MASTER SOFTWARE AS A SERVICE AGREEMENT

Between: RialtoInsights, Inc. "Provider"

And: _____"Customer"

1. Definitions

   "Order Form" means any mutually agreed ordering document issued by Rialto that referenced the MSA.

   "MSA" or Master Software as a Service Agreement means this document including the exhibits referenced in Section 3.

2. Effective Date

The MSA shall become effective when signed or accepted by Customer and received by Rialto ("Effective Date").

3. Referenced Documents

   3.1 The following documents shall apply in order of precedence as follows:

   - Order Form
   - MSA
   - Schedule 1 - Business Associate Agreement ("BAA")
   - Schedule 2 – Data Rights Agreement
   - Schedule 3 – General Terms and Conditions ("GTCs")

   3.2 The above Schedules are attached as of the Effective Date and are an integral part of the MSA. Rialto can update these Schedules where and as permitted in the respective Schedule.

4. Order

   4.1 This MSA establishes the contractual framework under which the parties may enter into an Order Form. An Order Form will detail the specific terms related to the transaction.
   4.2 Any contract previously executed by the parties remains unaffected unless the parties expressly agree to apply the MSA.

SCHEDULE 1 – BUSINESS ASSOCIATE AGREEMENT

This Business Associate Agreement ("BAA"), between RialtoInsights, Inc. ("Business Associate" or "Provider") and _____ ("Covered Entity" or "Customer"), which agreement is deemed to be an addendum to, and is governed by and subject to, the terms of the Master SaaS Agreement ("MSA").

RECITALS

Covered Entity and Business Associate are parties to the MSA pursuant to which Business Associate provides certain hosted subscription software or consulting services to Covered Entity and, in connection with the provision of such services, Covered Entity may need to disclose to Business Associate certain Protected Health Information ("PHI") that is subject to protection under the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 ("HIPAA"), the Health Information Technology for Economic and Clinical Health ("HITECH)" Act, Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 ("ARRA"), Pub. L. No. 111-5 (Feb. 17, 2009) and related regulations, the HIPAA Privacy Rule ("Privacy Rule"), 45 C.F.R. Parts 160 and 164, as amended, the HIPAA Security Rule ("Security Rule"), 45 CFR Parts 160, 162 and 164, and HITECH Omnibus Rules published on January 25, 2013 at 78 Fed. Reg. 5566.

The parties desire to comply with the HIPAA standards concerning the protection and privacy of PHI.

The purpose of this BAA is to comply with the requirements of the Privacy and Security Rules, including but not limited to the Business Associate Requirements at 45 CFR 164.504(e).

Therefore, in consideration of the mutual promises and covenants contained herein, the parties agree as follows:

SECTION I - DEFINITIONS

1.1 Definition. Unless otherwise provided in this BAA, capitalized terms shall have the same meaning as set forth in the Privacy Rule.

SECTION II - OBLIGATIONS OF BUSINESS ASSOCIATE

2.1 Use/Disclosure of PHI. In connection with its use and disclosure of PHI, Business Associate agrees that it shall use and/or disclose PHI as reasonably necessary to perform the services for, or on behalf of, the Covered Entity, provided such use or disclosure would not violate HIPAA if performed by the Covered Entity. Business Associate may use PHI to provide data aggregation services relating to the operations of the Covered Entity. As expressly authorized under the Data Rights Agreement, Business Associate may use PHI to create De-Identified Data in accordance with HIPAA and other applicable laws.

2.2 Safeguards for Protection of PHI. Business Associate agrees to use reasonable and appropriate safeguards (as determined by Business Associate), consistent with Subpart C of 45 CFR Part 164 with respect to electronic protected health information, to prevent use

or disclosure of PHI other than as provided for by the Data Rights Agreement.

2.3 Reporting.

2.3.1 Reporting of Impermissible Uses and Disclosures. Business Associate shall report to Covered Entity any use or disclosure of PHI which is not contemplated by this BAA of which Business Associate becomes aware.

2.3.2 Reporting of Breaches. Business Associate will report to you any Breach of your Unsecured PHI that Business Associate may discover to the extent required by 45 C.F.R. § 164.410. Business Associate will make such report without unreasonable delay, and in no case later than 5 business days after confirmation of such Breach.

