requested by Experian, Client will provide written certification of such destruction within thirty (30) days following Experian's request.

This Addendum, together with the Agreement (and the applicable schedules and supplements thereto), as amended, constitutes the entire agreement between the Parties with respect to Knowledge IQ Select Services provided hereunder and supersedes all prior proposals and agreements, both written and oral, and all other written and oral communications between the Parties, with respect to Knowledge IQ Select provided hereunder. In the event that any of the terms set forth in this Addendum conflict with the terms set forth in the Agreement, the terms set forth in this Addendum shall control.

Experian Information Solutions, Inc.

By: _____
Signature (Duly Authorized Representative Only)

Name: _____
Print

Title: _____

Addendum Effective Date: _____

_____
Print or Type Full Legal Name of Client

By: _____
Signature (Duly Authorized Representative Only)

Name: _____
Print

Title: _____

ADDENDUM FOR SYNTHETIC ID SERVICES
TO
ATTACHMENT FOR PRECISE ID TERMS TO EXPERIAN CROSSCORE SCHEDULE

This Addendum for Synthetic ID Services ("Addendum"), supplements the Attachment for Precise ID Terms ("Attachment"), to the Experian CrossCore Schedule dated ("CrossCore Schedule"), currently in place between Experian and Client. All capitalized terms not otherwise defined herein will have the meanings ascribed to such terms in Attachment, the CrossCore Schedule, and the Agreement.

1. Services. This Addendum applies to Experian's provision of synthetic identity services, which will be integrated with Experian's Precise ID Services and consist of two options (1) High Risk Fraud Score services, and (2) Synthetic ID Detection Rules services (collectively, the "Synthetic ID Services"). Experian will provide the Synthetic ID Services to Client for the fees set forth in the applicable pricing exhibit.

a. High Risk Fraud Score evaluates credit data to detect the presence of a synthetic identity. This score is separate from the Precise ID Services score and may be used with Experian's Precise ID FCRA Account Opening option only.

b. Synthetic ID Detection Rules incorporate credit and non-credit data to assess a set of conditions associated with synthetic identities. The rules are delivered separately from the Precise ID Services score and may be used in both GLB and FCRA versions of Precise ID Services.

2. Term. This Addendum will commence on the Addendum Effective Date set forth below and expire as set forth on the applicable pricing document, or, if earlier, upon the termination or expiration of the Attachment; subject to the termination rights set forth in the Agreement.

3. Outcome Reporting. Client agrees to provide Experian confirmed fraud feedback monthly during the Term based on its use of the Synthetic ID Services ("Outcome Reporting") in the format specified by Experian, or as otherwise agreed by the parties in writing. Outcome Reporting shall include without limitation, effectiveness and whether real consumers are flagged as synthetic. Experian may use Outcome Reporting for general product research and development after extraction of information identifying Client and consumers.

4.. Client's Certification of Use.

a. High Risk Fraud Score and Synthetic ID Detection Rules (with FCRA-Regulated Versions of Precise ID): For Client's use of the High Risk Fraud Score or use of the Synthetic ID Detection Rules with an FCRA-regulated version of Precise ID (including Precise ID for Account Opening), Client certifies that it will obtain and use as Client's sole permissible purpose under the FCRA either

(i) the consumer's written instructions pursuant to Section 7 of the Attachment;

(ii) where Client has a "legitimate business need for the information in connection with a business transaction that is initiated by the consumer" pursuant to Section 3.B. of the Attachment, and for which Client has a risk of financial loss in connection with one of the following transactions:

- Tenant Screening
- DDA Checking Account Opening
- Consumer pays by check
- Card not present (online payments);

or (iii) where Client has an open or active credit account with the consumer, to review the consumer's account to determine whether the consumer continues to meet the terms of the account,

b. Synthetic ID Detection Rules (with GLB-Regulated Versions of Precise ID): When using the Synthetic ID Detection Rules with a GLB-regulated version of Precise ID, Client certifies that it will use the Services solely to protect against or prevent actual or potential fraud, unauthorized transactions, claims or other liability under the Gramm-Leach-Bliley Act, 15 U.S.C.A. Sec 6801, *et seq*.

5. Data Use Restrictions. In addition to the use restrictions set forth in the Attachment or elsewhere in the Agreement:

a. Client will use the Synthetic ID Services solely to validate a consumer's identity or information for the purposes of fraud avoidance, identity verification, transaction authentication in connection with commercial transactions undertaken by a consumer with Client. Client shall not use the Synthetic ID Services or output for any other purpose, including without limitation, creating an internal database for any future purpose. Client will not use the Synthetic ID Services for marketing or solicitation, or for any illegal purposes, including, without limitation, for the purpose of intimidating, stalking or harassing any person or entity.

b. Client will not use the Synthetic ID Services in whole or in part (i) for any purposes enumerated in the FCRA in lieu of obtaining a consumer report as defined in the FCRA ("Consumer Report"); (ii) for the purpose of serving as a factor in establishing an individual's eligibility for personal credit or insurance or assessing risks associated with existing credit obligations, evaluating an individual for employment purposes, determining an individual's eligibility for a license or other benefit that depends on an applicant's financial responsibility or status, or for any other purpose under the FCRA; or (iii) in the preparation of a Consumer Report or in such manner that may cause the Synthetic ID Services to be characterized as a Consumer Report. Client further agrees that no adverse action (as defined in the FCRA), which is based in whole or in part on information obtained from the Synthetic ID Services, may be taken against any consumer.

c. Client will not deny any consumer access to any of Client's online or other services based in whole or in part on the Synthetic ID Services. The Synthetic ID Services will only be used to permit access to, or refer a consumer to, Client's additional authentication processes, and any denial of access must be based solely on such additional authentication processes.

d. Client may not resell, distribute, sublicense, or otherwise transfer the Synthetic ID Services or any of the data from the Synthetic ID Services to any third party.

e. Client will not (i) knowingly use the Synthetic ID Services in any manner that that may disable, impair, damage or interfere with any of the Synthetic ID Services, (ii) attempt to access or access or use the Synthetic ID Services in any unauthorized or illegal manner, (iii) reproduce, copy, sell, exploit, or transfer the Synthetic ID Services, or any portion of the Synthetic ID Services, or the rights to use the Synthetic ID Services, (iv) alter, modify, revise, or adapt the

Synthetic ID Services, in part or in whole, (v) create any derivative works from the Synthetic ID Services or any portion thereof, or reverse engineer, disassemble or decompile the Synthetic ID Services or any data or software contained therein, or (vi) use the Synthetic ID Services to construct products or services that are intended to displace or complete with the Synthetic ID Services.

f. Client will not use the Synthetic ID Services to transmit Inappropriate Content. "Inappropriate Content" means any content that is (i) unsolicited, including without limitation, unauthorized "bulk" messages, and (ii) a cause of the introduction of "viruses," "worms," "Trojan Horses," "e-mail bombs," "cancelbots" or other similar computer programming routines into the Services; (iii) unlawful; (iv) infringes the intellectual property rights of any person; or (v) executes, initiates or causes "phishing" or social engineering activities.

g. ***When using the High Risk Fraud Score*** Client shall not use information, including without limitation, scores, flags or other output, it receives from each Synthetic ID Services inquiry/transaction for any other purpose except that particular single inquiry/transaction made by Client. For example, Client shall not, without limitation, use the High Risk Fraud Score to create a negative list or blacklist for future use.

6. Domestic Access and Use. Client will not access, store, transmit, or use the Synthetic ID Services, or data obtained from the services, outside of the United States or its territories without the prior written approval of Experian, which approval must specifically reference access to the Synthetic ID Services outside of the United States, along with any applicable conditions for such access.

This Addendum, together with the Agreement (and the applicable schedules and supplements thereto), as amended, constitutes the entire agreement between the parties with respect to the Synthetic ID Services provided hereunder and supersedes all prior proposals and agreements, both written and oral, and all other written and oral communications between the parties, with respect to the Synthetic ID Services provided hereunder. In the event that any of the terms set forth in this Addendum conflict with the terms set forth in the Agreement, the terms set forth in this Addendum will control.

Experian Information Solutions, Inc.		_____ Print or Type Full Legal Name of Client
By: _____ Signature (Duly Authorized Representative Only)	**By:**	_____ Signature (Duly Authorized Representative Only)
Name: _____ Print	**Name:**	_____ Print
Title: _____	**Title:**	_____
Addendum Effective Date: _____		

ATTACHMENT FOR FRAUDNET TERMS
TO
EXPERIAN CROSSCORE SCHEDULE

This Attachment for FraudNet Terms (**"FraudNet Attachment"**) supplements the CrossCore Schedule to the Agreement currently in place between Experian and Client. Collectively, the CrossCore Schedule and the Agreement are referred to herein as the "Agreement." All capitalized terms not otherwise defined herein shall have the meanings ascribed to such terms in the Agreement.

1. Definitions

"Deliverable" is any work developed or created by Experian while providing the FraudNet Service to the Client (including a Delivery Plan) to Client.

"DeviceInsight Attributes" refers to the set of device related outputs such as the DeviceInsight Print, Time Differential Linking and "isRisky," generated by the FraudNet Service using the DeviceInsight Collected Data and Web Session Data.

"DeviceInsight Collected Data" refers to the specific properties of visitor devices connected to the Digital Properties that is captured by the DeviceInsight Collector.

"DeviceInsight Print" means a 40-character one-way hash of selected DeviceInsight Collected and Web Session Data generated by the FraudNet Service.

"Digital Properties" means Client's websites and mobile applications as described in the FN Use Case.

"Enrichment Data" means Experian and third-party data Experian uses in calculating the Risk Results for Client, including but not limited to device attributes, event look up data, BIN information lookup time zones, country code lookup data, country code lookup data time zones, internet provider lookup data, and/or internet provider lookup geolocation data.

"FraudNet Suite" means the FraudNet Service, the Licensed Software, other software utilized to provide the FraudNet Service, the DeviceInsight Collected Data, the DeviceInsight Prints, the DeviceInsight Attributes, the Risk Results, the Documentation, the Deliverables, and any other services as Experian may provide to Client from time to time, pursuant to the terms and conditions of this FraudNet Attachment.

"Go-Live Date" means the date that the implementation process and certification for the FraudNet Service as described in 3.a. have been completed.

"FraudNet Service" means the on-demand, Web-based online fraud detection services provided by Experian, including updates to the FraudNet Service, as further described in this FraudNet Attachment.

"Licensed Software" refers, collectively, to the DeviceInsight Collector and the Mobile SDK.

"DeviceInsight Collector" is code licensed for redistribution within Client's Digital Properties. When embedded in an HTML page or deployed in a mobile app on Client's Digital Properties, the DeviceInsight Collector captures the DeviceInsight Collected Data, packaging them into a string for downstream processing for the FN Use Case through the FraudNet Service.

"Mobile SDK" is Experian's mobile application software development kit.

"Risk Results" means the risk output generated by the FraudNet Service through use of the Enrichment Data, including risk score, audit trail and action.

"Subscription Fees" mean the fees paid by Client for the right to access and use the FraudNet Service and receive support for the FraudNet Service during the Term.

"Transaction Data" means the data elements submitted by Client for processing by the FraudNet Service. Client must submit Customer Data, as is entered by Client's customer to make a transaction on Client's website or application, to Experian. Client shall provide PAN, EIN, SSN, and PIN (whether a password or other security code) in a one-way hashed format ("Hashed Information Elements").

"FN Use Case" means the scope of use for which Client is authorized to use the FraudNet Suite as specified in the Pricing Exhibit.

"Web Session Data" refers to the standard data associated with a web session and includes such attributes as (A) the http header information from the session, (B) the full IP address of a visitor to a Digital Property, and (C) a session identifier. Web Session Data is not collected by the DeviceInsight Collector but is submitted by Client's HTTP client.

2. Rights and Licenses

a. DeviceInsight Collector. Use of the FraudNet Service requires deployment of the DeviceInsight Collector. Subject to the terms and conditions set forth in this FraudNet Attachment and the Agreement, Experian grants Client a nonexclusive, non-transferable, non-sublicensable license to reproduce and distribute the DeviceInsight Collector solely for use with a Client Digital Property for the sole purpose of capturing DeviceInsight Collected Data for transmission with the Web Session Data to the FraudNet Service in order for the FraudNet Service to generate the DeviceInsight Print.

b. Mobile SDK. Subject to the terms and conditions set forth in this FraudNet Attachment and the Agreement, Experian grants Client a nonexclusive, non-transferable, non-sublicensable license during the Term to install and use the Mobile SDK internally only for the sole purpose of designing, developing, and implementing a data transfer process for Client to upload visitor data from mobile devices operating the iOS or Android OS to the FraudNet Service and to transmit data to and from the FraudNet Service.

c. Client represents and warrants to Experian that: (i) it owns all right, title and interest, or possesses sufficient rights, in and to the Transaction Data and Web Session Data as may be necessary to permit the transmission, collection, storage, ownership and use of such data, as contemplated herein; and (ii) the Transaction Data and Web Session Data have been collected in accordance with all applicable laws, including regulations, and attorney general or agency guidance, guides, or rulemaking.

d. Client's right to use the Risk Results and any Enrichment Data therein is a personal, nontransferable, and nonexclusive license, limited to the Term for Client's internal business purposes.

3. Implementation and Use of the FraudNet Service

a. Implementation of the FraudNet Service. Implementation services will be performed according to Experian's implementation framework, configured in the manner prescribed by Experian. Client will pay a fee as set forth in Pricing Exhibit for these implementation services. Upon completion of the implementation process, Client will follow Experian's certification process prior to using the FraudNet Service in production. Any deviation from the plan, as well as any additional services requested by Client, will be billable at Experian's standard service rate then in effect; provided, however, that, Experian must obtain Client's advance written approval prior to performing any services deemed billable.

b. Use of the FraudNet Suite. Client will not (i) use the FraudNet Suite in any manner that is beyond the scope of the rights granted in this FraudNet Attachment; (ii) remove or obscure any copyright notice or other notice or terms of use contained in the Enrichment Data; or (iii) use the Enrichment Data to create or otherwise support the transmission of unsolicited, commercial email.

c. Restrictions on Use of FraudNet Suite. Client may not use the FraudNet Suite (including, without limitation, the FraudNet Service and

ATTACHMENT FOR FRAUDNET TERMS
TO
EXPERIAN CROSSCORE SCHEDULE

any Risk Results) as a factor in establishing a consumer's eligibility for credit, insurance, housing, employment or other eligibility or entitlement, or for any other use constituting a permissible purpose under the Fair Credit Reporting Act (**"FCRA"**), or otherwise in violation of any other applicable laws. Client acknowledges that none of the data used by Experian to provide the FraudNet Service has been collected by Experian for credit purposes, nor is it intended to be indicative of any consumer's credit worthiness, credit standing, credit capacity or other characteristics listed in Section 603(d) of the FCRA.

4. Term and Termination.

Unless terminated earlier pursuant to the Agreement or the CrossCore Schedule, this FraudNet Attachment shall commence on the FraudNet Attachment Effective Date and continue for the period set for the on the applicable Pricing Exhibit (the "Initial Term"). Thereafter, this FraudNet Attachment shall automatically renew for additional successive one (1) year terms (each a "Renewal Term") until either party provides the other party with sixty (60) days written notice of non-renewal prior to the end of the then current term (the Initial Term and the Renewal Term(s) collectively, the "Term").

Upon termination of the Agreement or this FraudNet Attachment for any reason, Client shall immediately discontinue use of the FraudNet Services, including updates and upgrades thereto, and any portion thereof, and return (or at Experian's option, destroy with certification to Experian) the same. Termination of this FraudNet Attachment does not relieve Client of its obligations under this FraudNet Attachment that call for performance after the termination date.

5. Ownership. As between Experian and Client, Experian retains all ownership and intellectual property rights in the FraudNet Suite (including the Transaction Data and the Web Session Data). Experian and applicable third parties shall retain all intellectual property rights in the Enrichment Data. For the avoidance of doubt, Client shall have no intellectual property right in the Enrichment Data.

5. Limitation of Liability for Enrichment Data. FOR THE AVOIDANCE OF DOUBT, AND NOTWITHSTANDING ANY OTHER PROVISION OF THIS FRAUDNET ATTACHMENT, THE CROSSCORE SCHEDULE OR THE AGREEMENT, IN NO EVENT SHALL EXPERIAN OR ANY THIRD PARTY PROVIDING ENRICHMENT DATA BE LIABLE TO THE CLIENT FOR ANY INCIDENTAL, INDIRECT, CONSEQUENTIAL, PUNITIVE OR SPECIAL DAMAGES (INCLUDING BUT NOT LIMITED TO DAMAGES TO BUSINESS REPUTATION, LOST BUSINESS, OR LOST PROFITS), WHETHER FORESEEABLE OR NOT AND HOWEVER CAUSED BY THE ENRICHMENT DATA OR CLIENT'S USE OF THE ENRICHMENT DATA, REGARDLESS OF THE THEORY OF LIABILITY (INCLUDING NEGLIGENCE AND STRICT LIABILITY), EVEN IF THE PARTIES ARE AWARE OR ADVISED OF THE POSSIBILITY THAT SUCH DAMAGES MIGHT ARISE.

6. Warranties

a. Licensed Software Warranty. Experian warrants that the current version of the Licensed Software will perform in all material respects in accordance with the Documentation furnished to Client by Experian for use with the FraudNet Service. In the event the current version of the Licensed Software is nonconforming, Experian will fix, provide a work around, or otherwise repair or replace the nonconforming Licensed Software, or, if Experian is unable to do so, terminate Client's access to the FraudNet Service and return Subscription Fees for the FraudNet Service previously paid to Experian for the period beginning with Client's notice of nonconformity through the remainder of the Term. Experian will have no liability under the foregoing warranty if the failure to conform is caused in whole or part by persons other than Experian, or by products, equipment or computer programs not furnished by Experian, or by Client's use of a non-current version of the Licensed Software. Notwithstanding the foregoing, Client shall be solely responsible for maintaining its Internet connection or dedicated communications line in good working condition and shall be solely responsible for any disruption in its ability to use the FraudNet Service that results from failures or malfunctions of its data communications line to Experian. NEITHER EXPERIAN NOR ANY THIRD PARTY MAKES ANY WARRANTY AS TO THE ENRICHMENT DATA. EXPERIAN DOES NOT WARRANT THAT THE ACCESS TO AND OPERATION OF THE SERVICES WILL BE UNINTERRUPTED OR ERROR-FREE, OR THAT ALL PROGRAMMING ERRORS WILL BE CORRECTED. ALSO, EXPERIAN DOES NOT WARRANT THAT THE FUNCTIONS CONTAINED IN THE FRAUDNET SUITE WILL OPERATE IN THE COMBINATION CLIENT SELECTS OR WILL MEET CLIENT'S REQUIREMENTS.

b. DISCLAIMERS OF WARRANTIES. EXCEPT AS OTHERWISE EXPRESSLY PROVIDED IN THIS FRAUDNET ATTACHMENT, THE FRAUDNET SUITE IS SUBJECT TO THE DISCLAIMERS OF WARRANTIES PROVIDED IN SECTION 7 OF THE CROSSCORE SCHEDULE.

This FraudNet Attachment, together with the Agreement (and the applicable schedules, supplements and exhibits thereto), as amended, constitutes the entire agreement between the Parties with respect to Services provided hereunder and supersedes all prior proposals and agreements, both written and oral, and all other written and oral communications between the parties, with respect to the Services provided hereunder. In the event that any of the terms set forth in this FraudNet Attachment conflict with the terms set forth in the Agreement, the terms set forth in this FraudNet Attachment shall control.

Experian Information Solutions, Inc.			Print or Type Full Legal Name of Client
By:	Signature (Duly Authorized Representative Only)	**By:**	Signature (Duly Authorized Representative Only)
Name:	Print	**Name:**	Print
Title:		**Title:**	
FraudNet Attachment Effective Date:_____			

ATTACHMENT FOR DIGITAL RISK SCORE TERMS
TO
EXPERIAN CROSSCORE SCHEDULE

This Attachment for Digital Risk Score Terms (**"DRS Attachment"**) supplements the CrossCore Schedule to the Agreement currently in place between Experian and Client. Collectively, the CrossCore Schedule and the Agreement are referred to herein as the "Agreement." All capitalized terms not otherwise defined herein shall have the meanings ascribed to such terms in the Agreement.

1. Description of Services.

This DRS Attachment applies to Experian's delivery of Digital Risk Score through CrossCore for the fees set forth in the applicable Pricing Exhibit.

2. Definitions.

"Deliverable" is any work developed or created by Experian while providing DRS Service to Client.

"DeviceInsight Attributes" refers to the set of device related attributes such as the Time Differential Linking and "isRisky," generated by the DRS Service using the DeviceInsight Collected Data and Web Session Data, and used internally to generate the Accept / Not Accept outcome.

"DeviceInsight Collected Data" refers to the specific properties of visitor devices connected to the Digital Properties that is captured by the DeviceInsight Collector.

"DeviceInsight Collector" is code licensed for redistribution within Client's Digital Properties. When embedded in an HTML page or deployed in a mobile app on Client's Digital Properties, the DeviceInsight Collector captures the DeviceInsight Collected Data, packaging them into a string for downstream processing for the Use Case through the DRS Service.

"Digital Properties" means Client's websites and mobile applications as described in the Use Case.

"**Enrichment Data**" means Experian and third-party data Experian uses in calculating the Risk Results for Client, including but not limited to device attributes, event look up data, BIN information lookup time zones, country code lookup data, country code lookup data time zones, internet provider lookup data, and/or internet provider lookup geolocation data.

"**DRS Service**" means the fraud detection services provided by Experian to Client, as described herein, the Licensed Software, other software utilized to provide the Service, the DeviceInsight Collected Data, the DeviceInsight Attributes, the Risk Results, the Documentation, the Deliverables and any other services as Experian may provide to Client from time to time, pursuant to the terms and conditions of this DRS Attachment. DRS Service is an Experian Service (as defined in the CrossCore Schedule).

"Go-Live Date" means the date that the implementation process and certification described in Section 4.b. have been completed.

"Licensed Software" refers, collectively, to the DeviceInsight Collector and the Mobile SDK.

"Mobile SDK" is Experian's mobile application software development kit.

"Risk Results" means the risk output, based on Client's transaction decision matrix, generated by the DRS Service, including audit trail and recommended action.

"Subscription Fees" mean the fees paid by Client for the right to access and use the DRS Service for the DRS Service during the applicable DRS Term.

"Transaction Data" means the data elements submitted by Client to the DRS Service for processing. Client must submit its Customer Data, as is entered by the Client's customer to make a transaction on the Client's website or application, to Experian, which shall include name, billing address, shipping address, phone number, and email. Client shall provide PAN, EIN, SSN, and PIN (whether a password or other security code) in a one-way hashed format ("Hashed Information Elements").

"**Use Case**" means the scope of use for which Client is authorized to use the DRS as specified in the Pricing Exhibit.

"Web Session Data" refers to the standard data associated with a web session and includes such attributes as (A) the http header information from the session, (B) the full IP address of a visitor to a Digital Property, and (C) a session identifier. Web Session Data is not collected by the DeviceInsight Collector but is submitted by Client's HTTP client.

3. Term and Termination.

Unless terminated earlier pursuant to the Agreement or the CrossCore Schedule, this DRS Attachment shall commence on the DRS Attachment Effective Date and continue for the period set for the on the applicable Pricing Exhibit (the "Initial Term"). Thereafter, this DRS Attachment shall automatically renew for additional successive one (1) year terms (each a "Renewal Term") until either party provides the other party with sixty (60) days written notice of non-renewal prior to the end of the then current term (the Initial Term and the Renewal Term(s) collectively, the "Term").

Upon termination of the Agreement or this DRS Attachment for any reason, Client shall immediately discontinue use of the Digital Risk Score, including updates and upgrades thereto, and any portion thereof, and return (or at Experian's option, destroy with certification to Experian) the same. Termination of this DRS Attachment does not relieve Client of its obligations under this DRS Attachment that call for performance after the termination date.

4. Provision of Digital Risk Score.

a. Availability of Digital Risk Score. Client's use of the DRS Service and related services are limited to its internal business purposes solely for the scope and use limitations specified herein.

b. Implementation of the DRS Service. Implementation services will be performed according to Experian's implementation framework, configured in the manner prescribed by Experian. Client will pay a fee as set forth in Pricing Exhibit for these implementation services. Upon completion of the implementation process, Client will follow Experian's certification process prior to using the DRS Service in production. Any deviation from the plan, as well as any additional services requested by Client, will be billable at Experian's standard service rate then in effect; provided, however, that, Experian must obtain Client's advance written approval prior to performing any services deemed billable.

c. Licensed Software Provided for Use with the DRS Service. Subject to the terms and conditions of this DRS Attachment, Experian grants Client the following nonexclusive, nontransferable licenses to use the Licensed Software solely as authorized below:

i. *DeviceInsight Collector*. Use of the DRS Service requires deployment of the DeviceInsight Collector. Subject to the terms and conditions set forth in this DRS Attachment and the Agreement, Experian grants Client the nonexclusive, non-transferable, nonexclusive license during the DRS Term to reproduce and distribute the DeviceInsight Collector only in conjunction with and as part of a Client Digital Property for the sole purpose of capturing DeviceInsight Collected Data from visitor devices for transmission, together with the Web Session Data, to the DRS Service for processing.

ii. *Mobile SDK*. Subject to the terms and conditions set forth in this DRS Attachment and the Agreement, Experian grants Client the nonexclusive, non-transferable, nonsublicensable license during the DRS Term to install and use the Mobile SDK internally only for the sole purpose of designing, developing, and implementing a data transfer process for Client to upload visitor data from mobile devices operating the iOS or Android OS to the DRS Service and to transmit data to and from the DRS Service.

5. Limitations on Use of Services.

a. Scope of Use. Client will not (i) use the DRS Service in any manner that is beyond the scope of the rights granted in this DRS Attachment; (ii) remove or obscure any copyright notice or other notice or terms of use contained in the Enrichment Data; or (iii) use the Enrichment Data to create or otherwise support the transmission of unsolicited, commercial email. Client's right to use the Risk Results and any Enrichment Data therein is a personal, nontransferable, and nonexclusive license, limited to the DRS Term for Client's internal business purposes.

b. FCRA Limitations. Client may not use or allow others to use the Digital Risk Score (including, without limitation, any Risk Results) as a factor in establishing a consumer's eligibility for credit, insurance, housing, employment or other eligibility or entitlement, or for any other use constituting a permissible purpose under the Fair Credit Reporting Act ("FCRA"), or otherwise in violation of any other applicable laws. Client acknowledges that none of the data used by Experian to provide the DRS Service has been collected by Experian for credit purposes nor is it intended to be indicative of any consumer's credit worthiness, credit standing, credit capacity or other characteristics listed in Section 603(d) of the FCRA.

c. Access to the DRS Service. Client is responsible for (i) all activities conducted under its User logins; and (ii) obtaining and maintaining the Client Equipment and any ancillary services needed to connect to, access or otherwise use the DRS Service, and ensuring that the Client Equipment and ancillary services comply with the configuration requirements specified by Experian. Client will transmit Transaction Data and Web Session Data to the DRS Service in the format specified by Experian.

d. Domestic Access and Use of DRS Service. Client shall not access, transfer, or use the Digital Risk Score (including the Risk Results and any Enrichment Data therein) outside the United States or its territories. Any direct or indirect access to, transfer, or use of the Digital Risk Score outside the United States or its territories shall require the prior written approval of Experian in a writing signed by an authorized representative of Experian.

6. Intellectual Property Ownership Rights.

a. By Experian. As between Experian and Client, Experian retains all ownership rights in the Digital Risk Score (including the Transaction Data and Web Session Data), including all intellectual property rights. Any and all rights to derivative works, modifications, additions or improvements to any of the Digital Risk Score will remain with and are hereby assigned to Experian, regardless of inventorship or authorship, and regardless of the party suggesting or making the derivative work, modification, addition or improvement. Experian and applicable third parties shall retain all intellectual property rights in the Enrichment Data. For the avoidance of doubt, Client shall have no intellectual property right in the Enrichment Data.

b. Reservation of Rights. Experian reserves all rights not expressly granted in this DRS Attachment. This DRS Attachment is not a sale of the Digital Risk Score (including, without limitation, the Licensed Software and other software utilized to provide the Digital Risk Score or any copy or part of the Digital Risk Score), and Client shall have no title to or ownership in the Digital Risk Score, or any copy or part thereof, regardless of the form on which the original and any copies may exist.

7. Fees.

a. Agreement to Pay. Client agrees to pay Experian fees specified in the Pricing Exhibit.

b. Expenses Reimbursement. Client will reimburse Experian for all reasonable, pre-approved and appropriately documented travel and related expenses incurred by Experian in performing any services at Client's location. Client will be responsible for its own travel and out-of-pocket expenses associated with attending any training services.

8. Infringement Indemnification.

a. Infringement. Experian agrees to indemnify and hold harmless Client from any and all loss, liability and expense (including reasonable attorneys' fees and court costs) incurred by Client as a result of any third party claim, demand or action against Client based on, related to or arising out of any claim that Licensed Software infringes any presently existing U.S. patent, copyright or trade secret of such third party. If such third party claim has occurred, or in Experian's judgment is likely to occur, Client agrees to allow Experian, at Experian's option and expense, (i) to procure the right for Client to continue using the Licensed Software in accordance with this DRS Attachment, or (ii) to replace or modify the Licensed Software in a functionally equivalent manner so that they become non-infringing. In the event that the above remedies are not available on commercially reasonable terms, Experian may refund to Client an amount equal to the unused portion of the fees paid by Client (calculated on a monthly basis from the effective date of termination through the end of the then current term), and terminate this DRS Attachment.

b. Conditions to Indemnification. The foregoing indemnity shall be contingent upon (i) Client giving prompt written notice to Experian of any claim, demand or action for which indemnity is sought; and (ii) Client fully cooperating in the defense or settlement of any such claim, demand or action, at the expense of Experian. Experian shall have no liability for any claim of infringement to the extent such a claim is based upon Client's use of (a) the Licensed Software which diverges in any way from a current unaltered release of the Service available from Experian (if such infringement would have been avoided by the use of such current unaltered release); or (b) the Licensed Software in combination with programs or data not provided by Experian. THIS SECTION 8 STATES EXPERIAN'S ENTIRE LIABILITY, AND CLIENT'S SOLE AND EXCLUSIVE REMEDY, REGARDING INTELLECTUAL PROPERTY INFRINGEMENT.

9. Limitation of Liability for Enrichment Data.

FOR THE AVOIDANCE OF DOUBT, AND NOTWITHSTANDING ANY OTHER PROVISION OF THIS DRS ATTACHMENT OR THE AGREEMENT, IN NO EVENT SHALL EXPERIAN OR ANY THIRD PARTY PROVIDING ENRICHMENT DATA BE LIABLE TO THE CLIENT FOR ANY INCIDENTAL, INDIRECT, CONSEQUENTIAL, PUNITIVE OR SPECIAL DAMAGES (INCLUDING BUT NOT LIMITED TO DAMAGES TO BUSINESS REPUTATION, LOST BUSINESS, OR LOST PROFITS), WHETHER FORESEEABLE OR NOT AND HOWEVER CAUSED BY THE ENRICHMENT DATA OR CLIENT'S USE OF THE ENRICHMENT DATA, REGARDLESS OF THE THEORY OF LIABILITY (INCLUDING NEGLIGENCE AND STRICT LIABILITY), EVEN IF THE PARTIES ARE AWARE OR ADVISED OF THE POSSIBILITY THAT SUCH DAMAGES MIGHT ARISE.

10. Warranties

a. Client Warranty. Client represents and warrants to Experian that: (i) Client shall comply with all federal, state and local laws, rules regulations and decisions applicable to Client's collection and provision to Experian of the Transaction Data and Web Session Data and Client's use of the Digital Risk Score provided pursuant to this DRS Attachment; (ii) Client owns all right, title and interest, or possesses sufficient rights, in and to the Transaction Data and Web Session Data as may be necessary to permit the transmission, collection, storage, ownership and use of the Transaction Data and Web Session Data contemplated herein; and (iii) the Transaction Data and Web Session Data has been collected in accordance with all applicable laws (including regulations and attorney general or agency guidance, guides, or rulemaking).

B. Experian Licensed Software Warranty. Experian warrants that the current version of the Licensed Software will perform in all material respects in accordance with the Documentation furnished to Client by Experian for use with the DRS Service. In the event the current version of the Licensed Software is nonconforming, Experian will fix, provide a work around, or otherwise repair or replace the nonconforming Licensed Software, or, if Experian is unable to do so, terminate Client's access to the DRS Service and return Subscription Fees for the DRS Service previously paid to Experian for the period beginning with Client's notice of nonconformity through the remainder of the DRS Term. Experian will have no liability under the foregoing warranty if the failure to conform is caused in whole or part by persons other than Experian, or by products, equipment or computer programs not furnished by Experian. Notwithstanding the foregoing, Client shall be solely responsible for maintaining its Internet connection or dedicated communications line in good working condition and shall be solely responsible for any disruption in its ability to use the DRS Service that results from failures or malfunctions of its data communications line to Experian. EXPERIAN AND ANY THIRD PARTIES MAKE NO WARRANTIES AS TO THE ENRICHMENT DATA. EXPERIAN DOES NOT WARRANT THAT THE ACCESS TO AND OPERATION OF THE SERVICES WILL BE UNINTERRUPTED OR ERROR-FREE, OR THAT ALL PROGRAMMING ERRORS WILL BE CORRECTED. ALSO, EXPERIAN DOES NOT WARRANT THAT THE FUNCTIONS CONTAINED IN THE DIGITAL RISK SCORE WILL OPERATE IN THE COMBINATION WHICH MAY BE SELECTED FOR USE BY CLIENT OR WILL MEET CLIENT'S REQUIREMENTS.

c. DISCLAIMERS OF WARRANTIES. EXCEPT AS OTHERWISE EXPRESSLY PROVIDED IN THIS DRS ATTACHMENT, THE DRS SERVICES ARE LICENSED AND PROVIDED "AS IS" WITHOUT ANY WARRANTY AS TO THEIR PERFORMANCE, ACCURACY, OR FREEDOM FROM ERROR, OR AS TO ANY RESULTS GENERATED THROUGH THEIR USE, INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF QUIET ENJOYMENT, DATA ACCURACY, SYSTEM INTEGRATION, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE

.

This DRS Attachment, together with the Agreement (and the applicable schedules, supplements and exhibits thereto), as amended, constitutes the entire agreement between the Parties with respect to Services provided hereunder and supersedes all prior proposals and agreements, both written and oral, and all other written and oral communications between the parties, with respect to the Services provided hereunder. In the event that any of the terms set forth in this DRS Attachment conflict with the terms set forth in the Agreement, the terms set forth in this DRS Attachment shall control.

Experian Information Solutions, Inc.			Print or Type Full Legal Name of Client
By:	Signature (Duly Authorized Representative Only)	**By:**	Signature (Duly Authorized Representative Only)
Name:	Print	**Name:**	Print
Title:		**Title:**	
DRS Attachment Effective Date:_____			

ADDENDUM FOR MULTI-FACTOR AUTHENTICATION SERVICES
TO
ATTACHMENT FOR PRECISE ID TERMS TO EXPERIAN CROSSCORE SCHEDULE

This Addendum for Multi-Factor Authentication Services ("Addendum"), supplements the Attachment for Precise ID Terms ("Precise ID Attachment") to the Experian CrossCore Schedule, ("CrossCore Schedule"), currently in place between Experian and Client. All capitalized terms not otherwise defined herein will have the meanings ascribed to such terms in the Precise ID Attachment.

1. Services. This Addendum applies to Experian's resale of services utilizing phone number verification and identification data licensed from third-party providers Telesign Corporation ("Telesign") and/or Danal, Inc. ("Danal"), which will be inserted into and leveraged by the Precise ID Services in order for Experian to deliver a "Pass" or "REFER" decision to Client through CrossCore in accordance with the terms of this Addendum (collectively, the "Multi-Factor Authentication Services"). For the avoidance of doubt, (i) the Multi-Factor Authentication Services shall be considered Services for purposes of the Agreement, and Ancillary Services for purposes of the CrossCore Services Schedule, and (ii) this Addendum shall be considered a Services Addendum for purposes of the CrossCore Schedule. Experian will deliver the Multi-Factor Authentication Services to Client for the fees set forth in the attached pricing exhibit.

2. Term. This Addendum will commence on the Addendum Effective Date set forth below and expire upon the termination or expiration of the Precise ID Attachment; provided that, in addition to the termination rights set forth in the CrossCore Schedule and Agreement, Experian may terminate this Addendum by providing thirty (30) days' prior written notice to Client in the event that the third-party services or data utilized in the Multi-Factor Authentication Services is no longer licensed to Experian.

3. Data Transmittal. Client authorizes Experian to provide Client's consumer inquiry data ("Inquiry Data") to Telesign and/or Danal as necessary for the provision of the Multi-Factor Authentication Services. Client acknowledges and agrees that Inquiry Data may be disclosed to Telesign and/or Danal's affiliates or data providers, as applicable, solely in connection with compliance audits, investigations, or complaint responses. Client acknowledges that any Inquiry Data provided to Telesign by Client or Experian, including personally identifiable consumer information, may be processed by Telesign outside of the United States. The Inquiry Data provided to Telesign will be limited to consumer phone numbers.

4. Representations and Warranties. In addition to the representations and warranties in the Precise ID Attachment or elsewhere in the Agreement, Client represents and warrants the following in connection with its use of the Multi-Factor Authentication Services.

a. The Inquiry Data collected from the consumer will be the minimum necessary for the use which the consumer is consenting.

b. Client will obtain the applicable consumer's consent for provision of the Inquiry Data to third parties.

c. Client will obtain clear and conspicuous authorization from the consumer allowing and directing the consumer's mobile carrier to discloe the consumer's mobile account details, along with a list of the specific details, for the purpose of verifying the consumer's identity. Such language could include, or be substantially similar to:

> *By clicking on SUBMIT, you authorize your wireless operator to disclose to us your account, subscriber, device and billing information if available, to support verification of your identity. Where applicable, this information may also be shared by us with other companies to support your transactions and for fraud avoidance purposes. You can find more detail about how we use your data at our Privacy Policy*

d. Where applicable, at the point of collecting the consumer phone number, Client will obtain consent to disclose the consumer's mobile number for the purpose of contacting the consumer via SMS text message for verification purposes. Such language could include, or be substantially similar to:

> *You authorize us to use the phone number provided to verify your identity, which may include disclosing the phone number provided to a third-party to send you a One-Time Password via SMS text message. If a One-Time Password is sent, mobile messaging rates may apply.*

e. Client will main a record of the consumer consents required herein, which shall be traceable to the consumer transactions and include a date and time stamp.

f. If the consumer consent will be used for more than a single transaction, Client will provide the consumer with information about how to opt out of the program.

g. Client is solely responsible for obtaining the appropriate consumer consent in compliance with the requirements herein and all applicable laws, rules, and regulations.

5. Data Use Restrictions. In addition to the use restrictions set forth in the Precise ID Attachment, the CrossCore Schedule or elsewhere in the Agreement:

a. Client acknowledges that the Multi-Factor Authentication Services contain Alternate Source Data, and Client will comply with all requirements in the Precise ID Attachment applicable to Alternate Source Data.

b. Client will not use the Multi-Factor Authentication Services in whole or in part (a) for any purposes enumerated in the FCRA in lieu of obtaining a consumer report as defined in the FCRA ("Consumer Report"); (b) for the purpose of serving as a factor in establishing an individual's eligibility for personal credit or insurance or assessing risks associated with existing credit obligations, evaluating an individual for employment purposes, determining an individual's eligibility for a license or other benefit that depends on an applicant's financial responsibility or status, or for any other purpose under the FCRA; or (c) in the preparation of a Consumer Report or in such manner that may cause the Multi-Factor Authentication Services to be characterized as a Consumer Report. Client further agrees that no adverse action (as defined in the FCRA), which is based in whole or in part on information obtained from the Multi-Factor Authentication Services, may be taken against any consumer.

c. Client will use the Multi-Factor Authentication Services solely to validate a consumer's identity or information for the purposes of fraud avoidance, identity verification, transaction authentication in connection with commercial transactions undertaken by a consumer with Client. Client will not use the Multi-Factor Authentication Services for marketing or solicitation, or for any illegal purposes, including, without limitation, for the purpose of intimidating, stalking or harassing any person or entity.

d. Client will not deny any consumer access to any of Client's online or other services based in whole or in part on the Multi-Factor Authentication Services. The Multi-Factor Authentication Services will only be used to permit access to, or refer a consumer to, Client's

additional authentication processes, and any denial of access must be based solely on such additional authentication processes.

e. Client may not resell, distribute, sublicense, or otherwise transfer the Multi-Factor Authentication Services or any of the data from the Multi-Factor Authentication Services to any third party.

f. Client will only use the Multi-Factor Authentication Services for the permitted uses under the Driver's Privacy Protection Act of 1994 and the Gramm-Leach Bliley Act to which Client has certified in this Addendum and in the Precise ID Attachment.

g. Client acknowledges that the government has placed restrictions upon the use of cell phone numbers. Client agrees that any use of the cell phone numbers provided by as part of the Multi-Factor Authentication Services will be used in strict accordance with all applicable laws, rules, and regulations. Client will not use the Multi-Factor Authentication Services, in part or in whole, for any purpose, or in any way, prohibited by any local, state, national or international laws, regulations, or orders applicable to Client's use of the Multi-Factor Authentication Services.

h. Client will not (i) knowingly use the Multi-Factor Authentication Services in any manner that that may disable, impair, damage or interfere with any of the Multi-Factor Authentication Services, (ii) attempt to access or access or use in any unauthorized or illegal manner any of Telesign or Danal's software, hardware, applications, services, other accounts, servers, computer systems or networks, or any information or materials, except as expressly authorized in writing, (iii) except as expressly authorized in writing, reproduce, copy, sell, exploit, or transfer the Multi-Factor Authentication Services, or any portion of the Multi-Factor Authentication Services, or the rights to use the Multi-Factor Authentication Services, (iv) alter, modify, revise, or adapt the Multi-Factor Authentication Services, in part or in whole, (v) create any derivative works from the Multi-Factor Authentication Services or any portion thereof, or reverse engineer, disassemble or decompile the Multi-Factor Authentication Services or any data or software contained therein, or (vi) use the Multi-Factor Authentication Services to construct products or services that are intended to displace or complete with the Multi-Factor Authentication Services.

i. Client will not use the Multi-Factor Authentication Services to transmit Inappropriate Content. "Inappropriate Content" means any content that is (a) unsolicited, including without limitation, unauthorized "bulk" messages, and (b) a cause of the introduction of "viruses," "worms," "Trojan Horses," "e-mail bombs," "cancelbots" or other similar computer programming routines into the Telesign or Danal platforms; (c) unlawful; (d) infringes the intellectual property rights of any person; or (e) executes, initiates or causes "phishing" or social engineering activities.