2.4 Subcontracts. Business Associate shall ensure that any agent, including any subcontractor, to whom it provides PHI shall agree to restrictions and conditions at least as protective as those found in this BAA with respect to PHI.

2.5 Access and Amendment by Covered Entity. At Covered Entity's reasonable request, Business Associate shall allow Covered Entity to inspect, copy, and amend PHI in the possession of Business Associate if Covered Entity does not also maintain such information.

2.6 Access by Department of Health and Human Services. Business Associate shall make its internal practices, books, and records relating to the use and disclosure of PHI available to the Secretary of the Department of Health and Human Services for purposes of determining Covered Entity's compliance with the Privacy and Security Rules.

2.7 Accountings of Disclosures. If Business Associate discloses PHI to any third party, Business Associate will make available to Covered Entity the information required to provide an Accounting of Disclosures in accordance with 45 C.F.R. § 164.528 of which Business Associate is aware, if requested by Covered Entity. Customer acknowledges that Business Associate shall not be obligated to provide any information directly to any individual or person other than Customer and the Covered Entity, and that Business Associate does not therefore expect to maintain documentation of such disclosure as described in 45 C.F.R. § 164.528. In the event that Business Associate does make such disclosure, it shall document the disclosure as would be required for Client to respond to a request by an Individual for an accounting of disclosures in accordance with 45 CFR §§ 164.504(e)(2)(ii)(G) and 164.528, and shall provide such documentation to Customer promptly upon Customer's request. In the event that a request for an accounting is made directly to Business Associate, Business Associate shall, within 5 business days, forward such request to Customer.

SECTION III - PERMITTED USES AND DISCLOSURES

3.1 General. Except as otherwise limited in this BAA, Business Associate may use or disclose PHI to perform functions, activities, or services for, or on behalf of, Covered Entity as specified in the Data Rights Agreement, provided that such use or disclosure would not

violate the Privacy Rule if done by Covered Entity.

SECTION IV - OBLIGATIONS OF COVERED ENTITY

4.1 Notice of Privacy Practices. In its Notice of Privacy Practices, Covered Entity has included and will continue to include information advising Individuals that Covered Entity may disclose their PHI to Business Associates.

4.2 Consents/Authorizations. Covered Entity shall not provide PHI to Business Associate without having obtained the individual's consent, authorization, and other permission that may be required by the Privacy Rule or applicable state laws and/or regulations.

4.3 Restrictions. Covered Entity will not agree to any restriction requests or place any restrictions in any notice of privacy practices that would cause Business Associate to violate this BAA or any applicable law.

4.4 Security Protocols for PHI. Covered Entity shall be responsible for using appropriate safeguards to maintain and ensure the confidentiality, privacy and security of PHI transmitted, electronically or otherwise, to Business Associate pursuant to law. Covered Entity shall provide Business Associate with its policies and procedures to prevent, detect, contain, and correct security violations for handling PHI, including its protocols for transmitting and receiving ePHI.

4.5 Compliance with HIPAA. Covered Entity will not request or cause Business Associate to make a Use or Disclosure of PHI in a manner that does not comply with HIPAA or this BAA.

SECTION V - TERM AND TERMINATION

5.1 Term and Termination. This BAA shall be effective as of the Effective Date and shall remain in effect until terminated pursuant to Section 5.2 below.

5.2 Termination. Either party has the right to terminate this BAA for any reason upon 30 days prior written notice to the other party. A material breach of this Addendum will be treated as a material breach of the Agreement. The parties' rights and obligations upon termination of the MSA pursuant to this Section 5.2 are as set forth in the termination provisions of the GTCs incorporated via reference into the MSA.

5.3 Effect of Termination. Upon termination of this BAA, for any reason, Business Associate shall, if feasible, return or destroy all PHI that Business Associate still maintains in any form and shall not retain any copies of such PHI. If such return or destruction is not feasible, Business Associate shall extend the protections of this BAA to the PHI and shall limit further uses and disclosures to those purposes that make the return or destruction of the PHI infeasible.

SECTION VI - MISCELLANEOUS

6.1 Amendment. The parties shall modify this BAA to bring it into compliance with any

changes in HIPAA or the Privacy and Security Rules that are made after the Effective Date.

6.2 Interpretation. Any ambiguity in this BAA shall be resolved in a manner that brings the BAA into compliance with the most current version of HIPAA and the Privacy and Security Rules.

6.3 No Third-Party Beneficiaries. Nothing expressed or implied in this BAA is intended to confer, nor shall anything herein confer, upon any other person, other than the parties and their respective successors or assigns, any rights, remedies, obligations or liabilities whatsoever.

SCHEDULE 2 – DATA RIGHTS AGREEMENT

SECTION I - SCOPE

1.1 The purpose of this Agreement is to establish the parties' respective rights regarding the creation, use, disclosure, and ownership of De-identified Data derived from Protected Health Information ("PHI") process by Provider on behalf of Customer.

1.2 The Parties intend for this Agreement to authorize Provider to de-identify PHI in accordance with applicable law and to establish the Provider's rights with respect to the resulting de-identified data.

SECTION II - AUTHORIZATION TO DE-IDENTIFY

2.1 Customer expressly authorizes Provider, acting as Customer's Business Associate, to de-identify PHI solely on behalf of Customer in accordance with 45 CFR §164.514.

2.2 Provider shall utilize either:

3.2.1 The Safe Harbor method described in 45 CFR §164.514(b)(2); or

3.2.3 The Expert Determination method described in 45 CFR § 164.514(b)(1).

2.3 Provider shall maintain documentation supporting the de-identification methodology employed.

2.4 If Provider uses a code or other means of record identification in connection with de-identification, Provider shall maintain such code separately and shall not disclose it in a manner prohibited by law.

SECTION III - LICENSE TO USE DE-IDENTIFIED DATA

3.1 Customer grants Provider a perpetual, irrevocable, worldwide, royalty-free, fully paid-up, transferable, sublicensable, non-exclusive right and license to use, reproduce, host, modify, analyze, combine, enrich, disclose, distribute, create derivative works from, license, commercialize, and sell the De-Identified Data for any lawful purpose.

SECTION IV - COMMERICAL USES AND OWNERSHIP

4.1 Without limiting the foregoing, Provider may use, disclose, license, commercialize, and sell De-Identified Data for analytics and benchmarking, quality improvement and operational analysis, research and development, product development and model or system training where lawful, comparative effectiveness and outcomes analysis, market intelligence, reporting, dashboarding, and any other lawful commercial or non-commercial purpose.

4.2 All derivative works, models, analytics, methodologies, scoring systems, reports, benchmarks, dashboards, insights, and other materials developed by or for Provider from or using De-Identified Data shall be owned exclusively by Provider, subject only to Customer's retained rights in PHI prior to de-identification.

SECTION V - ARTIFICIAL INTELLIGENCE

5.1 Provider may utilize De-Identified data for training, validating, testing, improving and operating machine learning and artificial intelligence models.

5.2 Provider shall not use identifiable PHI for foundation model training except as expressly permitted by applicable law.

5.3 Provider shall implement and maintain reasonable and appropriate technical and organizational safeguards designed to prevent memorization, retention or unintended disclosure of PHI or other identifiable information within machine learning and artificial intelligence models.

5.4 Provider shall establish and maintain processes to validate that only De-identified Data is used in AI training and operations, including periodic testing, auditing and evaluation of models and datasets for potential leakage or reidentification risk.

5.5 Providers shall promptly remediate any identified risk of memorization or leakage and, where such risk could reasonably result in the exposure of PHI, notify Customer in accordance with the BAA.

SECTION VI - REGULATORY CHANGES

6.1 If applicable law materially changes the requirements governing de-identification or secondary use of health information, the parties shall cooperate in good faith to amend this agreement as necessary to maintain compliance.

SECTION VII - SURVIVAL

7.1 Sections relating to ownership, licenses, confidentiality, restrictions on reidentification, limitation of liability and dispute resolution shall survive termination of the MSA and BAA to the extent permitted by applicable law.

SECTION VIII - REPRESENTATIONS

8.1 Customer represents that, to the extent required by law, it has obtained any consents, permissions, authorizations, and notices necessary for Provider to perform the services and exercise the rights expressly granted herein.

8.2 In the event of any conflict between this Agreement and any other Agreement between the Parties, the BAA shall control with respect to PHI and HIPAA-required obligations, this Agreement shall control with respect to De-Identified Data, commercialization rights, licensing rights, and related economic rights, and the general commercial terms shall control for remaining matters.