6. Domestic Access and Use. Client will not access, store, transmit, or use the Multi-Factor Authentication Services, or data obtained from the services, outside of the United States or its territories without the prior written approval of Experian, which approval must specifically reference access to the Multi-Factor Authentication Services outside of the United States, along with any applicable conditions for such access.

7. Post-Termination Requirements. Upon termination of this Addendum for any reason, Client agrees to cease using any and all data or information contained in, or obtained from, the Multi-Factor Authentication Services, and to remove all such data or information from its systems, including any back-ups and all other means of storage, magnetic, electronic or otherwise will immediately be permanently erased or destroyed; provided, however, that all data in Client's nonproduction back-up systems will be removed after no more than seven (7) years in accordance with Client's retention policies. If requested by Experian, Client will provide written certification of such destruction within thirty (30) days following Experian's request.

8. EXPERIAN AS RESELLER AND DISCLAIMER OF WARRANTIES. CLIENT ACKNOWLEDGES AND AGREES THAT EXPERIAN IS OPERATING AS A RESELLER OF DANAL AND TELESIGN'S SERVICES, WHICH COMBINE TO FORM THE MULTI-FACTOR AUTHENTICATION SERVICES, AND THAT EXPERIAN CANNOT AND WILL NOT BE A GUARANTOR OF THE ACCURACY OR RELIABILITY OF THE MULTIFACTOR AUTHENTICATION SERVICES. EXPERIAN MAKES NO REPRESENTATION OR WARRANTIES, EXPRESS OR IMPLIED, WITH RESPECT TO THE MULTIFACTOR AUTHENTICATION SERVICES DELIVERED BY EXPERIAN HEREUNDER AND EXPERIAN HEREBY EXPRESSLY DISCLAIMS ALL SUCH WARRANTIES, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, OR FITNESS FOR A PARTICULAR PURPOSE. EXPERIAN DOES NOT WARRANT, REPRESENT OR UNDERTAKE THE OPERATION OF THE MULTIFACTOR AUTHENTICATION SERVICES TO BE UNINTERRUPTED OR ERROR-FREE, NOR DOES EXPERIAN MAKE ANY WARRANTY OR REPRESENTATION REGARDING THE USE OR OUTPUT OF THE MULTIFACTOR AUTHENTICATION SERVICES IN TERMS OF CORRECTNESS, ACCURACY, COMPLETENESS, TIMELINESS, SECURITY, RELIABILITY OR OTHERWISE, OR THAT THE MULTI-FACTOR AUTHENTICATION SERVICES WILL MEET CLIENT'S REQUIREMENTS.

9. Third Party Beneficiaries. Danal and Telesign are third-party beneficiaries with full right, power, and authority to enforce the terms of this Addendum.

This Addendum, together with the CrossCore Schedule and Agreement (and the applicable schedules and supplements thereto), as amended, constitutes the entire agreement between the parties with respect to the Multi-Factor Authentication Services and supersedes all prior proposals and agreements, both written and oral, and all other written and oral communications between the parties, with respect to the Multi-Factor Authentication Services. In the event that any of the terms set forth in this Addendum conflict with the terms set forth in the CrossCore Schedule or Agreement, the terms set forth in this Addendum will control.

Experian Information Solutions, Inc.

By: _____
Signature (Duly Authorized Representative Only)

Name: _____
Print

Title: _____

Addendum Effective Date: _____

_____
Print or Type Full Legal Name of Client

By: _____
Signature (Duly Authorized Representative Only)

Name: _____
Print

Title: _____

EXPERIAN
ADDENDUM TO THE CROSSCORE SCHEDULE
FOR ACUANT SERVICES

This Addendum to the CrossCore Schedule for Acuant Services ("Addendum") supplements the CrossCore Schedule dated ("CrossCore Schedule") and the Experian Standard Terms and Conditions dated (together with the CrossCore Schedule, the "Agreements"), currently in place between Experian and Client. All capitalized terms not otherwise defined herein will have the meanings ascribed to such terms in the Agreements.

1. Acuant Services. This Addendum applies to Experian's provision of Acuant, Inc. ("Acuant") services through CrossCore (the "Acuant Services") to assist Client with verification of identification documents submitted by Client's customers, including photographic facial validation and verification of identifying information. Experian will provide the Acuant Services to Client for the fees set forth in the attached pricing exhibit.

2. Term. This Addendum will commence on the Addendum Effective Date set forth below and expire upon the termination or expiration of the CrossCore Schedule; provided that, in addition to the termination rights set forth in the Agreements, Experian may terminate this Addendum (i) upon ninety (90) days' written notice to Client, in the event that Experian anticipates that it will not have the right to continue to deliver the Acuant Services, or (ii) immediately upon written notice if Client fails to comply with any of the terms and conditions of this Addendum.

3. Data Transmittal. Client authorizes Experian to provide Client's data and information submitted through CrossCore to Acuant, Inc. ("Acuant"). Acuant may use such data and information solely to provide Acuant Services to Client and for Acuant's internal business purposes.

4. Use Scope and Limitations. Client is granted a non-transferable, non-exclusive, terminable, world-wide right use the CrossCore Service to connect to the proprietary Acuant Services for processing and the return of data to a device via the same proprietary interface (the "Application Program Interface" or "API") during the Term specified in Section 2 of this Addendum, subject to the following:

a. Client agrees to prevent unauthorized access to, or use of, the Acuant Services and shall notify Experian as soon as possible if it becomes aware of any unauthorized access or use.

b. Title and full, exclusive ownership rights in the Acuant Services is Acuant's intellectual property.

c. Any rights not explicitly granted to Client hereunder, are reserved to and shall remain solely and exclusively proprietary to Acuant and/or Experian.

d. Client acknowledges that the Acuant Service and API is confidential and proprietary information and contains trade secrets of Acuant or its licensors developed at substantial expense. Client agrees to treat the API and all documentation related to the Acuant Services with at reasonable degree of care and protection. Client will remain obligated, both during the term of this Addendum and thereafter, to hold in confidence its knowledge of the Acuant Services as a trade secret for the benefit of Acuant and its licensors.

5. Consent Required. Client agrees to obtain the consumer's consent to: (i) have a text message sent to them for the purposes of accessing a landing page where they will capture photos of their identification document and capture a "selfie" picture of their face, and (ii) have their selfie image used in the document and identity verification process. At the time the selfie is collected, Client agrees to provide notice that describes why it is being collected and obtains the consumer's affirmative consent to use the photo in the Acuant Service. For example: "By clicking submit, I agree that my photo may be scanned and compared to my [photo ID] for authentication purposes and that I have read and understand the Privacy Policy." Client certifies that Privacy Policy includes details regarding the use and storage practices of Biometric data in accordance with state regulations.

6. No Credit Use. Client will not use the Acuant Services in whole or in part (a) for any purposes enumerated in the Fair Credit Reporting Act, 15 U.S.C. § 1681, *et seq*. ("FCRA") in lieu of obtaining a consumer report as defined in the FCRA ("Consumer Report"); (b) for the purpose of serving as a factor in establishing an individual's eligibility for personal credit, insurance, or employment, or determining an individual's eligibility for a license or other benefit that depends on an applicant's financial responsibility or status, or for any other purpose under the FCRA; or (c) in the preparation of a Consumer Report or in such manner that may cause the Acuant Services to be characterized as a Consumer Report. Client further agrees that no adverse action (as defined in the FCRA), which is based in whole or in part on information obtained from the Acuant Services, may be taken against any consumer.

7. Compliance with Laws. Client agrees to only use the Acuant Services for lawful purposes and not to violate any law of any country or the intellectual property rights of any third party.

8. Disclaimer of Warranties. EXPERIAN AND ACUANT MAKE NO OTHER WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, AND EXPERIAN AND ACUANT SPECIFICALLY DISCLAIM THE WARRANTIES OF FITNESS FOR A PARTICULAR PURPOSE AND MERCHANTABILITY AND NON-INFRINGEMENT IN CONNECTION WITH THE ACUANT SERVICES OR THE API.

9. No Consequential Damages. Experian and Acuant shall not incur any liability for indirect, incidental, special, punitive or consequential damages for claims arising from or related to this Addendum, including without limitation those resulting from the furnishing to or performance or use of the Acuant Services or any component thereof by Client, including but not limited to reliance, cover or loss of anticipated profits or convenience, even if Client has been advised of the possibility of such damages.

10. Jurisdiction. This Addendum is to be governed by and interpreted in accordance with the laws of the State of Delaware, excluding that jurisdiction's choice of law regulations or statutes.

11. Third Party Beneficiary. Client understands and agrees that Acuant shall be a third-party beneficiary of this Acuant Addendum with the full right, power and authority to enforce its terms.

This Addendum, together with the Agreements, as amended, constitutes the entire agreement between the parties with respect to the Acuant Services provided hereunder and supersedes all prior proposals and agreements, both written and oral, and all other written and oral communications between the parties, with respect to the Acuant Services provided hereunder. In the event that any of the terms set forth in this Addendum conflict with the terms set forth in the Agreements, the terms set forth in this Addendum will control.

Experian Information Solutions, Inc.		_____ Print or Type Full Legal Name of Client
By:	_____ Signature (Duly Authorized Representative Only)	**By:** _____ Signature (Duly Authorized Representative Only)
Name:	_____ Print	**Name:** _____ Print
Title:	_____	**Title:** _____
Addendum Effective Date: _____		

EXPERIAN
BizID[SM] SERVICES SUPPLEMENT

This **BizID[SM] Services Supplement** ("Supplement") supplements either the Consumer Services Schedule or the Business Information Services Schedule to the Experian Standard Terms and Conditions, dated ("Agreement"), currently in place between Experian and Client.

1. Services. For the purposes of this Supplement, "Services" shall include the BizID[SM] Check, BizID[SM] Check with Score Services, and BizID Account Opening (collectively the "BizID[SM] Services"). Services also include validations and analytics projects ("Validations") described in a criteria letter and may utilize Depersonalized Data as defined below in Section 6. A criteria letter may include pricing and may be transmitted and approved by the parties via electronic mail.

A. The **BizID[SM] Check and BizID[SM] Check with Score Services** shall mean a service that provides with a single point of input for a Client to verify and validate business and/or business principal information against identifying information contained in multiple Experian databases. The BizID[SM] Check and BizID[SM] Check with Scores includes an option of receipt by Client of GLB-based Services.

B. The **BizID[SM] Account Opening Services** shall mean a service that provides a single point of input for a Client to verify and validate business and/or business principal information. BizID[SM] Account Opening Services also include an option for receipt by Client of FCRA-based scores and also allows for automated decisioning against both business and consumer identifying and credit information contained in multiple Experian databases.

C. For **Validations**, Client shall specify in writing to Experian any information field that can be used by Client to link directly or indirectly to the personally identifiable information of any consumer in the Client data file it provides to Experian for the Services. Client represents to Experian that Client has the authority to provide the data to Experian required for performance of the Services at the time Client provides such data, and agrees that Experian may use Client's consumer data for general product research and development after extraction of information identifying Client and the consumer whose records are utilized.

D. Client may request detailed output for the Services in addition to the fraud risk score, classification type, or final decision.

E. Client agrees to provide Experian confirmed fraud feedback monthly during the Term based on its use of the BizID[SM] Services ("Outcome Reporting") in the format specified by Experian, or as otherwise agreed by the parties in writing. Experian may use Outcome Reporting for general product research and development after extraction of information identifying Client and consumers.

F. Except to the extent set forth herein, the term "Services" (as used in the Agreement) shall include the BizID[SM] Services and Validations, and the terms and conditions in the Agreement relating to Services will apply to the BizID[SM] Services and Validations described herein. Experian will provide the Services to Client for the fees set forth in the pricing schedule for this Supplement.

2. Term. Unless a term is specified, this Supplement shall commence on the Effective Date and continue in force and effect to run coterminous with the Agreement, but Client or Experian may terminate this Supplement upon thirty days prior written notice to the other party.

3. Client's Certification of Use

A. GLB Certification. For GLB-based Services, Client certifies to Experian that Client will use the Services to protect against or prevent actual or potential fraud, unauthorized transactions, claims or other liability under the Gramm-Leach-Bliley Act, 15 U.S.C.A. Sec. 6801, *et seq.* Client will not use the "BizID[SM] Check or BizID[SM] Check with Score for the granting or denial of credit or for the setting of credit terms or pricing.

B. Credit Information Certification. It is the position of the Federal Trade Commission that the federal Fair Credit Reporting Act (the "FCRA" – 15 U.S.C. §1681 *et seq*.) governs the use of the consumer credit information contained in BizID[SM] Account Opening or any other Experian services containing consumer credit information. For the FCRA-based Services, Client certifies that it will use Experian consumer credit information provided to Client solely in connection with a current commercial (i.e. not for personal, family or household purposes) credit transaction involving the individual on whom such information is sought, and only if the individual has given written instruction for the provision of such information in accordance with the "permissible purpose" provisions of the FCRA. Every inquiry Client makes on an individual will appear on such individual's Experian consumer credit report and will include Client's business name and address. If Client's "permissible purpose" is based upon the written instructions of the consumer via the Internet, then Client shall obtain the consumer's written instructions in a manner substantially similar to that provided for in Section A of the attached Exhibit A, or if Client obtains the consumer's consent to access credit data over the telephone, Client shall do so as provided for in Section B of Exhibit A. Client acknowledges and agrees that unless the number of inquiries made with respect to a consumer report is among the top four factors adversely affecting the credit score provided as part of the BizID[SM] Services, Experian does not output the same as an adverse action factor. If Client is using the BizID[SM] Services for mortgage lending credit decisions, Client further acknowledges that it must obtain a credit score that will disclose such key factor in accordance with the requirements of Section 609(g) of the FCRA. In any case, Client certifies that it will request and use all data received from Experian solely for its internal purposes in connection with transactions involving the consumer as to whom such information is sought and that it will not provide the Services to any third party.

C. Use of OFAC Data. Matching of names to the OFAC list is based on very limited identification information. A match does not necessarily indicate that the consumer about whom Customer inquired is the same person referenced by OFAC. Accordingly, if Client receives an OFAC result code in Client's BizID[SM] Services, Client acknowledges that any action taken by Client regarding a consumer must be taken based on Client's complete investigation of the consumer and not based solely on the OFAC information.

D. Certification for Use of Motor Vehicle and Property Data. If Client chooses to use vehicle ownership data in the Services, Client certifies that its use is in compliance with the Driver's Privacy Protection Act of 1994 (18 U.S.C. Sec. 2721(b)(3)). Further, motor vehicle department data and

property information will be used solely for authentication purposes.

E. Client's Use of Alternate Source Data. Certain product options offer questions which use information from Experian's non-FCRA data sources ("Alternate Source Data"). Client certifies that it will not use the Alternate Source Data with the FCRA or GLB regulated Services provided hereunder for the granting of or denial of credit or any other FCRA permissible purpose.

4. System Implementation Approval. If applicable, Experian will configure the Services pursuant to specifications provided by Client in the Sign Up Form to be provided to Client under separate cover letter. Upon completion of the configuration, Client shall test and audit performance of the Services to ensure proper configuration. Client shall notify Experian if the Services fail to meet the configuration requirements, and Experian shall modify the configuration to meet Client's requirements set forth in the Sign Up Form. Such modification constitutes Client's sole remedy for failure to configure the Services in accordance with the Sign Up Form and Experian's maximum liability for any such failure.

5. Client Use Restrictions. Except as expressly contemplated by this Supplement, Client shall not (a) distribute, publish, transmit or disseminate, in any form or by any means (including, without limitation, any internet) any part of the Services or the data delivered as part of the Services (the "Data"), (b) allow any third party to access the Services or the Data (including evaluation results), (c) sell, sublicense, resell or otherwise transfer any of the Services or the Data, or (d) use the Services or Data to identify or solicit potential customers for its products or services.

6. Depersonalized (Coded) Data/Historical Validation. Depersonalized Data means certain data about consumers possessed by Experian and retained for modeling and research purposes which has consumers' identifying information coded or masked. Upon Client's request, Experian will provide the Depersonalized Data that may also include a record identifier. Client certifies to Experian that Client has no known ability to, and will not seek to (a) link the Depersonalized Data or record identifier to the individual identity of the consumer, including but not limited to, name, address, social security number, or customer account number, whose credit data is contained in or used to prepare the Services, or (b) otherwise identify the individual identity of the consumer whose credit data is contained in or used to prepare the Depersonalized Data. Client agrees that it will not, either directly or indirectly, itself of through any agent or third party, without the prior written consent of Experian request, compile, store, maintain, resell or use the Depersonalized Data to build its own credit reporting database. Client shall be solely responsible for assuring the secure and confidential manner in which it stores, delivers and transmits the Depersonalized Data to its authorized employee users.

7. Referrals. Client authorizes Experian to use Client's name in any reference list of current clients of BizID[SM] Services.

This Supplement, and if applicable, the Sign Up Form and its Exhibits, together with the Agreement and its applicable Business Services Schedule or Consumer Services Schedule as amended herein constitutes the entire agreement between the parties with respect to the subject matter hereof and supersedes all prior proposals and agreements, both written and oral, and all other written and oral communications between the parties.

Experian Information Solutions, Inc.			
			Print or Type Name of Client
By:	Signature (Duly Authorized Representative Only)	**By:**	Signature (Duly Authorized Representative Only)
Name:	Print	**Name:**	Print
Title:		**Title:**	
Supplement Effective Date: _____			

EXPERIAN
BizID[SM] SERVICES SUPPLEMENT

EXHIBIT A

A. FCRA Compliance--Written Instructions. Client shall substantially comply with the following web site requirements:

(1) Client will prominently display a message specifically informing the consumer that his or her credit profile will be consulted for the purpose for which it is to be used and no other purpose, and that clicking on the "I AGREE" button following such notice constitutes written instructions to the Client under the FCRA. Client agrees that the notice provided by Client will be substantially as follows:

> "You understand that by clicking on the I AGREE button immediately following this notice, you are providing 'written instructions' to (*Client*) under the Fair Credit Reporting Act authorizing (*Client*) to obtain information from your personal credit profile or other information from Experian. You authorize (*Client*) to obtain such information solely to _____ *(insert purpose e.g. to confirm your identity to avoid fraudulent transactions in your name.)*

(2) The "I AGREE" button must immediately follow the notice provided for above. The notice and "I AGREE" button must be separate from any other notice or message contained on the web site.

(3) The consumer must have the ability to fully review any of the terms to which he or she is agreeing immediately preceding the consensual click.

(4) The consumer must not be able to proceed in the process without affirmatively agreeing to the terms in the notice.

(5) The consumer must have the ability (should they choose) to print out the terms to which he or she is agreeing, including their consent.

(6) The record of the consumer's 'written instruction' by clicking "I AGREE" must be retained by Client in a form that is capable of being accurately reproduced for later reference by the parties.

B. Written Instructions by Telephone. If Client is obtaining "written instructions" over the telephone, Client shall substantially comply with the following requirements which are designed to comply with the Electronic Records and Signatures in Commerce Act:

(1) Client will ask each consumer to confirm his or her consent to access such person's credit report for authentication purposes by asking the following: "In order to verify your identity, you need to authorize Client to access your credit report for authentication purposes. Please confirm your authorization to access your credit report for authentication purposes by pressing the # key now";

(2) The consumer must not be able to proceed in the process without affirmatively agreeing to allow access to his credit report as provided above; and

(3) The record of the consumer's 'written instruction' by pressing the # symbol must be retained by Client in a form that is capable of being accurately reproduced for later reference by the parties.

Membership Application

Experian Information Solutions Division

Important: All information must be completed in its entirety. Please print clearly and legibly to ensure accurate and timely processing.

Business Information

Legal Name (under which tax returns are filed): _____

DBA or Assumed Name: _____ Type of Business: _____

Time in Business: _____ yrs _____ mos. Annual Revenue: _____ Estimated # of Credit Reports Accessed Monthly: _____

Type of Ownership: ☐ Corporation ☐ LLC ☐ Sole Proprietorship ☐ Partnership ☐ Nonprofit ☐ Other _____

Business License (attach as necessary) Do you have an **Investigation License**? ☐ **Yes** ☐ **No** If Yes, please provide a copy

Business Website: _____ Business Email Address: _____

Number of Owners and percentage ownership (if publicly traded, provide exchange name and stock symbol): _____

Owners' Name, title, address and phone numbers: _____

Will you be using a third party or technology partner to access? If yes, please provide that party's name: _____

What services does that third party provide (if applicable): _____

Business Physical Address (**no P.O. box numbers):** _____

City: _____ State: ___ ZIP: _____ How Long? _____ yrs _____ mos.

Primary Phone: ( ) _____ Fax: ( ) _____ Is this a **residential** address? ☐ **Yes** ☐ **No**

Contact for Physical Inspection: _____ Title : _____

Phone Number : ( ) _____ Email Address: _____

Billing Address (if different): _____ City: _____ State: ___ ZIP: _____

Billing Contact: _____ Title: _____ Phone: ( ) _____

Previous Business Address: _____

City: _____ State: ___ ZIP: _____ How Long? _____ yrs _____ mos.

Have you previously applied or have been an Experian Member? ☐ **Yes** ☐ No **If Yes, when?** _____

Under what business name? _____ Previous Member number (if known): _____

Principal of the Company

(Must be completed by majority owner or general partner, as applicable)

(Must be completed unless the business is a publicly traded entity on a recognized stock exchange or the business is a state or federally regulated financial institution). Please provide exchange name and stock symbol or charter number and name of regulatory agency:_____

I understand I am providing written instructions to Experian under the Fair Credit Reporting Act authorizing Experian to obtain my credit report. I authorize Experian to obtain this information solely to process this application.

Principal signature: _____ Date: _____ Social Security Number: _____ Year of Birth: _____

Principal name: _____ Title or Position: _____ Phone: ( ) _____

Residential Address: _____ City: _____ State: ___ ZIP: _____

Parent or Affiliated Business Information

Parent Company Name (if applicable):_____

Contact Name: _____ Title: _____ Phone: ( ) _____

Address: _____ City: _____ State: ___ ZIP: _____

Permissible Purpose/Appropriate Use

(Application will not be processed unless this information is provided.)

Provide detailed description of your use of Experian products and consumer data. Also, describe the nature of your business interaction with consumers.

_____

Head Designate for Internet Access

Full Name & Title: _____ Email Address: _____

Phone Number ( ) _____

User ID - First Choice (minimum 6 characters) _____

User ID - Second Choice (minimum 6 characters) _____

Organization Static IP Address(es) _____

Head Designate Certificate. This form is to be used by Experian to identify the individual that will act on behalf of the Client in regards to end user access to Experian's systems. Client's Head Security Designate will submit all requests to create, change or lock Client employee end user access to accounts and permissions associated with Experian's systems and information via the Internet. The Head Security Designate must be an authorized representative of the Client's organization and must be available to interact with Experian on information and product access matters in accordance with the attached Access Security Requirement for FCRA and GLB 5A Data. Such requirements may be updated from time to time by Experian in accordance with the terms therein. This Head Designate Authorization Form must be signed by a duly authorized representative of the Client. The Client acknowledges and agrees that Client 1) has received the Access Security Requirement for FCRA and GLB 5A Data, 2) has read and understands the Clients' obligations described in the Access Security Requirement for FCRA and GLB 5A Data, 3) will communicate the contents of the Access Security Requirement for FCRA and GLB 5A Data and any subsequent updates thereto to all employee end users that shall have access to Experian's systems and information via the Internet, and 4) will abide to the provisions of the Access Security Requirement for FCRA and GLB 5A Data. Changes in Head Security Designate status (e.g., transfer or termination) are to be reported to Experian immediately. On an annual basis Experian will require the Head Security Designate to attest to the accuracy and currency of the status of the employee end users that access accounts and permissions to Experian's systems and information via the Internet. Attestation must be completed within 30 days of notification to Client, or the Head Security Designate will be prohibited from accessing Experian's systems and information until such attestation is complete.

If this application involves Company's use of consumer credit products then the following shall apply:

I have read and understand the **"FCRA Requirements"** notice and Experian's **"Access Security Requirements For FCRA and GLB 5A Data"** and will take all reasonable measures to enforce them within my facility. I certify that I will use the Experian product information for no other purpose other than what is stated in the Permissible Purpose/Appropriate Use section on this application and for the type of business listed on this application. I will not sell the report to any consumer directly or indirectly. I understand that if my system is used improperly by Company personnel, or if my access codes are made available to any unauthorized personnel due to carelessness on the part of any employee of my company, I may be held responsible for financial losses, fees, or monetary charges that may be incurred and that my access privilege may be terminated.

Important Tax Notice
If Company is exempt from sales tax in any of the states where the information is delivered to you or accessed by you, please send Experian a completed and signed sales tax exemption certificate for each of those states.

I certify that I have read the above statements and all information provided is accurate.

_____ _____

Legal Company Name DBA Name (If Applicable)

X_____ _____

Authorized Signature Date

_____ _____

Type or Print Name of Authorized Signer Title

If you have questions or need additional information, please call 1-800-831-5614.

Experian Data Quality
Standard Terms and Conditions

1. DEFINITIONS

"Affiliated Company" shall mean any company which directly or indirectly controls, is controlled by, or is under common control with, Experian Marketing Solutions, LLC.

"Agreed Units" shall mean an agreed number of consumable units (such as professional services days and/or transactional clicks).

"Agreement" shall mean the Experian Data Quality Standard Terms and Conditions and each Quotation.

"Confidential Information" shall mean any and all information relating to the trade secrets, operations, processes, plans, intentions, product information, prices, know-how, designs, customer lists, market opportunities, transactions, affairs and/or business of the parties and/or to their customers (including Customer Data), suppliers, Customers or Affiliated Companies in or on any medium or format.

"Contract Year" shall mean a 12-month period from the Effective Date or any anniversary of the Effective Date exclusive of any development periods.

"Customer" shall mean the customer purchasing Experian Data Quality Licensed Materials or Services as listed in a Quotation.

"Customer Data" shall mean any data owned by the Customer and provided to Experian Data Quality in connection with this Agreement.

"Data Set" shall mean any data set forming part of the Licensed Materials.

"Data Set Updates" shall mean any update to a Data Set supplied to the Customer under this Agreement included within the fee for the Licensed Materials.

"Documentation" shall mean any user guide, operational manual and any other materials relating to the use or operation of the Services and/or the Licensed Materials provided to the Customer by Experian Data Quality.

"Effective Date" shall mean the date specified as such in the Quotation.

"End Of Service Life Policy" shall mean the End Of Service Life Policy available at www.qas.com/legal.

"Experian Data Quality" shall mean Experian Marketing Solutions, LLC., a Delaware limited liability company with offices for its Data Quality division located at 53 State Street, 20th Floor, Boston MA 02109.

"**Force Majeure"** shall mean any events beyond the reasonable control of the party including, without limitation, acts of God, public enemies, or terrorists, labor disputes, equipment malfunctions, material or component shortages, supplier failures, embargoes, rationing, acts of local, state or national governments or public agencies, utility or communication failures or delays, fire, earthquakes, flood, epidemics, riots and strikes.

"Initial Term" shall mean the period specified as such in the Quotation.

"**Intellectual Property Rights"** shall mean copyright, database right, domain names, patents, registered and unregistered design rights, registered and unregistered trademarks, and all other industrial, commercial or intellectual property rights existing in any country and all the rights to apply for the same.

"Licensed Materials" shall mean the Licensed Programs and/or any other software, data or related documentation made available by Experian Data Quality to the Customer under this Agreement.

"Licensed Programs" shall mean any Experian Data Quality proprietary software made available by Experian Data Quality to the Customer under this Agreement.

"New Releases" shall mean any maintenance release relating to the Licensed Materials including, but not limited to, error fixes, minor upgrades and patches (but not including New Versions), included within the fee for the Licensed Materials.

"New Version" shall mean a new version of the Licensed Materials not included within the fee for the Licensed Materials.

"Outsource Agent" shall mean a third party service provider of the Customer.

"Permitted Purpose" shall mean, unless otherwise stated in the Quotation, the internal business purposes of the Customer.

"Quotation" shall mean the Experian Data Quality document entitled "Quotation" signed by the Customer, and/or any other document signed by the Customer which identifies itself as a "Quotation" for the purposes of this Agreement and/or any QAS statement of work relating to Services, recording certain agreed details relating to this Agreement, including any special terms referred to or contained in such document.

"Renewal Date" shall mean any date on which the Customer would be entitled to terminate this Agreement under Section 3.1.

"Renewal Fee" shall mean the fee specified as such on the Quotation.

"Services" shall mean the services specified in the Quotation.

"Third Party Software" shall mean any third party software forming part of the Licensed Materials.

"Worldwide Support Policy" shall mean the Experian Data Quality worldwide support policy available at www.qas.com/legal and detailed in Section 8.1.

2. PRIMARY OBLIGATIONS

2.1. Experian Data Quality shall:

2.1.1. provide the Licensed Materials and Services in accordance with this Agreement;

2.1.2. use all reasonable care and skill in the performance of the Services.

2.2. The Customer shall be responsible for installing the Licensed Materials (as applicable) and shall use reasonable efforts to ensure that any Customer Data provided to Experian Data Quality is complete, accurate and in the agreed upon format.

2.3. Each party shall use all reasonable efforts to perform its obligations under this Agreement in accordance with any written timetable agreed upon between the parties.

3. TERM

3.1. This Agreement shall commence on the Effective Date and, subject to the provisions of this Agreement, shall continue until terminated by either party serving on the other not less than sixty (60) days prior written notice of termination to expire on the last day of the Initial Term or any subsequent anniversary of that date.

3.2. If this Agreement relates to Agreed Units being made available to the Customer as set out in the Quotation, the entitlement of the Customer to use these Agreed Units shall (unless otherwise stated in the Quotation) expire on the last day of the Initial Term irrespective of whether all of the Agreed Units have been used by the Customer and without any obligation on the part of Experian Data Quality to provide any refund for unused Agreed Units. If this Agreement relates wholly to Agreed Units being made available to the Customer then notwithstanding Section 3.1 this Agreement shall end upon the first to occur of:

3.2.1. all of the Agreed Units having been used by the Customer; or

3.2.2. the last day of the Initial Term.

4. PAYMENTS AND INVOICING

4.1. The Customer shall pay the fees set out in and/or referred to in the Quotation. The fees do not include applicable federal, state, local, or foreign sales or use taxes, and Customer will pay or reimburse Experian Data Quality for such taxes.

4.2. All invoices are payable within thirty (30) days after the date of invoice. If Customer fails to pay any invoice in accordance with the foregoing terms, Customer shall also pay interest on the unpaid amount at the lesser of one and one-half percent (1.5%) per month or the maximum amount allowed by law.

4.3. Experian Data Quality shall notify the Customer in writing at least ninety (90) days before the Renewal Date of any increase to the Renewal Fee in accordance with Sections 4.4 and/or 4.5, and such increased Renewal Fee shall apply in place of that originally set out in the Quotation unless this Agreement has been terminated prior to the Renewal Date in accordance with Sections 3.1 or 12.

4.4. Subject to Section 4.3, if any third party licensor of a Data Set or Third Party Software provider imposes any increase in royalties, Experian Data Quality shall be entitled to increase the Renewal Fee by the amount of any and all such increase(s) in royalties.

4.5. Subject to Section 4.3, Experian Data Quality shall be entitled to increase the Renewal Fee by an amount which does not exceed the percentage increase in the Consumer Price Index (CPI-U, US City Average, All Items) published by the Bureau of Labor Statistics for the most recent twelve (12) month period ending on December 31st prior to the Renewal Date.

5. COMPLIANCE AND AUDIT

5.1. Both parties agree to comply with all federal, state and local laws, rules and regulations applicable to each party's provision or use of the Customer Data, Licensed Materials, Licensed Programs and Services.

5.2. Experian Data Quality will have the right, on reasonable notice and during normal working hours, to audit the Customer's and any of its agents' compliance with its obligations under this Agreement in relation to the use of any software, data, Services or other materials. Experian Data Quality shall:

5.2.1. observe the Customer's procedures relating to the protection of confidential information;

5.2.2. take all reasonable steps to minimize disruption to Customer's business during such audit;

5.2.3. be responsible for the costs of conducting such audit, except where Customer is found to be non-compliant with its obligations under this Agreement, in which case Experian Data Quality may charge Customer for its reasonable costs in conducting the audit.

6. CONFIDENTIALITY

6.1. Each party when a recipient of Confidential Information shall:

6.1.1. keep the Confidential Information strictly confidential and not disclose any part of such Confidential Information to any person except as permitted by or as required for the performance of the recipient's obligations under this Agreement;

6.1.2. take reasonable steps to prevent unauthorized access to the Confidential Information.

6.2. Each party may disclose Confidential Information to the following persons, and allow its use in accordance with this Agreement provided that any party to whom it discloses Confidential Information shall observe the restrictions in this Section 6:

6.2.1. employees and officers of the recipient who require it for the recipient to perform its obligations under this Agreement;

6.2.2. the recipient's auditors and professional advisors solely for the purposes of providing professional advice;

6.2.3. if Experian Data Quality is the recipient, to Experian Data Quality Affiliated Companies and to the agents and sub-contractors of Experian Data Quality and Experian Data Quality Affiliated Companies, involved in performing Experian Data Quality's obligations under this Agreement.

6.3. The restrictions in Section 6.1 do not apply to any information to the extent that it:

6.3.1. is or comes within the public domain other than through a breach of Section 6.1; or

6.3.2. is in the recipient's possession (with full right to disclose) before receipt from the other party; or

6.3.3. is lawfully received from a third party (with full right to disclose); or

6.3.4. is independently developed by the recipient without access to or use of the Confidential Information; or

6.3.5. is required to be disclosed by law or by a court of competent jurisdiction provided that the recipient agrees to give prior written notice of such disclosure to the disclosing party and to take any reasonable and lawful actions available to it to avoid and/or minimize the extent of such disclosure.

7. WARRANTY AND DISCLAIMERS

7.1. Each party warrants that it has the full power and authority to enter into this Agreement.

7.2. Experian Data Quality warrants that the Licensed Programs will conform to any description specified in the Documentation, subject to the Licensed Programs being used in accordance with this Agreement and the Documentation. If the Customer notifies Experian Data Quality that any Licensed Program has failed to comply with this warranty, Experian Data Quality will (as the Customer's sole remedy in respect to such failure) as soon as reasonable, replace the relevant Licensed Programs with software programs which do comply.

7.3. Because the Licensed Materials and Services contain information provided to Experian Data Quality by other sources, Experian Data Quality cannot be an insurer or guarantor of the accuracy, completeness, or reliability of the Licensed Materials, Licensed Programs and Services.

7.4. THE WARRANTIES IN THIS SECTION 7 ARE THE ONLY WARRANTIES EXPERIAN DATA QUALITY HAS GIVEN CUSTOMER WITH RESPECT TO THE LICENSED PROGRAMS. EXPERIAN DATA QUALITY MAKES NO REPRESENTATION OR WARRANTIES, EXPRESS OR IMPLIED, WITH RESPECT TO THE SERVICES, DATA SETS, LICENSED MATERIALS, LICENSED PROGRAMS, OR ANY OTHER MATERIALS (TANGIBLE OR INTANGIBLE) SUPPLIED BY EXPERIAN DATA QUALITY HEREUNDER, AND EXPERIAN DATA QUALITY HEREBY EXPRESSLY DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTIES WITH RESPECT THERETO, INCLUDING WITHOUT LIMITATION, ANY WARRANTIES AS TO THE ACCURACY, COMPLETENESS OR CURRENTNESS OF ANY DATA OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY, OR FITNESS FOR A PARTICULAR PURPOSE.

8. SOFTWARE SUPPORT

8.1. Experian Data Quality will provide technical support to the Licensed Materials in accordance with its published Worldwide Support Policy, provided that:

8.1.1. if the Customer has acquired any software from an Experian Data Quality business partner which includes Licensed Materials (as specified in the Quotation), that partner shall be responsible for providing primary support;

8.1.2. if any such software is proprietary Third Party Software, Experian Data Quality shall not be liable for any failure to provide support in accordance with the Worldwide Support Policy to the extent that this is caused by any failure of the relevant third party;

8.1.3. when the Licensed Materials have had a "Last Ship Date" set, as defined in the End Of Service Life Policy, Experian Data Quality technical support shall be provided according to the End of Service Life policy.

9. INTELLECTUAL PROPERTY RIGHTS AND LICENSE

9.1. All Intellectual Property Rights in the Customer Data will remain vested in the Customer (or its relevant licensors).

9.2. All Intellectual Property Rights in the Services and the Licensed Materials will remain vested in Experian Data Quality (or its relevant licensors).

9.3. The Customer grants Experian Data Quality a limited royalty free, non-exclusive, non-transferable license to use (and copy) the Customer Data solely for the purposes of performing its obligations under this Agreement.

9.4. Experian Data Quality grants to the Customer a limited, non-exclusive, non-transferable license to use the Licensed Materials for the Permitted Purpose in accordance with this Agreement. By using the Licensed Materials and/or the Services the Customer agrees to comply with the terms of this Agreement.

9.5. If any of the Licensed Materials are licensed on a user, copy, application or transaction basis, and the number of users, copies, applications or transactions stated in the Quotation is exceeded, the Customer shall promptly notify Experian Data Quality in writing. Customer shall be obligated to pay an increased license fee relative to the increased number of users, copies, applications or transactions from the date when such permitted use is exceeded.

9.6. If at any time the parties agree to modify the Services and/or Licensed Materials as ordered on a Quotation then Experian Data Quality shall issue a revised Quotation reflecting such modifications. Experian Data Quality will not be obligated to initiate any such modified Services and/or Licensed Materials until the Customer has agreed in writing to the revised Quotation. Such modifications may include but not be limited to;

9.6.1. varying the number of permitted users;

9.6.2. increasing the number of permitted transactions;

9.6.3. upgrading the Licensed Programs;

9.6.4. including additional Data Sets; and/or

9.6.5. changing the location, application, equipment or operating environment which applies to the Services and/or Licensed Materials in question.

If the number of permitted users, transactions or Data Sets increases, the Customer shall not be entitled to renew this Agreement with respect to only those additional permitted users, transactions or Data Sets without renewing the original users, transactions or Data Sets.

9.7. The Renewal Fee shall be contingent upon the renewal of all Licensed Materials purchased in the previous Contract Year.

9.8. The Customer agrees that it will:

9.8.1 use the Services and the Licensed Materials for the Permitted Purpose only and in accordance with the Documentation and ensure that all personnel who use the Licensed Materials are employees, temporary employees or individual contractors of the Customer;

9.8.2 only use the Licensed Materials in connection with those products or applications within those divisions or territories as specified in the Quotation;

9.8.3 only use any software comprised within the Licensed Materials on computer equipment complying with such minimum specifications as may be agreed by the parties in writing, or in the absence of agreement as may reasonably be specified by Experian Data Quality;

9.8.4 not sell, transfer, sub-license, distribute, commercially exploit or otherwise make available to, or allow use of for the benefit of, any third party any of the Services and/or Licensed Materials, except as permitted in Section 9.8.1;

9.8.5 not copy, adapt, alter, modify, reverse engineer, decompile or otherwise interfere with the Licensed Materials or combine the same with other materials without the prior written consent of Experian Data Quality except as permitted by law and provided that the Customer is permitted to retain a copy of the Licensed Materials for the purposes of load balancing, back up and disaster recovery only;

9.8.6 only use any software comprised within the Licensed Materials on equipment owned, operated or controlled by the Customer at premises owned or used by the Customer, or on such other site as may be agreed by the parties from time to time in writing;

9.8.7 not allow any third party to amend, modify or otherwise alter the Licensed Materials without Experian Data Quality's prior written consent.

10. THIRD PARTY CLAIMS

10.1. Subject to Section 10.3, Experian Data Quality shall indemnify, defend and hold harmless Customer and its officers, directors, and employees from and against any and all any third party claim, damage, loss, liability, cost or expense, including reasonable attorneys' fees ("Claims") to the extent arising as a result of any:

10.1.1. (i) direct infringement by Experian of any United States patent, copyright, trade secret, or other intellectual property right in connection with the Licensed Programs; or (ii) Experian Data Quality violation of any applicable federal, state or local law, regulation, rule or judicial or administrative order in Experian Data Quality's performance of the Services or provision of the Licensed Materials.

10.2. To the fullest extent permitted by law, Customer shall indemnify, defend and hold harmless Experian Data Quality and its officers, directors, and employees from and against any and all Claims to the extent arising as a result of any:

10.2.1. (i) infringement of any United States patent, copyright, trade secret, or other intellectual property right in connection with the Customer Data; or (ii) Customer violation of any applicable federal, state or local law, regulation, rule or judicial or administrative order in Customer's use of the Services or use of the Licensed Materials.