SCHEDULE 3 - GENERAL TERMS AND CONDITIONS

SECTION I - DEFINITIONS

1.1 “Agreement” means the agreement as defined in the applicable Order Form.

1.2 “Authorized User” means any individual to whom Customer grants access authorization for use of the service that is an employee, agent, contractor, or representative of Customer.

1.3 “Cloud Service” means any distinct, hosted, supported, and operated on demand solution provided by Rialto under an Order Form.

1.4 “Confidential Information” means all information which the disclosing party protects against unrestricted disclosure to others, that the disclosing party or its representatives designates as confidential, internal and/or proprietary at the time of disclosure, should reasonably be understood to be confidential at the time of disclosure given the nature of the information and circumstances surrounding its disclosure.

1.5 “Customer Data” means any content, materials data and information that Authorized Users enter into the production system of a Cloud Service or that Customer derives from its use of and stores in the Cloud Service (e.g. Customer specific reports). Customer data and its derivatives do not include Provider’s Confidential Information.

1.6 “Documentation” means Provider’s then-current technical and functional documentation relating to the Cloud Services, or which Provider makes available to Customer as part of the Service, including technical and functional specifications as updated from time to time in accordance with the Agreement.

1.7 “Intellectual Property Rights” means patents of any type, design rights, utility models or other similar invention rights, copyrights and related rights, trade secret, know-how or confidentiality rights, trademarks, trade names and service marks, and any other

intangible property rights, whether registered or unregistered, including applications (or rights to apply) and registrations for any of the foregoing, in any country, arising under statutory or common law or by contract and whether or not perfected, no existing or hereafter filed, issued, or acquired.

1.8 "Order Form" means the ordering document for a Cloud Service and/or Professional Service that references the General Terms and Conditions.

1.9 "Professional Services" means implementation services, consulting services or other related services provided under an Order Form and may also be referred to in the Agreement as "Consulting Services".

SECTION II - SCOPE

2.1 Provider shall provide the services, software, analytics, hosting, support, implementation, consulting, data processing, and related deliverables described in the applicable Order Form.

2.2 Provider may use affiliates, subcontractors, cloud providers, and service providers in performing the services, provided Provider remains responsible for its contractual obligations.

SECTION III – FEES AND TAXES

3.1 Customer shall pay Provider the fees set forth in the applicable Order Form. Unless otherwise stated, invoices are due within thirty (30) days after the invoice date. Overdue undisputed amounts may accrue interest at the lesser of one and one-half percent (1.5%) per month or the maximum rate permitted by law.

3.2 If Customer does not pay fees in accordance with the terms of the Agreement, then in addition to any other available remedies, Provider may suspend Customer's use of the applicable Cloud Service and other services until payment is made. Provider shall provide Customer with prior written notice of suspension.

3.3 Fees are exclusive of taxes, duties, levies, and similar governmental charges. Customer shall be responsible for all sales, use, excise, value-added, withholding, and similar taxes arising from the transaction.

SECTION IV - CUSTOMER RESPONSIBILITIES

4.1 Customer shall timely provide Provider with access to personnel, systems, facilities, data, and information reasonably necessary for Provider to perform the services. Customer is responsible for the accuracy, completeness, legality, and sufficiency of data, instructions, and materials Customer provides to Provider.

4.2 Customer shall obtain and maintain all consents, notices, permissions, and authorizations required for Provider to perform the services and exercise the rights granted under the applicable Order Form. Customer shall not direct Provider to act in a manner Provider reasonably believes would violate applicable law, the BAA, or the Data Rights Agreement.

SECTION V – INTELLECTUAL PROPERTY

5.1 Provider retains all rights, title, and interest in and to its software, tools, templates, Documentation, processes, methods, models, analytics methods, prompts, workflows, know-how, and pre-existing materials, including all modifications, improvements, derivative works, and enhancements thereto whether or not developed for Customer.

5.2 Customer retains ownership of Customer Data provided to Provider, subject to the rights granted in the Order Form, the BAA, and the Data Rights Agreement. Unless expressly stated otherwise in an Order Form, Customer receives only a limited, non-exclusive, non-transferable right to use the deliverables for Customer's internal business purposes.

5.3 No rights in de-identified data are granted to Customer except as expressly set forth in the Data Rights Agreement.

SECTION VI – CONFIDENTIALITY

6.1 Each Party shall protect the other Party's Confidential Information using at least reasonable care and shall not use or disclose such Confidential Information except as necessary to perform under these GTCs or the applicable Order Form. Provider's Confidential Information includes but is not limited to Provider's pricing, product plans, source code, architecture, security materials, data methodologies, de-identification methodologies, and non-public documentation.

6.2 Confidential Information does not include information that is or becomes public through no fault of the receiving Party, was lawfully known by the receiving Party without restriction before receipt, is lawfully received from a third party without restriction, or is independently developed without use of the disclosing Party's Confidential Information.

SECTION VII - WARRANTIES

7.1 Compliance with Law

Each party warrants its current and continuing compliance with all laws and regulations applicable to it in connection with:

(a) in the case of Provider, the operation of Provider's business as it relates to Cloud Service and/or Professional Services; and

(b) in the case of Customer, Customer Data and Customer's use of Cloud Service.

7.2 Provider warrants that it will perform the services in a professional and workmanlike manner consistent with generally accepted industry standards.

7.3 Remedies

Customer's sole and exclusive remedies and Provider's entire liability for breach of the warranty will be:

(a) correction of the deficient Cloud Service; and

(b) if Provider fails to correct the deficient Cloud Service, Customer may terminate its subscription for the affected Cloud Service. Any termination must occur within 3 months of Provider's failure to correct the deficient Cloud Service.

SECTION VIII - INDEMNIFICATION

8.1 Provider shall indemnify Customer from third-party claims arising directly from Provider's gross negligence, willful misconduct, or material breach of these GTCs or an Order Form.

8.2 Customer shall indemnify Provider from third-party claims arising out of Customer's breach of these GTCs or an Order Form, Customer's failure to obtain required permissions or authorizations, Customer's use of deliverables, outputs, or data in violation of law, or Customer's combination of Provider deliverables with other products, data, or services not supplied by Provider where the claim would not have arisen but for that combination.

SECTION IX - LIMITATION OF LIABILITY

9.1 Neither party's liability is capped for damages resulting from willful misconduct or fraud.

9.2 Limited Liability - Except as set forth in Section 10.1, the maximum aggregate liability of either party to the other or to any other person or entity for all events (or series of connected events) arising in any 12 month period will not exceed the annual subscription fees paid for the applicable Cloud Service associated with the damages for that 12 month period.

9.3 Exclusion of Damages

In no case will:

(a) either party be liable to the other party for any special, incidental, consequential, or indirect damages, loss of goodwill or business profits, work stoppage or for exemplary or punitive damages; and

(b) Provider be liable for any damages caused by any Cloud Service provided for no fee.

Except for liability arising from gross negligence, willful misconduct, fraud, breach of confidentiality, payment obligations, or indemnification obligations, neither Party shall be liable for indirect, incidental, consequential, special, exemplary, or punitive damages.

SECTION X TERMINATION

10.1 These GTCs begin on the Effective Date and remain in effect until terminated by either Party upon thirty (30) days' written notice, provided any active Order Form remains until completed or terminated. Either Party may terminate an Order Form for material breach if the breach is not cured within thirty (30) days after written notice. Provider may suspend or terminate Cloud Services and/or Professional Services immediately if Customer requires Provider to act unlawfully, fails to pay undisputed fees, or materially breaches confidentiality or data-use restrictions.

10.2 These GTCs are governed by the laws of the State of Delaware, without regard to conflict-of-laws principles. Exclusive venue shall be the state or federal courts located in Kent County, Delaware. Amendments must be in writing and signed by both Parties. These GTCs may be executed in counterparts and by electronic signature.

SECTION XI AUTHORITY

11.1 The undersigned represents and warrants they are a duly authorized officer, member, partner, owner or other authorized representative of the Customer and have full authority to execute and deliver this Agreement on its behalf.

Accepted and Agreed,

CUSTOMER: _____	RIALTOINSIGHTS, INC.
BY:_____	BY: _____
Print Name _____	ROBERT MYERS, CEO
Title _____	336 North 26th Street Camp Hill, PA 17011
Address: _____ _____	
DATE:_____	DATE:_____