10.3. If any Claims are made, or in Experian Data Quality's reasonable opinion are likely to be made, by any third party

alleging that its Intellectual Property Rights are infringed by the Customer's use of the Licensed Materials as permitted by the terms of this Agreement, Experian Data Quality may at its sole option and expense:

10.3.1. procure for the Customer the right to continue using the relevant Licensed Programs (or any part of them) in accordance with the terms of this Agreement;

10.3.2. modify the relevant Licensed Programs to avoid the infringement or replace the relevant Licensed Programs with non-infringing materials, while providing the same, or substantially similar, functionality to the infringing materials;

10.3.3. terminate this Agreement and Experian Data Quality shall refund to the Customer on a pro rata basis the amount of any fee paid in advance which relates to use of the relevant Licensed Materials, Data Set and/or Third Party Software during any period following termination.

10.4. Procedure. A party seeking indemnification for a Claim pursuant to this Agreement ("Indemnified Party") shall provide written notice detailing the circumstances of the Claim to the party responsible for indemnifying against the Claim ("Indemnifying Party") promptly following the discovery of such Claim by the Indemnified Party. Failure to timely provide such notice shall not diminish the Indemnifying Party's indemnification obligation except to the extent the Indemnifying Party's ability to defend such Claim is materially prejudiced by such failure or delay. The Indemnified Party shall provide the Indemnifying Party with such information and cooperation as the Indemnifying Party may reasonably request.

10.5. This Section 10 sets out the entire liability of Experian Data Quality and the sole remedy of the Customer with respect to any claims relating to the indemnities given herein.

11. LIMITS ON LIABILITY

11.1. Neither party excludes nor limits its liability to the other for any of the following (and nothing in this Agreement shall be construed as excluding or limiting such liability):

11.1.1. for personal injury or death resulting from its negligence or that of its employees, agents and/or sub-contractors;

11.1.2. for breach of Section 6;

11.1.3. for any matter which it would be illegal for that party to exclude and/or limit its liability; or

11.1.4. for a party's fraudulent misrepresentation

11.1.5. Customer breach of Section 9.8.4;

11.1.6. Customer breach of Section 13.4.

11.2. EXCEPT AS PROVIDED IN SECTIONS 10.1, 10.2 AND 11.1, THE LIABILITY OF EACH PARTY TO THE OTHER FOR ANY OR ALL LOSSES OR INJURIES FROM ANY ACTS OR OMISSIONS UNDER THIS AGREEMENT, REGARDLESS OF THE NATURE OF THE LEGAL OR EQUITABLE RIGHT CLAIMED TO HAVE BEEN VIOLATED, SHALL NOT EXCEED THE AMOUNT PAID BY CUSTOMER TO EXPERIAN DATA QUALITY UNDER THIS AGREEMENT FOR THE PARTICULAR LICENSED MATERIALS OR SERVICES WHICH ARE THE SUBJECT OF THE ALLEGED BREACH DURING THE TWELVE MONTH PERIOD PRECEDING THE ALLEGED BREACH.

11.3. NOTWITHSTANDING ANY OTHER PROVISION OF THIS AGREEMENT, IN NO EVENT SHALL EITHER PARTY BE LIABLE TO THE OTHER PARTY FOR ANY INCIDENTAL, INDIRECT, CONSEQUENTIAL, PUNITIVE OR SPECIAL DAMAGES (INCLUDING BUT NOT LIMITED TO DAMAGES TO BUSINESS REPUTATION, LOST BUSINESS, LOST PROFITS, OR LOST ANTICIPATED SAVINGS), WHETHER FORESEEABLE OR NOT AND HOWEVER CAUSED, EVEN IF SUCH PARTY IS ADVISED OF THE POSSIBILITY THAT SUCH DAMAGES MIGHT ARISE.

12. TERMINATION

12.1. Either party may terminate this Agreement (or part of it with respect to a particular part of the Licensed Materials) upon written notice to the other party in the following circumstances:

12.1.1. if the other party commits a material breach of any of its obligations under this Agreement which is not cured within thirty (30) days after receipt of a notice from the non-breaching party;

12.1.2. if the other party becomes insolvent, files or has filed against it a petition in bankruptcy or;

12.1.3. (in the case of termination by Experian Data Quality only and subject to Section 12.2) if Experian Data Quality loses the right to distribute any Data Set as contemplated by this Agreement, or (subject to Experian Data Quality giving the Customer not less than twelve (12) months prior written notice) if Experian Data Quality decides to discontinue the provision of any Data Set.

12.2. If Experian Data Quality terminates the provision of any Data Set or Third Party Software under Section 12.1, or the Customer terminates the provision of any Data Set or Third Party Software under Section 13.4, Experian Data Quality shall refund to the Customer on a pro rata basis the amount of any fee paid in advance which relates to use of the relevant terminated Data Set or Third Party Software during any period following termination.

12.3. The Customer's right to use the Licensed Materials or Services shall cease upon termination of this Agreement.

13. DATA SET UPDATES AND THIRD PARTY TERMS

13.1. Experian Data Quality will provide the Customer with Data Set Updates of Data Sets and New Releases of the Licensed Programs (which do not include upgrades to Licensed Programs which Experian Data Quality identifies as New Versions) in accordance with Experian Data Quality's policy and the End of Service Life Policy. The Customer shall install all such Data Set Updates and New Releases as soon as reasonable in order to receive Experian Data Quality's technical support services as specified in Section 8.

13.2. New Versions will be made available by written agreement and may be subject to an additional charge.

13.3. New Versions, New Releases and Data Set Updates made available to the Customer shall (unless otherwise agreed) be subject to the provisions of this Agreement as if they were part of the original Licensed Materials.

13.4. The Customer shall comply with any relevant Data Set license or Third Party Software terms imposed on Experian Data Quality by a third party licensor in relation to a Data Set or Third Party Software as notified to the Customer by Experian Data Quality or as made available on Experian Data Quality's website at www.qas.com/legal (or such other url as Experian Data Quality informs the Customer of from time to time). If at any time during the term of this Agreement, any such data license or Third Party Software terms change, Experian Data Quality will notify the Customer, and the Customer shall be entitled to terminate the use of any Data Set or Third Party Software materially and adversely affected by the change upon written notice to Experian Data Quality, in which case Section 12.2 shall apply.

13.5. If the Quotation indicates that any Outsource Agent is to have access to or manage any of the Services or Licensed Materials on behalf of the Customer the following terms shall apply:

13.5.1. the Outsource Agent shall have access to the relevant Services or Licensed Materials on behalf of the Customer only and for no other purpose;

13.5.2. any employees, temporary employees or individual contractors of the Outsource Agent making use of the Services or Licensed Materials shall count as users of the Customer for licensing purposes; and

13.5.3. the Customer shall require that the Outsource Agent and its employees, temporary employees or individual contractors comply with all relevant provisions of this Agreement.

14. GENERAL

14.1. All notices, requests and other communications hereunder shall be in writing and shall be deemed delivered at the time of receipt if delivered by hand or communicated by electronic transmission, or, if mailed, three (3) days after mailing by first class mail with postage prepaid. Notices to Experian Data Quality and Customer shall be addressed to the addresses provided on the Quotation, or to such other address as either party shall designate in writing to the other from time to time. Experian Data Quality may provide notice under Section 4.3 by email.

14.2. This Agreement will be binding upon and will inure to the benefit of the parties hereto and their respective heirs, representatives, successors and permitted assignees. This Agreement may not be assigned, transferred, shared or divided in whole or in part by either party without the prior written consent of the other party, such consent not to be unreasonably withheld or delayed, except that Experian Data Quality may assign or transfer any or all of its obligations under this Agreement to any Experian Affiliated Company without Customer's consent.

14.3. Experian Data Quality shall be entitled to sub-contract any or all of its obligations under this Agreement to a sub-contractor but by doing so Experian Data Quality shall be responsible for the acts and omissions of the sub-contractor to the same extent as if it had carried out the obligations itself pursuant to this Agreement.

14.4. If any part of this Agreement is found to be invalid or unenforceable by any court or other competent body, such invalidity or unenforceability shall not affect the other provisions of this Agreement and such other provisions shall remain in full force and effect.

14.5. Neither party will be liable for any delay or failure in the performance of its obligations under this Agreement if such delay or failure is due to an event of Force Majeure.

14.6. If either party fails to exercise a right or remedy that it has or which arises in relation to this Agreement, such failure shall not prevent that party from exercising that right or remedy subsequently in respect to that or any other incident.

14.7. A waiver of any breach or provision of this Agreement shall only be effective if it is made in writing and signed on behalf of the party who is waiving the breach or provision. Any waiver of a breach of any term of this Agreement shall not be deemed a waiver of any subsequent breach and shall not affect the enforceability of any other term of this Agreement.

14.8. This Agreement is governed by and construed in accordance with the internal substantive laws of the State of Illinois. Any dispute under this Agreement shall be brought in the federal or state courts in Cook County, Illinois.

14.9. This Agreement may only be amended in writing signed by authorized representatives of both parties.

14.10. This Agreement sets out all the terms agreed between the parties relating to the subject matter of this Agreement and supersedes any previous agreement between the parties relating to the same subject matter. It is a condition of this Agreement that neither of the parties shall be bound by, or liable to the other party for, any representation, promise or inducement (other than fraudulent misrepresentations) made by it or by any agent or person on its behalf which is not expressly contained in this Agreement.

14.11. Subject to any contrary provision in any Data Set license terms referred to in Section 13.4, the parties hereby agree that nothing in this Agreement shall be construed as creating a right which is enforceable by any person who is not a party to this Agreement or a permitted assignee of such a party.

14.12. Nothing in this Agreement is intended to, or shall, operate to:

14.12.1. create a partnership or joint venture of any kind between the Customer and Experian Data Quality;

14.12.2. authorize either party to act as agent for the other party;

14.12.3. authorize either party to act in the name or on behalf of, or otherwise to bind, the other party in any way.

14.13. In this Agreement:

14.13.1. the singular includes the plural and vice versa;

14.13.2. the headings are for ease of reference only and shall not affect the construction or interpretation of this Agreement;

14.13.3. where any matter is to be agreed, such agreement must be recorded in writing;

The contents of the Quotation shall prevail over the contents of these terms and conditions to the extent of any conflict or inconsistency, except that the obligations on the part of the Customer in relation to any Data Set shall prevail over all other terms.

IN WITNESS WHEREOF, the Parties have executed this Agreement as of the dates set forth below.

EXPERIAN MARKETING SOLUTIONS, LLC

By _____

Name_____

Title _____

Date_____

_____

By _____

Name _____

Title _____

Date_____

DATA PROVIDER LICENSE

Canada Data

This Data Provider License for Canada Post Data ("License") contains the terms and conditions specified by Canada Post Corporation ("Canada Post") in connection with Customer's use of Canada Post Data as defined herein, and is incorporated into the Experian Data Quality Standard Terms and Conditions (the "Agreement") by reference.

Definitions
"Canada Post Data' means Postal Code Address Data and Point of Call Address Data, collectively.

"Postal Code^{OM} Address Data" means the data file of Canadian address ranges created and owned by Canada Post that is provided to Customer in Experian Data Quality's proprietary format. Postal Code Address Data is used within the QAS Pro and QAS Pro Web products.

"Point of Call Address Data" means the Canada Post database that consists of Postal Code Address Data, along with other data compiled by Canada Post that is created and owned by Canada Post and provided to Customer in Experian Data Quality's' proprietary format. Point of Call Address Data is used within the CorrectAddress and QAS Batch products.

"Statement of Accuracy" means a statement generated by Experian DATA QUALITY software that has been recognized by Canada Post as meeting Canada Post's address accuracy standards, that determines the percentage of correctly addressed items, when compared against Canada Post's Current Canada Post Data file, for mail to be deposited for delivery with Canada Post.

Any term not otherwise defined herein, shall have the meaning specified in the Agreement.

1. License
Experian Marketing Solutions, Inc. ("Experian Data Quality") holds a non-exclusive license from Canada Post which authorizes it to distribute the Canada Post Data in conjunction with Experian Data Quality software. In return for the fees paid by Customer for the Licensed Materials, Experian Data Quality grants Customer a personal, non-exclusive, non-transferable license to use the Canada Post Data incorporated within the Licensed Materials subject to the terms of the Agreement and this License.

2. Term
This License commences on the Effective Date specified on the Quotation and continues until the Agreement is terminated.

3. Fees
The fees paid by the Customer for the Licensed Materials include an amount due to Canada Post for use of the Canada Post Data. No further fees are due to Canada Post for the use of the Canada Post Data.

The license fee for the Canada Post Data incorporated within Experian Data Quality's fees are neither established, controlled nor approved by Canada Post.

4. Trademarks
Postal Code is an official mark of Canada Post Corporation.

This License does not grant or imply any grant of a license to use any trademark owned by Canada Post or Experian Data Quality.

Customer shall not remove any proprietary notices (including, but not limited to trade marks or official marks of Canada Post and Experian Data Quality) placed on the Canada Post Data or Licensed Materials or on reports generated through the use of the Canada Post Data or Licensed Materials or on any media on which the same are supplied.

5. Restrictions on use of Point of Call Address Data
The following restrictions apply to Point of Call Address Data only.

5.1 Customer may not use the Point of Call Address Data in a call centre, for on-line purchases, as a component of any interactive voice response application, or for any other interactive application where individual addresses are validated and corrected.

5.2 Customer may only use the Point of Call Address Data for the purposes of:

a. validating and correcting mailing addresses, and
b. addressing mail for delivery by Canada Post and producing corresponding Statements of Accuracy only for the purposes of providing the same to Canada Post in relation to such addressed mail when it is deposited with Canada Post for delivery.

5.3 For addressing mail covered by a valid Statement of Accuracy, the most current data is to be used in the production of the Statement of Accuracy. Use of data that is not current at the time a Statement of Accuracy is created is strictly prohibited.

6. Liability and Indemnification

Neither Experian Data Quality nor Canada Post shall be liable for any damage or loss that Customer may suffer or incur as a result of use of any of the Canada Post Data whether resulting from a defect or error in any of the Canada Post Data or otherwise. Without limiting the generality of the preceding sentence, Customer agrees that neither Experian Data Quality nor Canada Post shall be liable to Customer for any damage to data or programs, or any claims for any direct damages or for any special, incidental or consequential damages (including, but not limited to, loss of profit, revenues, and savings) even if Experian Data Quality or Canada Post knew or should have known of the possibility of such damages. Customer shall indemnify Experian Data Quality and Canada Post with respect to all such matters.

EXPERIAN DATA QUALITY

DATA PROVIDER AND THIRD PARTY SOFTWARE TERMS AND CONDITIONS –

DATA APPEND DATA LICENSE

Experian Data Quality holds a non-exclusive license from its Data Supplier which authorizes it to append data to Customer's Housefile on the following terms and conditions ("Data Append Data License"). This Data Append Data License is incorporated into the Agreement by reference.

Definitions:

"Advertisements" means advertisements or marketing campaigns.

"Agreement" means the Experian Data Quality Standard Terms and Conditions, each Quotation and Statement of Work.

"Data Supplier" means the third party supplier of the data to be appended.

"Housefile" means the Customer's file of contacts to be appended with the Licensed Data.

"Housefile Customers" means the contacts listed on the Housefile.

"Licensed Data" means the data specified on the Quotation and Statement of Work to be appended to Customer's Housefile.

Any term not otherwise defined herein, shall have the meaning specified in the Agreement.

1. License Grant.

1.1. Experian Data Quality hereby grants to Customer a non-transferable, non-exclusive perpetual license to append Licensed Data to the Housefile and to use such appended Licensed Data for lawful marketing purposes in accordance with the terms of this Data Append Data License and the Agreement, which terms shall survive any termination or expiration of this Data Append Data License and the Agreement.

1.2. Customer acknowledges that the Licensed Data is owned by a third-party Data Supplier and that Customer has no proprietary rights in the Licensed Data other than those granted under the Data Append Data License and the Agreement.

1.3. Customer acknowledges that the Data Supplier is an intended third party beneficiary of the provisions of this Data Append Data License and as such is entitled to directly enforce in its own name the rights and obligations undertaken by Customer and to seek all legal and equitable remedies as are afforded to Experian Data Quality.

2. Use of Data.

2.1. Customer's use of the Licensed Data will comply with all privacy, data protection, credit, and any other laws, statutes and governmental regulations applicable to such use of the Licensed Data.

2.2. Customer shall not use the Licensed Data in Advertisements that violate the proprietary or intellectual property rights of any third parties.

2.3. Advertisements shall not contain any content or material which is discriminatory, profane or obscene, or which is illegal in the United States.

2.4. Customer shall use the Licensed Data for marketing and management purposes only and shall not transfer possession, right or title of or to such data for any other purpose whatsoever.

3. Indemnification.

3.1. Customer agrees to indemnify and hold harmless Experian Data Quality and the Data Supplier from and against any and all losses arising out of or resulting from Customer's misuse or unauthorized use of the Licensed Data. If the Licensed Materials includes phone number append, such indemnification includes but is not limited to failure to fulfil any compliance requirement or obligation under any applicable federal or state law, rule, or regulation relating to telephone solicitations or Do Not Call requirements.

4. The following terms apply if the Licensed Data includes phone numbers to be appended.

4.1. Experian Data Quality may provide Customer with telephone numbers of consumers who have registered under one or more "Do Not Call" lists maintained by the Federal Trade Commission and/or a state agency (the "DNC Lists"). In using the materials supplied by Experian Data Quality, Customer represents and warrants that Customer will comply with any and all federal and state laws, rules, and regulations regarding telephone solicitations and Do Not Call requirements.

4.2. Experian Data Quality disclaims any warranty, express or implied, that any telephone numbers on DNC Lists have been identified or deleted from the information supplied to Customer by Experian Data Quality. Furthermore, Experian Data Quality disclaims all responsibility for ensuring that Customer complies with the laws establishing the DNC Lists.

5. The following terms apply if the Licensed Data includes email addresses to be appended.

5.1. A customized permission request message will be sent to Housefile Customers that will direct them to a website where they can respond. Once there, the Housefile Customers can opt-out of future email messages from the Customer and third-party vendor or update their contact information.

5.2. Customer shall not send email solicitations to those email address records identified as having opted-out.

6. The following terms apply if the Licensed Data includes business email addresses to be appended.

6.1. Customer acknowledges that the email addresses provided by business email appending will include addresses constructed using algorithmic rules based on corporate email address patterns. Any email addresses appended in conjunction with these services will be the property of Customer except that Data Supplier shall retain the right to use domain names and email patterns obtained in connection with the services solely for the purposes of providing email append services to other clients.

7. The following terms apply if the Licensed Data includes Social Media Matching Services.

7.1. Customer acknowledges that Data Supplier and/or its agent may maintain a copy of any email addresses provided by Customer solely for the purpose of indexing and providing social media matching to other clients.

North American Support Policy

Client Technical Support

Contents

1. Introduction

This North American Support Policy (this "Policy") should be read in conjunction with the Agreement entered into between Experian Data Quality ("EDQ") and Client (also referred to as "Customer"). The purpose of this Policy is to describe the availability and level of Client Technical Support provided by EDQ and the Client's responsibilities to enable EDQ to deliver such support.

2. Explanation of Terms

Any capitalized terms in this Policy are to be defined as set forth in the Agreement between EDQ and Client, except where explicitly defined below:

Term	Description
Custom Products and/or Integration Services	Custom products or services created by EDQ on Client's behalf, and not covered by this Policy.
Initial Response Time	The targeted time frame in which EDQ will endeavor to respond to Client's initial request for Client Technical Support, and, where a specific response time window has not been specified, the time interval within which EDQ will communicate regarding the request.
Policy	The North American Support Policy; this document.
EDQ Client Technical Support or Support	Technical Support offered in relation to the Licensed Materials as detailed in this Policy and more specifically at Section 3.
EDQ Concierge Support	Premium Technical Support and bundled services provided by EDQ at an additional charge to Client.
Concierge Support Fact Sheet	Document containing Concierge specific Terms and Conditions. Any Term or Condition not specifically defined in the EDQ Concierge Support Fact Sheet shall be covered under the North American Support Policy or existing governing Agreement with Client.

3. General Terms of Technical Support

3.1 Prerequisites for Client Access to EDQ Client Technical Support

During the term outlined in Client's ordering documents, access to EDQ Client Technical Support will be provided in accordance with the governing licensing terms and conditions, for the License term outlined within their Order Form, (or similar ordering document) and/or incorporated schedules or amendments entered into at the point of sale of the Licensed Materials (collectively, the "Agreement"), based on the following criteria:

- Client has a current and fully executed governing Agreement in place with EDQ
- Client has a current license for all applicable Licensed Programs, Data Sets and/or Services in use by the Client
- The Licensed Programs, Data Sets and/or Services are being used in accordance with the terms contained within the governing Agreement and Client is not in breach of the Agreement.

EDQ may elect not to provide access to EDQ Client Technical Support for Clients that do not meet the above criteria. All Clients provided access to EDQ Client Technical Support will receive support during the operating hours outlined in Section 5.4 of this Policy, unless otherwise specified in their current governing Agreement.

3.2 EDQ Obligations

EDQ Client Technical Support shall include support for Licensed Programs (including standard EDQ built integrations) and EDQ services (excluding Professional Services work performed under an SOW). Licensed Programs and/or standard integrations that have been altered or modified by anyone other than EDQ or its licensors may not be supported. Support includes general product and technical assistance for all current and supported EDQ software releases and/or standard integrations, running on the infrastructure and/or environment for which they are intended. Support shall not include:

i. Data imports and/or data conversion;
ii. Data entry, manipulation, and/or maintenance;
iii. Project management, training, customizations, or any services otherwise provided by EDQ's Professional Services group; or
iv. Any systems or programs not supplied by EDQ.

Support during upgrades is included, however, Client Technical Support does not perform upgrades or other services related to upgrades. Software used other than in accordance with the Documentation, as well as any discrepancies that do not significantly impair or affect the operation of the software are not covered. All services provided by EDQ's Professional Services group (including support for Custom Products and/or Integration Services) are subject

to availability at then-current rates unless otherwise specified in your current governing Agreement.

3.3 Supported Languages

All Support provided by EDQ is delivered in English, unless otherwise stated within Client's current governing Agreement.

4. Client Responsibilities

4.1 EDQ Expectations of their Clients

The ability of EDQ to respond quickly and effectively to cases is dependent on Client fulfilling the responsibilities and requirements set forth in this Policy.

Clients will use commercially reasonable efforts to:

- Ensure all individuals contacting support on behalf of the Client have appropriate knowledge and skills involving applicable Licensed Materials
- Provide information relevant to the case and any recent changes to the operating environment within a reasonable period of time after submitting a case, or upon request by EDQ
- Provide EDQ with reasonable and suitable access to the environment being supported, as described in Section 4.2 below
- Assume responsibility for fully protecting Customer Data against loss or corruption. EDQ will not be responsible for the loss of information or data while providing support
- Act upon recommended solutions provided by EDQ within a reasonable period of time
- Apply updates made available by EDQ, or its authorized partners, in a timely manner

Client's inability to or unwillingness to apply recommended solutions, updates or workarounds may result in Support Tickets (Cases) being closed.

4.2 Access to Client Data

In order to allow the proper diagnosis of support cases, EDQ may require access to Customer Data. Access may include, but is not limited to:

- Ability to view the user's desktop
- Copies of reports, screen prints, and/or other static data
- Access to test or backup systems
- Access to test or production databases

In all cases, EDQ will ensure that requests for access (whether to the production database, backup systems, Customer Data or otherwise), either directly or from a copy, are only made when no alternative is appropriate and feasible. If Client is unable to provide access to data

that has been requested, they should discuss alternative solutions with EDQ. EDQ reserves the right to automatically close cases when Client has not provided adequate, necessary data for a full analysis within a reasonable period of time.

5. Accessing Client Technical Support

5.1 Support Ticket (Case) Submission

5.1.1 Methods

Client may access EDQ Client Technical Support through any of the following methods:

Email*

General Support:	us.support.qas@experian.com
Concierge Support:	Provided in the Concierge Support Fact Sheet

Telephone

General Support:	888-712-3332
Concierge Support:	Provided in the Concierge Support Fact Sheet

**EDQ recommends that all non-critical support tickets be submitted via email*

5.1.2 Support Ticket (Case) Requirements

Cases may only be opened using one of the methods described above. When opening a case, Clients must provide the following information:

- Client ID
- Contact Name
- Contact Telephone Number
- Product and Version
- Description of Issue

In addition, the following information may also be requested in order to troubleshoot or resolve the case:

- Steps taken to reproduce the issue
- Screen prints
- Hardware & software environmental information

5.2 Support Ticket (Case) Severity Levels

Cases will be initially prioritized by EDQ based on the following guidelines. The case severity may change over time as more information becomes available or workarounds are provided. EDQ will make every reasonable effort to ensure submitted cases are assigned the proper level of severity.

Severity	Description
Priority 1 (P1)	Client's production system is significantly impaired with core EDQ functionality essentially unavailable. Client's day to day use of the EDQ software is severely impacted. There is no available workaround.
Priority 2 (P2)	Client's production system is able to run core processes but other EDQ functionality is significantly impaired. Client's ability to carry out day to day use of the EDQ software is severely impacted. There is no reasonably acceptable workaround.
Priority 3 (P3)	An area of core EDQ functionality is generating errors but this is not preventing Client from performing day to day use of the EDQ software. A workaround may be available.
Priority 4 (P4)	Any EDQ issue experienced in a non-production environment or in a production environment that is not impacting the function of the software to any material extent. A workaround may or may not be available. Examples include cosmetic defects on screens, errors in documentation, or an enhancement request.

5.3 Target Initial Response Times

Submitted cases will be responded to in the order in which they are received, with consideration given for higher severity levels. The Initial Response Time is the time it takes before EDQ makes initial contact with the individual who submitted the case. Initial Response Times are not a resolution goal and should not be interpreted as a guarantee of service. EDQ will use all commercially reasonable efforts to adhere to the time frames listed in this Section. EDQ does not provide case resolution targets and Initial Response Time should not be interpreted as a commitment regarding resolution timeframes.

Initial Response from EDQ includes, but is not limited to:

- An email response from EDQ and/or automated system requesting additional information, providing an update on the case, or indicating the support request has been received and is in process of being addressed
- Response provided via telephone or voicemail indicating the case has been received and is in the process of being addressed

	P1**	P2	P3	P4
General Support	1 hour	2 hours	4 hours	1 business day
Concierge Standard	1 hour	2 hours	4 hours	1 business day
Concierge Premier	45 min	1.5 hours	3 hours	1 business day
Concierge Elite	30 min	1 hour	2 hours	1 business day

***EDQ requires that all P1 cases be submitted via the applicable toll-free phone numbers listed in Section 5.1.1.*

5.4 Support Hours

5.4.1 General Support

EDQ Client Technical Support is available 24/7 via email submission, as well as via toll-free phone numbers listed in Section5.1.1.

5.4.2 Concierge Support

EDQ Concierge Support resources are available only between the hours of 8AM – 8PM Eastern Time, Monday through Friday (excluding EDQ North America recognized holidays) ("Concierge Hours"). EDQ General Support resources will provide coverage outside Concierge Hours to all Concierge Clients.

When a Client enrolled in Concierge Support submits a case after Concierge Hours, the case will be responded to and handled by the EDQ Client Technical Support team. The case will continue to be worked on by the EDQ Client Technical Support team until it is resolved or until an EDQ Concierge Support resource is available, whichever occurs first.

6. Support Life Cycle

Unless otherwise specified in Client's current governing Agreement, EDQ operates a release policy in which the current release and the immediately preceding previous release are supported. As EDQ continuously enhances and improves its product offerings, it may become necessary to declare a particular release or configuration (e.g., a particular operating system release) at the "end of life" stage for the purpose of support.

When this occurs, EDQ reserves the right to discontinue support for that product release or configuration. End of life notices are generally available at least 6 to 12 months in advance of the end of life date. For additional information, visit the End of Service Life Policy available at www.qas.com/support. EDQ may, at its sole discretion, continue to provide support for product releases or configurations beyond the end of life date. Should EDQ provide support for such releases or configurations, Clients who wish to obtain support for the end of life product release or configuration may be subject to additional fees.

7. Intellectual Property

For the avoidance of doubt, all modifications made to Licensed Materials in response to Technical Support cases will be considered part of the Licensed Materials and EDQ will own all Intellectual Property Rights in such modifications, even if originating from a suggestion or enhancement request made by Client.

"HERE Data End User Terms"

The data ("Data") is provided for your personal, internal use only and not for resale. It is protected by copyright, and is subject to the following terms and conditions which are agreed to by you, on the one hand, and HERE Global B.V. located at Kennedyplein 222-226, 5611 ZT Eindhoven, The Netherlands, and its affiliates ("HERE") and its licensors (including their licensors and suppliers) on the other hand.

Terms and Conditions

Personal Use Only. You agree to use this Data together with the application with which the Data was provided ("Application") for the solely personal, non-commercial (unless otherwise authorized in your agreement with the Application provider) purposes for which you were licensed, and not for service bureau, time-sharing or other similar purposes. Accordingly, but subject to the restrictions set forth in the following paragraphs, you agree not to otherwise reproduce, copy, modify, decompile, disassemble or reverse engineer any portion of this Data, and may not transfer or distribute it in any form, for any purpose, except to the extent permitted by mandatory laws.

Restrictions. Except where you have been specifically licensed to do so by the Application provider, and without limiting the preceding paragraph, you may not (a) use this Data with any products, systems, or applications installed or otherwise connected to or in communication with vehicles, capable of vehicle navigation, positioning, dispatch, real time route guidance, fleet management or similar applications; or (b) with or in communication with any positioning devices or any mobile or wireless-connected electronic or computer devices, including without limitation cellular phones, tablets, smart watches or other wearables, palmtop and handheld computers, pagers, and personal digital assistants or PDAs.

Warning. The Data may contain inaccurate or incomplete information due to the passage of time, changing circumstances, sources used and the nature of collecting comprehensive geographic data, any of which may lead to incorrect results.

No Warranty. This Data is provided to you "as is," and you agree to use it at your own risk. HERE and its licensors (and their licensors and suppliers) make no guarantees, representations or warranties of any kind, express or implied, arising by law or otherwise, including but not limited to, content, quality, accuracy, completeness, effectiveness, reliability, fitness for a particular purpose, usefulness, use or results to be obtained from this Data, or that the Data or server will be uninterrupted or error-free.

Disclaimer of Warranty: HERE AND ITS LICENSORS (INCLUDING THEIR LICENSORS AND SUPPLIERS) DISCLAIM ANY WARRANTIES, EXPRESS OR IMPLIED, OF QUALITY, PERFORMANCE, MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT. Some States, Territories and Countries do not allow certain warranty exclusions, so to that extent the above exclusion may not apply to you.

Disclaimer of Liability: HERE AND ITS LICENSORS (INCLUDING THEIR LICENSORS AND SUPPLIERS) SHALL NOT BE LIABLE TO YOU: IN RESPECT OF ANY CLAIM, DEMAND OR ACTION, IRRESPECTIVE OF THE NATURE OF THE CAUSE OF THE CLAIM, DEMAND OR ACTION ALLEGING ANY LOSS, INJURY OR DAMAGES, DIRECT OR INDIRECT, WHICH MAY RESULT FROM THE USE OR POSSESSION OF THE INFORMATION; OR FOR ANY LOSS OF PROFIT, REVENUE, CONTRACTS OR SAVINGS, OR ANY OTHER DIRECT, INDIRECT, INCIDENTAL, SPECIAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF YOUR USE OF OR INABILITY TO USE THIS INFORMATION, ANY DEFECT IN THE INFORMATION, OR THE BREACH OF

THESE TERMS OR CONDITIONS, WHETHER IN AN ACTION IN CONTRACT OR TORT OR BASED ON A WARRANTY, EVEN IF HERE OR ITS LICENSORS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Some States, Territories and Countries do not allow certain liability exclusions or damages limitations, so to that extent the above may not apply to you.

Export Control. You shall not export from anywhere any part of the Data or any direct product thereof except in compliance with, and with all licenses and approvals required under, applicable export laws, rules and regulations, including but not limited to the laws, rules and regulations administered by the Office of Foreign Assets Control of the U.S. Department of Commerce and the Bureau of Industry and Security of the U.S. Department of Commerce.

Entire Agreement. These terms and conditions constitute the entire agreement between HERE (and its licensors, including their licensors and suppliers) and you pertaining to the subject matter hereof, and supersedes in their entirety any and all written or oral agreements previously existing between us with respect to such subject matter. This agreement is without prejudice to your agreement with the Application provider.

Governing Law. The above terms and conditions shall be governed by the laws of the State of Illinois, U.S.A., except if you are located in Europe, Middle East, Africa or Russia in which case the laws of The Netherlands shall apply, in each case without giving effect to (i) the conflict of laws provisions, or (ii) the United Nations Convention for Contracts for the International Sale of Goods, which are explicitly excluded. You agree to submit to the jurisdiction of the State of Illinois, U.S.A., except if Dutch law applies the jurisdiction of The Netherlands shall apply, for any and all disputes, claims and actions arising from or in connection with the Data provided to you hereunder.

Additional Terms.

- In certain parts of the Territory or with respect to certain parts of the Data additional terms may apply. You expressly agree, and procures that any Sub-licensee agrees, to such supplier terms as made available at https://legal.here.com/terms/general-content-supplier/terms-and-notices/; and
- All copies of the Data and packaging relating thereto shall include the third party notices set out at https://legal.here.com/terms/general-content-supplier/terms-and-notices/ ;

Government End Users. If the Data is being acquired by or on behalf of the United States government or any other entity seeking or applying rights similar to those customarily claimed by the United States government, the Data is a "commercial item" as that term is defined at 48 C.F.R. ("FAR") 2.101, is licensed in accordance with these End-User Terms, and each copy of Data delivered or otherwise furnished shall be marked and embedded as appropriate with the following "Notice of Use," and shall be treated in accordance with such Notice:

NOTICE OF USE

Contractor (Manufacturer/ Supplier) Name: HERE

Contractor (Manufacturer/Supplier) Address: 425 W. Randolph Street, Chicago, Illinois 60606

This Data is a commercial item as defined in FAR 2.101 and is subject to these End-User Terms under which this Data was provided.

If the Contracting Officer, federal government agency, or any federal official refuses to use the legend provided herein, the Contracting Officer, federal government agency, or any federal official must notify HERE prior to seeking additional or alternative rights in the Data.

EXPERIAN DATA QUALITY DATA PROVIDER AND THIRD PARTY SOFTWARE TERMS AND CONDITIONS –

PHONE VALIDATION
DATA SET LICENSE

This Phone Validation Data Set License (the "License") is entered into pursuant to the Experian Standard Terms and Conditions ("the Agreement"). In the event of a conflict between the Agreement and this License, this License shall prevail. This License applies to the following products: QAS Phone: 10-digit Validation, Professional Services - Phone Validation & Type Indicator and ISV Force Phone Validate - Per Click.

Definitions:

"Licensed Service" means a service that validates the 10-digit number and identifies whether the telephone type is landline, mobile, or other. Available for USA and CAN telephone numbers.

"Query" means any unique access of the Licensed Services.

Any term not otherwise defined herein, shall have the meaning specified in the Agreement.

1. License Grant.

1.1. During the term of the Agreement and subject to the terms and conditions of this License, Experian Data Quality hereby grants to Customer a non-transferable, non-exclusive license to use the Licensed Service in support of Customer's business purposes.

2. Client Obligations/Use.

2.1. Customer agrees that it shall comply with all applicable privacy and data protection laws, rules and regulations related to its use of the Licensed Service, including information provided to and from the Licensed Service;

2.2. Customer agrees that to use the Licensed Service only to obtain information on a Query basis, and that all Queries to the Licensed Service will be primary; that is, except for use of existing customer information, there will be no queries with another third party product or service to obtain information that might be obtained from the Licensed Service without first making a Query to the Licensed Service;

2.3. Customer shall use the Licensed Service on a per Query basis and except for use in the transaction when initiated the Query, Customer shall not capture, store, record, cache, use for verification, or otherwise retain or use the information provided in response to a Query;

2.4. Customer agrees that it shall that it shall not: (i) disassemble, deconstruct, decompile or otherwise reverse engineer the Licensed Service; (ii) use information obtained from the Licensed Service to create a competing service; or (iii) sell, transfer, sub-license, distribute, commercially exploit or otherwise make available to, or allow use of for the benefit of, any third party any of the Services or information from the Licensed Service, except that Customer's independent contractors may use the Licensed Services in accordance with the Agreement and this License;

2.5. Customer agrees that information from the Licensed Service shall not be used by Customer for (i) using a phone number to look up an account in real-time or linking to other internal data in real-time; (ii) any real-time geographic call routing service (defined as connecting a caller to one location selected from multiple locations based on the geographic location of the caller; or (iii) speaking back or displaying information about locations selected from multiple locations based on the geographic location of the caller while the caller is on the line.

2.6. Customer is responsible for all fees relating to a telecommunication provider's connectivity services between Customer and the Licensed Service portal (i.e. fees for the purchase and/or lease, installation, testing, maintenance, repair and operation of all hardware/communication lines/equipment from the transaction/query origination point to the receiving point).

2.7. The Licensed Service uses redundant servers located at geographically diverse sites so that loss of a single server does not interrupt provision of the Licensed Service. In order for the Licensed Service to work properly, Customer's systems that connect to the Licensed Service must be configured using standard practices. For Web services, Customer's system must be configured to connect the production gateway for SOAP-based Queries. Experian Data Quality shall not be responsible for any unavailability of the Licensed Service caused by Customer's failure to properly configure its systems.

2.8. Client acknowledges that it may be able to access services other than the Licensed Service described herein. Some of those services require licenses and/or permission from other third party public or private entities. By accessing such services, Customer warrants that it has obtained the necessary licenses and/or permissions outside the license granted herein to legally access such services. Additionally, Customer will be responsible for any unauthorized access to services that are not the Licensed Services at the rate of $0.50 per Query and shall be subject to all terms and conditions governing the Licensed Services for such unauthorized access.

2.9. Client acknowledges that Experian and its third party provider reserve the right to utilize submitted Queries for the sole purpose of corroborating the association of data points with their repositories.

3. Warranties

3.1. Experian Data Quality warrants that the Licensed Service has been designed in a good workmanlike manner in accordance with industry standards.

3.2. Experian Data Quality does not warrant the uninterrupted or error-free operation of the Licensed Service.

3.3. Customer acknowledges that certain states have enacted laws placing restrictions on telemarketing activities, including but not limited to permitting a telephone subscriber to give public notice that he/she does not wish to receive sales solicitation telephone calls. Experian Data Quality disclaims any warranty, express or implied, that the names and/or telephone numbers of all such subscribers have been identified on or deleted from the information supplied by Customer to the Licensed Service.

3.4. EXCEPT AS OTHERWISE PROVIDED IN THIS LICENSE, EXPERIAN DATA QUALITY MAKES NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED, WITH RESPECT TO THE LICENSD SERVICE, INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTIBILITY, ACCURACY, COMPLETENESS OR CURRENTNESS OR FITNESS FOR A PARITCULAR PURPOSE. EXPERIAN DATA QUALITY DOES NOT WARRANT THAT THE LICSED SERVICE OR ANY INFORMATION DERIVED FROM THE LICENSED SERVICE WILL FULFILL ANY OF CUSTOMER'S PARTICULAR PURPOSES OR NEEDS.

3.5. Customer warrants that (i) all telephone numbers provided by Customer shall be lawfully obtained by Customer based on consumer initiated transactions; (ii) its use of information from the Licensed Services will be legal; and (iii) that it does not have a line of business in the outsourced call center industry.

4. Indemnification.

4.1. In addition to the other indemnification obligations in the Agreement, Customer agrees to indemnify and defend Experian Data Quality against any loss or damages from all third party claims or legal proceedings brought against Experian Data Quality arising from the misuse of data related to this License by Customer and Customer's breach of this License. Experian Data Quality shall cooperate with Customer in the handling of such claim, provided, however, that Customer must receive Experian Data Quality's prior written consent (which consent shall not be unreasonably withheld or delayed) to any settlement that (i) includes an admission of liability by Experian Data Quality; (ii) requires payment of any amounts not covered by Customer's indemnification obligations; (iii) includes actions that affect Experian Data Quality's rights in or to its intellectual property or that of its data supplier; (iv) does not include a complete release for Experian Data Quality.

5. Termination

5.1. Customer acknowledges that Experian Data Quality's termination rights as set forth in Section 12.1.3 of the Agreement and Customer's termination rights as set forth in section 13.4 of the Agreement shall apply to the Licensed Service.

QAS PROSPECT IQ SERVICES SCHEDULE

This QAS Prospect IQ Services Schedule ("Schedule") is entered into effective _____ ("Effective Date") between Experian Marketing Solutions, LLC ("Experian Data Quality") and _____ ("Customer") pursuant to the Experian Data Quality Standard Terms and Conditions ("Agreement"). Experian Data Quality and Customer may be referred to in this Schedule individually as a "Party" and collectively as the "Parties."

This Schedule provides the terms and conditions applicable to Experian Data Quality's provision to Customer of the QAS Prospect IQ Services, a hosted software service which delivers Experian Data Quality data and analytics in real time, to enhance the accuracy and quality of Customer's customer data as selected by Customer, and as specified in the Attachment hereto.

Experian Data Quality and Customer hereby agree as follows:

1. Definitions.

(a) "Affiliate" shall mean, in reference to a Party, any person or entity controlling, controlled by or under common control with such Party.

(b) "Applicable Law" means any and all applicable federal, state and local laws, regulations, rules, and judicial and administrative decisions, including without limitation any such laws, regulations, rules, and decisions relating to the age of the relevant customer or consumer whose data is included in the Customer Data.

(c) "Change Order" shall mean a written modification to this Schedule, as signed by representatives of both Parties.

(d) "Claim" shall mean any third party claim, damage, loss, liability, cost or expense, including reasonable attorney's fees.

(e) "Customer Data" shall mean any customer or consumer data that Customer or Customer's designee supplies to Experian Data Quality pursuant to this Schedule.

(f) "Enhanced Records" means the records returned by Experian Data Quality to Customer for each record processed by Experian Data Quality.

(g) "Experian Data Quality Data" shall mean any customer or consumer data (including those included in any scores or other results) that Experian Data Quality provides to Customer pursuant to this Schedule.

(h) "Initial Term" shall mean the period specified as such in the Quotation.

(i) "QAS Prospect IQ – Standardization and Data Append Services" means the standardization and enhancement of Customer Data with Experian Data Quality Data which may include appends for each customer record (raw data elements as well as ranges or segments).

(j) "Quotation" shall mean the Experian Data Quality document entitled "Quotation" or "Order Form" signed by the Customer, and/or any other document signed by the Customer which identifies itself as a "Quotation" or "Order Form" for the purposes of this Agreement and/or any statement of work relating to Services, recording certain agreed details relating to this Agreement, including any special terms referred to or contained in such document.

(k) "Security Breach" shall mean any actual, potential or threatened unauthorized access to or use of any Experian Data Quality Data.

(l) "Website" shall mean those Customer-hosted world wide web subscriber pages that Visitors use to access information and provide information to Customer used in the QAS Prospect IQ Services.

Any terms not defined herein shall have the meaning ascribed to them in the Agreement.

2. QAS Prospect IQ Services.

2.1. Services. Experian Data Quality shall perform the QAS Prospect IQ – Standardization and Data Append Services selected by Customer as indicated in Attachment A. Experian Data Quality will process Customer Data received via the Services below, then return the Enhanced Record directly to Customer. No further processing is required under this Schedule. Experian Data Quality grants to Customer access to its QAS Prospect IQ services listed in the Attachment via the applicable Integration Method specified therein and accessible by prior approved Customer IP addresses. In the event that Customer selects any additional Experian Data Quality products and/or services, then the additional terms and conditions set forth on the Attachments hereto shall apply with respect to such additional Experian Data Quality products and/or services. The Parties may supplement or change the selection of QAS Prospect IQ Services to be provided to Customer hereunder pursuant to a Change Order and subject to Experian Data Quality's approval. Experian Data Quality will not be obligated to initiate any changes to the QAS Prospect IQ Services provided to Customer hereunder until the Parties have executed the applicable Change Order. In the event of a conflict among or between the terms of this Schedule, the Agreement, the Service Order or a Change Order the following precedence shall apply: (i) Change Order; (ii) any Attachment(s); (ii) Schedule; then, (iii) the Agreement.

2.2. Services Fulfillment. Customer shall transmit record requests for the QAS Prospect IQ Services using the transmission format described in Attachment A. Customer is solely responsible for its transmission lines and all costs and expenses therefore. Experian Data Quality shall fulfill Customer's QAS Prospect IQ Service requests in accordance with the provisions of this Schedule. Experian Data Quality's service level goals and associated reporting procedures to support the service level goals for the QAS Prospect IQ Services are set forth in the Attachments hereto. Customer acknowledges and agrees that such service level goals are non-binding; provided, that Experian Data Quality shall use its commercially reasonable efforts to meet such service level goals.

2.3. Customer Support. Customer shall perform those services, tasks, responsibilities, reviews, and approvals ("Customer Tasks"), and provide that or those data, materials, information, cooperation, and access to Customer resources ("Customer Support") as Experian Data Quality may otherwise reasonably request in connection with the QAS Prospect IQ Services. Customer's failure to timely perform any Customer Tasks or provide any Customer Support may result in or require a change to the QAS Prospect IQ Services, timelines, or fees and require the Parties to modify this Schedule to document such impact. In any event, Experian Data Quality may equitably delay any QAS Prospect IQ Services to the extent impacted by a Customer failure to perform any Customer Tasks or provide any Customer Support.

2.4 Integration. Professional Services to integrate QAS Prospect IQ into Customer's environment are subject to a separate Statement of Work to be mutually agreed by the parties

3. Term. This Schedule shall commence as of the Effective Date and subject to the provisions of this Schedule, shall continue until terminated by either party serving on the other not less than sixty (60) days prior written notice of termination to expire on the last day of the Initial Term or any subsequent anniversary of that date.

4. License; Intellectual Property Ownership.

(a) Customer hereby grants to Experian Data Quality for the Term a personal, nonexclusive and non-transferable license to use the Customer Data pursuant to the QAS Prospect IQ Services, subject to the restrictions herein and subject to the provisions of Section 5.1(a) below. Customer shall not provide access to the QAS Prospect IQ Services to or permit use of the QAS Prospect IQ Services by or on behalf of any third party; provided, however, that notwithstanding the foregoing, Customer may provide access to the QAS Prospect IQ Services by a third party processor, provided that any such third party processor is approved in advance in writing by Experian Data Quality and such third party processor and Customer enter into a Third Party Processor Undertaking in the form required by Experian Data Quality. Experian Data Quality may suspend Customer's license to use the QAS Prospect IQ Services immediately upon written notice if Customer's use of the QAS Prospect IQ Services is

contrary to the use restrictions herein. Experian Data Quality hereby grants to Customer for the Term a personal, non-exclusive and non-transferable license to receive and use Enhanced Records solely for Customer's internal, direct call center marketing campaigns associated with the Customer Data and such other marketing uses as may be approved in advance and in writing by Experian Data Quality (the "Purpose"), subject to the restrictions set forth herein and subject to the provisions set forth above relating to a third party processor.

(b) Customer acknowledges and agrees that (i) Experian Data Quality has expended substantial time, effort, funds and intellectual capital to create and develop the QAS Prospect IQ Services, (ii) all right, title, and interest to QAS Prospect IQ Services shall at all times remain in Experian Data Quality, and (iii) all applicable rights to patents, copyrights, trademarks and trade secrets in QAS Prospect IQ Services, and to any update, modification, or enhancement to, or derivative work of, QAS Prospect IQ Services, including, without limitation, any update, modification, enhancement to, or derivative work of, QAS Prospect IQ Services, made as a result of or in connection with any suggestion, input or recommendation made by Customer, shall remain Experian Data Quality's proprietary property. Nothing contained in this Schedule shall be deemed to convey to Customer or to any other party any ownership interest in or to intellectual property, information or materials provided in connection with QAS Prospect IQ Services and Experian Data Quality shall in all cases be deemed to have retained any and all such rights.

5. Data and Use Restrictions.

5.1. Customer Data.

(a) Experian Data Quality shall use Customer Data solely to perform the QAS Prospect IQ Services pursuant to this Schedule and for no other purpose. Experian Data Quality shall not disclose Customer Data to any third party, except as directed by Customer, as necessary for Experian Data Quality to provide the QAS Prospect IQ Services, as required by Applicable Law or where such third party agrees to be bound by confidentiality obligations and other restrictions on the use of such Customer Data that are no less restrictive than the confidentiality obligations and restrictions on the use of Customer Data as are set forth herein. Experian Data Quality shall destroy or return Customer Data promptly following completion of the applicable QAS Prospect IQ Services; provided, however, that, notwithstanding the foregoing, Experian Data Quality shall be entitled to retain Customer Data following completion of the applicable QAS Prospect IQ Services for the following limited purposes: (i) to the extent necessary to validate and/or enforce its rights under this Agreement, including, without limitation, for billing, auditing and reporting purposes and (ii) to use Customer performance data resulting from Experian Data Quality performance of the QAS Prospect IQ Services as aggregated with other Experian Data Quality Customer performance data relating to the QAS Prospect IQ Services to develop statistical information regarding the QAS Prospect IQ Services, conduct Experian Data Quality internal analysis, and communicate the aggregated QAS Prospect IQ Services performance standards and results; provided, however, that in no event shall Customer be identifiable as a source of such performance data.

(b) Customer hereby certifies to Experian Data Quality that, prior to collecting any Customer Data from a customer and/or consumer, it will implement a posted privacy policy outlining its data sharing practices, which policy shall include, without limitation, any third party data sharing practices, disclosure relating to enhancement of the customer's and/or consumer's online data with offline data, and opt-out choices from such policy by the customer and/or consumer. Such privacy policy must be located on the applicable homepage as well as on each page where any customer's and/or consumer's data will be collected. Customer also hereby certifies to Experian Data Quality that it will obtain all necessary customer and/or consumer consent to provide and otherwise has all necessary rights to provide Experian Data Quality with Customer Data. Customer also hereby certifies to Experian Data Quality that it will comply with clear and conspicuous consumer notice and consent procedures for the provision of Customer Data to Experian Data Quality and will notify consumers that their Customer Data may be supplemented with additional data (including without limitation phone numbers) available to Customer from third party sources (e.g. Experian Data Quality), as necessary to comply with Applicable Law or as specified in writing by Experian Data Quality from time to time during the Term hereof, and that Experian Data Quality shall have the right to conduct reasonable audits of Customer to confirm compliance therewith.

(c) Customer shall use reasonable efforts to assure that the Customer Data does not: (i) incorporate or include any consumer data obtained from consumer(s) domiciled outside the United States; (ii) contain names of individuals under the age of eighteen (18) years; or (iii) contain any social security numbers, driver's license or state identification card numbers, account numbers, credit or debit card numbers, or any other information as may be specified in writing by Experian Data Quality from time to time during the Term hereof, and Customer shall be responsible for Customer's provision of any such Customer Data to Experian Data Quality and for Experian Data Quality use of such Customer Data in accordance with this Schedule. Customer shall at all times comply with all Applicable Law and take all reasonable security measures in connection with the transmission of Customer Data to Experian Data Quality.

(d) Any Customer failure to comply with the foregoing obligations set forth in this Section 6.1 shall be considered a material breach of this Schedule.

5.2. Experian Data Quality Data; Experian Data Quality Data Use.

(a) Customer shall use the Experian Data Quality Data solely for the Purpose and in strict accordance with: (i) the Data License Term and Data Usage Limitations outlined in the Attachment, (ii) all Applicable Law; and (iii) relevant industry guidelines (including, but not limited to, Direct Marketing Association Guidelines). Experian Data Quality shall have the right to conduct reasonable audits of Customer to confirm compliance with the foregoing. Customer acknowledges that Experian Data Quality does not match the Experian Data Quality Data provided to Customer against DNC Registries. Customer certifies that it has requested or received and will strictly use Experian Data Quality Data based upon either statutory exemptions or exclusions under all Applicable Law relating to DNC Registries, including but not limited to those exemptions based on business relationship. Any Customer failure to comply with the foregoing obligations shall be considered a material breach of this Schedule.

(b) Customer shall not (i) resell, license, or otherwise provide or disclose Experian Data Quality Data to any third party; (ii) copy or otherwise reproduce any Experian Data Quality Data; (iii) attempt to discover or reverse engineer any confidential and proprietary criteria developed or used by Experian Data Quality in the compilation of the Experian Data Quality Data or the performance of the QAS Prospect IQ Services; (iv) merge or incorporate the Experian Data Quality Data with any third party file without Experian Data Quality's prior written consent; (v) use Experian Data Quality Data to enhance any third party file or list, or develop, publish or maintain any list, enhancement, directory, or other similar product; (iv) use Experian Data Quality Data in any marketing communication that refers to selection criteria or presumed knowledge about the recipient; (vii) permit access to Experian Data Quality Data to individuals incarcerated in prisons or correctional institutions, or (viii) use the Experian Data Quality Data in any manner apart from the Enhanced Records.

(c) Customer acknowledges that Experian Data Quality Data has not been collected for credit purposes and is not intended to be indicative of any consumer's credit worthiness, credit standing, credit capacity, or other characteristics listed in Section 603(d) of the Fair Credit Reporting Act ("FCRA"), 15 USC Section 1681a. Customer shall not use any Experian Data Quality Data as a factor in establishing any consumer's eligibility for (i) credit or insurance used primarily for personal, family or household purposes, (ii) employment purposes, or (iii) other purposes authorized under Section 604 of the FCRA, 15 USC Section 1681b or any similar statute. In addition, Customer acknowledges that Experian Data Quality is neither guarantying nor warranting that the QAS Prospect IQ Services or any Experian Data Quality Data, including, without limitation, any Enhanced Record, will accurately predict any outcome or result. In addition, Customer acknowledges that the QAS Prospect IQ Services are provided to Customer for informational purposes only, and Experian Data Quality does not warrant or guaranty that Customer's use of such QAS Prospect IQ Services or Experian Data Quality Data will be in compliance with Applicable Law.

5.3. Change in Laws; Restrictions. Upon advance, written and reasonable notice to Customer, Experian Data Quality may withdraw or decline to provide to Customer any Experian Data Quality Data or QAS Prospect IQ Services to comply with any requirements imposed by any Applicable Law or in the event Customer's use of the QAS Prospect IQ

Services or Experian Data Quality Data is the subject to a substantial, adverse and documented consumer reaction related to consumer privacy issues and the Parties shall amend this Schedule to reflect such requirements. In addition, Experian Data Quality may impose reasonable restrictions or requirements upon the use of the Experian Data Quality Data or QAS Prospect IQ Services or make other changes to this Schedule at any time upon reasonable advance written notice to Customer to address matters concerning compliance with laws, privacy, confidentiality, and other issues to which consumers may be sensitive.

5.4. Security.

(a) Customer will maintain reasonable security procedures and practices to protect the Experian Data Quality Data in Customer's possession from unauthorized acquisition, access, destruction, use, modification, disclosure or any other event that would be deemed under Applicable Law a breach of the security, confidentiality or integrity of such Experian Data Quality Data (each a "Security Breach"). Experian Data Quality may from time to time specify, by written notice, certain security measures to protect Experian Data Quality Data, and to conduct reasonable audits of Customer to confirm compliance therewith. Any Customer failure to comply with the foregoing obligations shall be considered a material breach of this Schedule.

(b) Customer shall provide Experian Data Quality with immediate written notice upon discovery or notification of any Security Breach, or of any event or circumstance that could reasonably and foreseeably result in a Security Breach. Such notification shall contain a detailed description of the incident, the Experian Data Quality Data accessed, the identity of affected consumers, and such other information as Experian Data Quality may request concerning the Security Breach. Customer shall reasonably cooperate with Experian Data Quality to determine all steps to investigate, identify, prevent and mitigate the effects of any Security Breach (including steps for recovery), and shall immediately and at Customer's own expense take such steps (including as reasonably required by Experian Data Quality), and shall thereafter keep Experian Data Quality informed of the results and progress of such steps.

(c) At Experian Data Quality's election, Customer shall be solely responsible for providing all consumer, governmental and/or other notices ("Notices") required under Applicable Law relating to a Security Breach, notwithstanding whether such Applicable Law would require another party to provide such Notices. Experian Data Quality shall have the right to review and finally approve such Notices as related to Experian Data Quality Data. In no event, without Experian Data Quality's prior written approval, shall such Notices identify Experian Data Quality as the source of data or otherwise reference Experian Data Quality. Experian Data Quality reserves all rights to take any additional actions it deems appropriate to comply with Applicable Law or to protect its interests in the event of a Security Breach.

5.5. Retained Rights. Experian Data Quality shall own and retain exclusively all right, title and interest in and to the Experian Data Quality Data, any technologies, methods, processes, techniques or other intellectual property rights used or developed in the performance of the QAS Prospect IQ Services, and any enhancements, modifications, updates, improvements to, or derivative works of, the foregoing.

5.6 Exceptions to Limitation of Liability.

The limitation of liability set forth in Section 11 of the Agreement shall not apply to each Party's obligations under Section 6 below, Customer's breach of any of the provisions of Section 5.2, or Customer's transmission of Customer Data to Experian Data Quality.

6. Indemnification.

6.1. Experian Data Quality. Experian Data Quality shall indemnify, defend and hold harmless Customer and its officers, directors, employees and Affiliates from and against any and all Claims to the extent arising as a result of Experian Data Quality's violation of any Applicable Law in the performance of the QAS Prospect IQ Services, provided Customer has used the QAS Prospect IQ Services and Experian Data Quality Data in accordance with this Schedule.

6.2. Customer. Customer shall indemnify, defend and hold harmless Experian Data Quality and its officers, directors, employees and Affiliates from and against any and all Claims arising in connection with any: (i) Customer's violation of any Applicable Law in Customer's use or collection of any Customer Data supplied to Experian Data Quality; (ii) Customer's violation of a consumer's privacy rights or breach of any notice and consent procedures for the provision of Customer Data to Experian Data Quality in Customer's use or collection of any Customer Data supplied to Experian Data Quality or Customer's use of the QAS Prospect IQ Services or any Experian Data Quality Data; (iii) Security Breach; or (iv) Customer's violation of any Applicable Law in Customer's use of the QAS Prospect IQ Services or any Experian Data Quality Data.

6.3. Procedures. A party seeking indemnification for a Claim pursuant to this Schedule ("Indemnitee") shall provide the party obliged to provide indemnification pursuant to this Schedule ("Indemnitor") written notice detailing the circumstances of the claim promptly following the discovery of such Claim. Failure to timely provide such notice shall not diminish Indemnitor's indemnification obligation except to the extent Indemnitor's ability to defend such Claim is materially prejudiced by such failure or delay. Indemnitee shall provide Indemnitor such information and cooperation as Indemnitor may reasonably request.

7. General.

7.1. Incorporation by Reference; Precedence. This Schedule shall be deemed part of and incorporated into the Agreement.

7.2. Complete Agreement. This Schedule, with the Agreement, and as supplemented by the Quotation, Special Terms, sets forth the entire understanding of Experian Data Quality and Customer with respect to the subject matter hereof and supersedes all prior agreements, communications or representations, whether oral or written, made by any representative of either party relating thereto. This Schedule may be executed in one or more counterparts, each of which shall be deemed an original and shall constitute the same instrument.

7.3. Amendment. This Schedule may only be supplemented, modified or amended upon written agreement by authorized representatives of the Parties that specifically references this Schedule.

IN WITNESS WHEREOF, the Parties have executed this Schedule as of the dates set forth below.

Experian Marketing Solutions, LLC	_____ **("CUSTOMER")**
By _____	By _____
Name_____	Name _____
Title _____	Title _____
Date_____	Date_____

Attachment A: Order Details

QAS Prospect IQ – Integration Method	The integration method to be used by Customer to query the QAS Prospect IQ service shall be as set forth below where the applicable box below has been checked: ☐ ***SOAP-based Web Services API*** ☐ ***XML-based HTTPS Post*** All files sent by Customer to Experian Data Quality for processing must conform to security, format and processing requirements determined by Experian Data Quality.
Experian Data Quality Data:	In this Attachment A, "Experian Data Quality Data" refers to the following data attributes to be returned in an Enhanced Record:
Data License Term	The duration of Customer's permitted use of Experian Data Quality Data may not exceed (i) 365 days for individual or household- licensed data, and (ii) 24 hours for zip, zip+4 or other geo-licensed data, where the duration period of both (i) and (ii) are measured from the initial transmission or delivery of Experian Data Quality Data to Customer.
Data Usage Limitations	Customer may use the Experian Data Quality Data only in the following scenario:

The following additional terms and conditions shall apply in the event Customer provides Experian Data Quality Data of any kind to its end user Customers:

When the Customer wishes to use the Services in respect of each End User Customer, the Customer will inform Experian Data Quality and Experian Data Quality will provide a separate Customer ID ("Customer ID") in respect of that End User Customer to enable reporting in respect of that End User Customer.

The Customer may only cache or otherwise store the Experian Data Quality Data on behalf of an End User Customer where that End User Customer has been issued a Customer ID and only if such storage complies with the License Term above.

The Customer may not use the Experian Data Quality Data for End User Customers with more than one Customer ID. Each End User Customer must be issued and hold a unique Customer ID and via the Customer, request the Experian Data Quality Data in respect of a Lead.

Additional Customer Indemnity. In addition to the indemnification obligations listed in the Schedule, Customer shall indemnify Experian Data Quality and its officers, directors, and employees from and against any and all Claims to the extent arising as a result of any: (i) infringement of any United States patent, copyright, or trade secret, or any other third party rights in connection with Experian Data Quality use of any Customer end user data; (ii) Security Breach; (iii) end user Claim (except to the extent arising solely as a result of Experian Data Quality's gross negligence or willful misconduct); and (vi) violation of any applicable law in Customer's receipt or provision, or an end user's use of, Experian Data Quality Data or Services

Additional Customer Obligations: Customer agrees to and shall comply with the following:

(a) Customer shall not use the Services or Experian Data Quality Data or resell or distribute the Services or Experian Data Quality Data to any party other than an authorized end user in accordance with this SOW. Customer shall not license, sublicense nor distribute an Experian Data Quality Data file in its entirety, nor in its substantial entirety, to any third party.

(b) Customer shall enter into an end user agreement with each Customer end user that includes terms for end user use of the Experian Data Quality Data which, at a minimum, requires end user compliance with the Confidentiality provision set forth in the Agreement, end user compliance with all applicable laws and applicable industry self-regulatory guidelines, prohibits end user resale or redistribution of Experian Data Quality Data, and limits use of the Experian Data Quality Data to end user internal use only.

(d) Customer shall determine the applicability of any laws.

(e) Customer shall be solely responsible for the use of the Experian Data Quality Data and Services.

(f) Customer shall not grant access to the Services or Experian Data Quality Data to any business that employs individuals incarcerated in prisons or correctional institutions or to any such individuals.

(g) Customer agrees and acknowledges that Experian Data Quality may suspend or cancel Services in the event any such end user fails to comply with any applicable Laws.

(h) Customer may only disclose and append the Summarized Credit Statistics, in whole or in part, to any third party as inputs into their online content or decision-making engine or process, and shall not be used to make decisions on firm offers of credit or any decisions regarding credit worthiness.

Commented [A1]: Remove following language if no end user involved.

Business Data

For the purposes of this Attachment A, the term "Business Data Services" shall mean the supply of business credit and information services to be provided by the Experian Business Information Services Group ("BIS") to Experian Data Quality for use within the QAS Prospect IQ Services on behalf of Customer. Experian Data Quality will provide the Business Data Services to Customer for the fees as mutually agreed upon in the Experian Data Quality Quotation.

(a) Definitions

(1) Business Credit Services means those services provided by Experian Data Quality involving the supply of information about businesses from BIS's business credit reporting database. BIS will work with Experian Data Quality to provide the Business Data Services requested by Customer.

(2) BIS Data means any data which BIS provides to Experian Data Quality on behalf of Customer in performing Business Data Services except that data which Customer provides to Experian Data Quality ("Customer Data") for file enhancement or other processing services.

(b) Use Restrictions

(1) Customer certifies that it will request and use business credit information received from Experian Data Quality for Customer's own internal business use and not for resale, transfer or redistribution to third parties.

(2) Customer agrees that it will not copy or otherwise reproduce any BIS Data except as necessary for back up or security purposes. Under no circumstances will Customer attempt, directly or indirectly, to discover or reverse engineer any confidential and proprietary criteria developed or used by BIS or Experian Data Quality in performing the Business Data Services. Except as required by law, Customer agrees not to divulge, sell, or transfer the information provided via the Services to any third party without BIS' prior written consent. Without limiting the foregoing, Customer will not use any BIS Data supplied hereunder as the identifying source of business contacts for marketing purposes or for any list rental fulfillment or to select out names from its own or another database for resale. Following termination of this Schedule, Customer may retain the BIS Data for its own internal purposes and as required by law, subject to all confidentiality and use restriction provisions contained in this Schedule or the Agreement.

Commented [A2]: Remove if not business data is included.

Premier Summarized Credit Statistics

In the event Customer receives from Experian Data Quality data and/or services that contain financial information that has been statistically aggregated by combining records without personal information to a minimum of combined records at the ZIP Code +4 level, previously referred to as Summarized Credit Statistics, and now known and referred to herein as "Premier Summarized Credit Statistics", Customer hereby represents and warrants to Experian Data Quality that Customer shall use, protect, maintain and store any and all Premier Summarized Credit Statistics, or any lists derived from the Premier Summarized Credit Statistics in strict accordance with the following:

1. Customer shall use the Premier Summarized Credit Statistics solely for internal purposes in connection with Customer's customer or prospect lists and in no event shall Customer disclose the Premier Summarized Credit Statistics, in whole or in part, to, or use the Premier Summarized Credit Statistics for the benefit of, any third party.
2. Customer shall not duplicate or copy the Premier Summarized Credit Statistics except as necessary for record retention or legal purposes.
3. Customer shall not attempt to derive, decode, or otherwise reverse engineer any of the variables within, or processes utilized by Experian Data Quality in the development of, the Premier Summarized Credit Statistics.
4. Customer shall not use Premier Summarized Credit Statistics for any purpose at an individual consumer level, including portfolio review purposes, or to link Premier Summarized Credit Statistics data to or seek to determine the identity or any identifying attributes (such as name, address, Social Security number, or customer account number) of any individual .
5. Customer shall use the Premier Summarized Credit Statistics only in a positive or inclusive manner and will not use the Premier Summarized Credit Statistics to deny or exclude the offer of services or goods to a consumer or in any manner to discontinue, cancel, or deprive any individual or group of individuals of an already existing right or benefit.
6. Customer shall not use the Premier Summarized Credit Statistics to satisfy compliance with any Customer legal requirement or in a manner that violates any local, state or federal laws or regulations nor in a manner which is subject to the Equal Credit Opportunity Act (15 U.S.C. §1691 et seq.) or the Fair Credit Reporting Act (15 U.S.C. §1681 et seq.), including credit eligibility or collections.
7. If Customer has been authorized in the applicable Statement of Work to use the Premier Summarized Credit Statistics for modeling purposes, Customer shall use the Premier Summarized Credit Statistics only as input variables in a model (having a minimum of 2 variables) that results in scores that may then be used for internal analyses, profiling, list generation, or list segmentation;
8. Customer shall not use Premier Summarized Credit Statistics as the basis of any published analysis or study without Experian Data Quality's express written authorization, including in any services that will be shared with any third party.
9. Customer shall not use Premier Summarized Credit Statistics in connection with adult entertainment products or services, media/journalists, or for credit repair.

Commented [A3]: Remove if no PSCS data is included.

VANTAGE SCORE

The following terms apply to Customer's use of the VantageScore data:

Customer will request VantageScores only for Customer's exclusive use. Customer may store VantageScores solely for Customer's own use in furtherance of Customer's original purpose for obtaining the VantageScores. Customer shall not use the VantageScores for model development or model calibration, except in compliance with the following conditions: (1) the VantageScores may only be used as an independent variable in custom models; (2) only the raw archived VantageScore and VantageScore segment identifier will be used in modeling (i.e. no other VantageScore information including, but not limited to, adverse action reasons, documentation, or scorecards will be used); and (3) Customer's analytics and/or third party modeling analytics performed on behalf of Customer, using VantageScores, will be kept confidential and not disclosed to any third party other than as expressly provided for below in subsections (ii), (iii), and (iv) of this paragraph. Customer shall not reverse engineer the VantageScore. All VantageScores provided hereunder will be held in strict confidence and may never be sold, licensed, copied, reused, disclosed, reproduced, revealed or made accessible, in whole or in part, to any person, except (i) to those employees of Customer with a need to know and in the course of their employment; (ii) to those third party processing agents and other contractors of Customer who have executed an agreement that limits the use of the VantageScores by the third party only to the use permitted to Customer and contains the prohibitions set forth herein regarding model development, model calibration, reverse engineering and confidentiality; (iii) when accompanied by the corresponding reason codes, to the consumer who is the subject of the VantageScore; or (iv) as required by law.

Commented [A4]: Remove if no VantageScore data is included.

Pander Records

Experian hereby permits Client to receive the Pander Records from Experian and the Direct Marketing Association (DMA).

Pander Records are defined as follows: 1) Experian's Pander Records are individuals who have contacted Experian directly and requested to be removed from Experian's consumer marketing lists, 2) DMA Pander Records are individuals who have contacted the DMA requesting to be removed from acquisition lists for direct marketing purposes.

Client shall only use the Pander Records for the following uses:

Commented [A5]: Remove if no Pander records included

1. Appending - the use of the mail Pander Records included in this data license is for matching to inquirers for the sole purposes of increasing match rates.
2. List rental - the mail Pander Records are to be used solely for suppression, the name and/or address components of the Pander Record may not be used for any list rental marketing purposes.
3. Modeling/analysis - all Pander Records are prohibited from use for modeling and analytical purposes.

Deceased Records

Client shall only use the Deceased Records for the following uses:
Deceased Individual Suppression, matching and flagging, or receipt of the Deceased records from any Experian application for identification and deletion. The information contained in the Licensed Data regarding Deceased Individuals shall be used by Client solely for the purpose of suppressing the records of deceased individuals from marketing or prospect lists. Use of a Deceased Individual Suppression File is understood to mean matching to the Experian Licensed Data to identify those individuals which are deceased. The deceased information is to be used for the sole purpose of deleting the records of such deceased individuals from any list used for solicitation or any other external purpose. The Deceased File Data shall not be used for any other purpose including, but not limited to, promotions to surviving household members, or any other type of marketing or promotion.
For install files there is a legal requirement that you keep the deceased file data up-to-date. Therefore, when Experian provides an update to the Deceased data file you are required to implement the new file immediately.
You should not take any adverse action against any individual without further investigation to verify the death listed.

Commented [A6]: Remove if no Deceased records included

Experian Data Quality
SaaS Fair Usage Policy

As part of our commitment to providing a high-quality, fast and reliable service, Experian Data Quality has a Fair Use Policy (also referred to as the FUP) for its Software as a Service (SaaS) Products, specifically:

- Capture API - Address Validate (Previously known as Pro On Demand)
- Capture Application
- QAS For Salesforce.com
- QAS For Microsoft Dynamics CRM 2011
- QAS For Microsoft Dynamics CRM 2013
- QAS For Oracle CRM

The FUP contains guidelines for customers' use of the Experian Data Quality SaaS products to ensure that each customer has a consistently high-quality experience. Experian Data Quality takes measures to ensure usage is within reasonable parameters and in accordance with the license.

Why do we have a Fair Usage Policy?

Experian Data Quality SaaS products offer a multi-tenant service. This means that our products are used concurrently by a number of subscribers. If a single customer places very high demands on the service then it is possible that this will affect the experience for other users.

The vast majority of our customers use their service considerately and their usage levels during peak hours don't disproportionately affect the shared network and service capacity. Even though only a very small number of our customers may use the service inappropriately, their activity has the potential to affect the service for others. Our Fair Use Policy manages inappropriate use and makes sure the service can be used fairly by everyone.

The Fair Usage Policy

Usage of Experian Data Quality SaaS products is monitored on a continuous basis. Only customers that consistently generate exceptionally high load over a sustained period of time will be affected by the Experian Data Quality FUP. This is currently defined as per the limits detailed below, although Experian Data Quality reserves the right to amend these limits.

- The FUP covers the Internal use of Experian Data Quality SaaS products.
  - Internal usage of the Experian Data Quality SaaS products is charged annually on a per-seat basis.
  - Fair Usage of the product is defined in terms of the number of address searches per-seat per-day.
  - The FUP for internal usage is **500** address searches per-seat per-day. This equates to over 60 searches per-seat per-hour, based on an eight hour day.

- The FUP also covers the External use of Experian Data Quality SaaS products:
  - External usage is when the product is used on a customer-facing website.
  - An annual license is a fixed price annual fee (not charged on a per-click basis).
  - The FUP for an Annual License is **1,000,000** address searches per year. This equates to over 2700 address searches per day based on a daily average.

- The FUP does not apply to Experian Data Quality SaaS products when sold on a per-click basis.
- If a customer repeatedly exceeds this FUP Experian Data Quality reserves the right to restrict service or levy charges for excessive usage.

Extenuating Circumstances

Experian Data Quality understands that customers will occasionally have very high volumes of traffic outside of normal usage patterns. In those cases where this traffic can be predicted Experian Data Quality request to be informed with as much notice as possible to ensure that service delivery remains consistently high.

Changes to the Fair Usage Policy

This Fair Usage Policy may be updated from time to time, and the latest version of the document is available from the Experian Data Quality SaaS Self Service Portal: https://portal.experianmarketingservices.com

USPS® DATA PROVIDER TERMS AND CONDITIONS

This license for USPS® data ("License") contains the terms and conditions specified by the United States Postal Service® (USPS®) in connection with Customer's use of the USPS Data (as defined herein), and is incorporated into the Experian Data Quality Standard Terms and Conditions (the "Agreement") by reference. Addendum 1 applies if Customer receives DPV™ and/or LACSLink™ data.

Definitions
"USPS Data" refers to address data created by United States Postal Service and provided to Customer as a component of Experian Data Quality's software products and/or services. USPS Data includes the ZIP + 4® Data, DPV Data, and LACSLink Data (as defined herein). It also includes any accompanying written materials that have been produced by Experian Data Quality.

"ZIP + 4 Data" refers to the ZIP + 4 and City State files for the United States of America produced by the USPS and provided to Customer in Experian Data Quality's proprietary format. ZIP + 4 Data is used in the following Experian Data Quality software products: QAS Pro and QAS Pro Web.

Any term not otherwise defined herein, shall have the meaning specified in the Agreement.

1. License
Experian Data Quality holds a non-exclusive license from USPS which authorizes it to sub-license the USPS Data. In return for the fees paid by Customer for the Licensed Materials, Experian Data Quality grants Customer a personal, non-exclusive, non-transferable license to use the USPS Data subject to the terms of the Agreement and this License.

2. Term
This License commences on the Effective Date specified on the Quotation and continues until the Agreement is terminated.

3. Fees
The fees paid by the Customer for the Licensed Materials include an amount due to USPS for use of the USPS Data. No further fees are due to USPS for the use of the USPS Data.

The license fee for the USPS Data incorporated within Experian Data Quality's fees is not established, controlled or approved by USPS.

4. Ownership of the USPS Data
Customer owns the magnetic or other physical media on which the USPS Data is supplied (if any), but USPS retains title and ownership of the USPS Data recorded on the original media and all subsequent copies of the USPS Data, regardless of the form or media in or on which the original and other copies may exist. This License is not a sale of the original USPS Data or any copy.

5. Trademarks
The United States Postal Service is the owner of numerous trademarks, including but not limited to: United States Postal Service®, Postal Service™, Post Office™, United States Post Office®, "ZIP + 4®", "CASS™", CASS Certified™, DPV™, LACSLink™ and Suite^{Link}.

This License does not grant or imply any grant of a license to use any trademark owned by USPS or Experian **Data Quality**.

Customer shall not remove any proprietary notices (including, but not limited to Trade Marks or Service Marks of USPS and Experian **Data Quality**) placed on the USPS Data or Licensed Materials or on reports generated through the use of the USPS Data or Licensed Materials or on any media on which the same are supplied.

6. Restrictions on use

6.1 The USPS Data is copyrighted by USPS. If Customer or Customer's agents are installing the USPS Data at their site, Customer may make one (1) copy of the USPS Data solely for backup purposes. Customer must reproduce and include the copyright notice on the backup copy. Unauthorized copying of the USPS Data, including USPS Data that has been modified, merged or included with the Licensed Materials is expressly forbidden. Customer may be held legally responsible for any copyright infringement that is caused or encouraged by its failure to abide by the terms of this License.

6.2 Customer may not use the Licensed Materials to create a list of addresses if Customer did not previously have access to such addresses.

7. The USPS requires that USPS Data remain current and therefore provides regular updates. To ensure compliance and in accordance with USPS requirements, the Licensed Materials including USPS Data have been designed to cease functionality when the USPS Data has aged more than 105 days.

8. Warranty and Liability

THE USPS DATA IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND. FURTHER, USPS DOES NOT WARRANT, GUARANTEE, OR MAKE ANY REPRESENTATIONS REGARDING THE USE, OR THE RESULTS OF THE USE OF THE USPS DATA IN TERMS OF CORRECTNESS, ACCURACY, RELIABILITY, CURRENTNESS OR OTHER QUALTIES. EXPERIAN DATA QUALITY ASSUMES NO LIABILITY FOR THE USPS DATA.

Addendum 1
for the use of DPV™ and LACSLink™ Data

This Addendum 1 applies if the Quotation includes QAS Batch and CorrectAddress with USA Data. It also applies if the Quotation includes QAS Pro and QAS Pro Web with USA Data if DPV/LACS data is specified.

Definitions

"DPV Data" refers to a confidential and proprietary hash table created by the United States Postal Service® designed to help mailers validate the accuracy of address data by confirming valid delivery points, and that Experian Data Quality has integrated into its own proprietary software.

"LACSLink Data" refers to a confidential and proprietary system created by the United States Postal Service® for providing changes to a location's delivery address (for example implementation of a 911 emergency system which normally involves changing rural-style addresses to city-style addresses or in renaming or renumbering existing city-style addresses) and that Experian Data Quality has integrated into its own proprietary software.

Any term not otherwise defined herein, shall have the meaning specified in the Agreement.

1. Confidentiality

DPV and LACSLink Data are confidential and shall remain the property of USPS. Nothing contained in this USA Data Provider License shall give Customer any right, title, or interest in or to DPV or LACSLink Data except as a Customer under the terms of this License.

Customer agrees to hold all information concerning DPV and LACSLink Data in trust, to disclose said information only in accordance with the provisions of this License, to take all reasonable steps to safeguard the confidentiality of the DPV and LACSLink Data and any or all parts thereof and to prevent unauthorized disclosure thereof by Customer's employees, agents, representatives, and customers. Unauthorized disclosure includes using the product for artificially creating address lists; providing DPV and LACSLink Data or any portion thereof to any third party for any purpose or under any conditions except as expressly authorized by this License; or any other use of the data that is not specifically authorized by this License.

2. Restrictions on Use.

2.1. Customer shall not export the DPV Data or LACSLink Data outside the boundaries of the United States of America or its territories.

2.2. Customer shall not use the DPV or LACSLink Data to artificially compile a list of delivery points not already in Customer's possession or to create other derivative products based upon information received from or through use of the DPV or the LACSLink Data.

2.3. No proprietary Customer address list(s) or service products or other system of records that contain address attributes updated through use of DPV or LACSLink Data shall be rented, sold, distributed, or otherwise provided in whole or in part to any third party for any purpose containing address attributes derived from the use of DPV or LACSLink Data.

2.4. Use of LACSLink Data is limited to updating addresses and mailing lists to prepare items for delivery by USPS in conformance with USPS requirements.

2.5. Use of DPV Data and LACSLink Data is not permitted in conjunction with the Bulk Processing implementation of Pro Web.

3. Stop DPV Processing function

To detect conditions when address records appear to be the result of artificial manufacture and not legitimately obtained addresses, a seed table of artificially obtained addresses is provided by the USPS as a part of DPV. When the program detects an apparent artificial address, a "Stop DPV™ Processing" function is invoked and the product will cease providing further delivery point verification.

Should Customer encounter the Stop DPV Processing function, Customer shall notify Experian Data Quality immediately. As required, Experian Data Quality will then report the incident including Customer's name and address to the USPS. The USPS will typically allow functionality of the DPV to be restored for a first occurrence, but retains the right to suspend operation of this feature, without liability of any sort, when multiple incidents of artificial address detection occur.

4. Use of DPV in an online format

4.1. Where DPV Data is used in an online format, the information returned to the inquiring system shall be limited to confirmation of whether the input is a known address record.

4.2. Where DPV Data is used in an online interface environment, the Customer shall design the interface to prevent unauthorized access from anonymous sources. Customers providing online inquiry capability shall know their end users and shall not respond to inquiries from unknown users.

4.3. In the implementation of DPV Data in an online environment, the Customer shall take all steps necessary to prevent the potential misuse of the DPV Data from users attempting to automate the submission of addresses to the online inquiry system in a simulated manual-entry mode.

4.4. Customers shall have a management process to monitor the volume of inquiries made through their online system interface and validate that no obvious simulation of manual entry is occurring.

5. Warranty and Liability regarding DPV and LACSLink Data

OTHER THAN AS SPECIFICALLY SET FORTH IN THIS LICENSE, EXPERIAN DATA QUALITY MAKES NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED, AS TO MERCHANTABILITY, FITNESS FOR ANY PARTICULAR PURPOSE OR OTHERWISE WITH RESPECT TO DPV OR LACSLINK, NOR SHALL EXPERIAN DATA QUALITY BE LIABLE FOR ANY SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES EVEN IF IT HAS BEEN OR IS HEREAFTER ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. EXPERIAN DATA QUALITY SHALL NOT BE LIABLE FOR ANY DESIGN, PERFORMANCE OR OTHER FAULT OR INADEQUACY OF THE DPV OR LACSLINK DATA, OR FOR DAMAGES OF ANY KIND ARISING OUT OF OR IN ANY WAY RELATED TO OR CONNECTED WITH SUCH FAULT OR INADEQUACY. IN NO EVENT SHALL EXPERIAN DATA QUALITY'S LIABILITY TO CUSTOMER UNDER THIS LICENSE, IF ANY, EXCEED THE PRO RATA PORTION OF THE ANNUAL LICENSE FEE BASED ON THE EFFECTIVE DATE OF CANCELLATION WITHIN THIRTY (30) CALENDAR DAYS OF THE DATE OF CANCELLATION.

6. Indemnification regarding DPV and LACSLink Data

6.1. Experian Data Quality agrees to hold harmless, defend and indemnify Customer for infringement of any U.S. copyright, trademark, or service mark in the DPV Data and LACSLink Data provided by Experian Data Quality to Customer under this License. The foregoing obligation shall not apply unless Experian Data Quality shall have been informed within seven (7) calendar days by Customer of the suit or action alleging such infringement and shall have been given such opportunity as is afforded by applicable laws, rules, or regulations to participate in the defense thereof.

6.2. Customer agrees to hold harmless, defend, and indemnify Experian Data Quality for infringement of any U.S. patent, copyright, trademark, or service mark arising out of any modification to or development of applications, materials, and interfaces used by Customer with the DPV or LACSLink Data under this License. In addition, Customer further agrees to hold harmless, defend and indemnify Experian Data Quality and its officers, agents, representatives, and employees from all claims, losses, damage, actions, causes of action, expenses, and/or liability resulting from, brought for, or on account of any injury or damage received or sustained by any person, persons or property growing out of, occurring, or attributable to any work performed under or related to this License, resulting in whole or in part from any breach of this License or from the negligence or intentional misconduct, including any unauthorized disclosure or misuse of the DPV and LACSLink Data, including data derived from the DPV and LACSLink Data, by Customer, or any employee, agent, or representative of Customer.