Q4 Data Protection Addendum Controller to Processor Transfers of Personal Data

This Data Protection Addendum ("Addendum") forms part of the Master Subscription Agreement ("Agreement") between: (i) Q4 Inc. ("Processor) acting on its own behalf and as agent for each Processor's Affiliate; and (ii) Customer ("Controller") acting on its own behalf and as agent for each Controller Affiliate and is effective as of the execution of an applicable Order Form ("Effective Date").

By signing the applicable Order Form, Customer enters into this DPA on behalf of itself and, to the extent required under applicable Data Protection Laws and Regulations, in the name and on behalf of its Authorized Affiliates, if and to the extent Q4 processes Personal Data for which such Authorized Affiliates qualify as the Controller. For the purposes of this DPA only, and except where indicated otherwise, the term "Customer" shall include Customer and Authorized Affiliates. All capitalized terms not defined herein shall have the meaning set forth in the Agreement. In the course of providing the Services to Customer pursuant to the Agreement, Q4 may Process Personal Data on behalf of Customer and the Parties agree to comply with the following provisions with respect to any Personal Data, each acting reasonably and in good faith.

The terms used in this Addendum shall have the meanings set forth in this Addendum. Capitalized terms not otherwise defined herein shall have the meaning given to them in the Agreement. Except as modified below, the terms of the Agreement shall remain in full force and effect.

In consideration of the mutual obligations set out herein, the parties hereby agree that the terms and conditions set out below shall be added as an Addendum to the Agreement. Except where the context requires otherwise, references in this Addendum to the Agreement are to the Agreement as amended by, and including, this Addendum.

1. Definitions

1.1 In this Addendum, the following terms shall have the meanings set out below and cognate terms shall be construed accordingly:

1.1.1 "**Applicable Laws**" means (a) European Union or Member State laws with respect to any Controller Personal Data in respect of which any Controller Group Member is subject to EU Data Protection Laws; and (b) any other applicable law with respect to any Controller Personal Data in respect of which any Controller Group Member is subject to any other Data Protection Laws;

1.1.2 "**Controller Affiliate**" means an entity that owns or controls, is owned or controlled by or is or under common control or ownership with Controller, where control is defined as the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of an entity, whether through ownership of voting securities, by contract or otherwise;

1.1.3 "**Controller Group Member**" means Controller and/or any Controller Affiliate;

1.1.4 "**Controller Personal Data**" means any Personal Data Processed by a Contracted Processor on behalf of a Controller Group Member pursuant to or in connection with the Agreement;

1.1.5 "**Contracted Processor**" means Processor, Affiliate Processor, Subprocessor, Subprocessor Affiliate, sub-subprocessor, sub-subprocessor affiliate, etc.;

1.1.6 "**Data Protection Laws**" means EU Data Protection Laws and, to the extent applicable, the data protection or privacy laws of any other country;

1.1.7 "**EEA**" means the European Economic Area;

1.1.8 "**EU Data Protection Laws**" means EU Directive 95/46/EC, as transposed into domestic legislation of each Member State and as amended, replaced or

superseded from time to time, including by the GDPR and laws implementing or supplementing the GDPR;

1.1.9 "**GDPR**" means EU General Data Protection Regulation 2016/679;

1.1.10 "**Processor**" means any person (including any third party and any Processor Affiliate, but excluding an employee of Processor or any of its sub-contractors) appointed by or on behalf of the Controller Process Personal Data on behalf of any Controller Group Member in connection with the Agreement;

1.1.11 "**Processor Affiliate**" means an entity that owns or controls, is owned or controlled by or is or under common control or ownership with Processor, where control is defined as the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of an entity, whether through ownership of voting securities, by contract or otherwise.

1.1.12 "**Processor Group Member**" means Processor and/or any Processor Affiliate;

1.1.13 "**Restricted Transfer**" means:

1.1.13.1 a transfer of Controller Personal Data from any Controller Group Member to a Contracted Processor; or

1.1.13.2 an onward transfer of Controller Personal Data from a Contracted Processor to another Contracted Processor, or between two establishments of a Contracted Processor,

in each case, where such transfer would be prohibited by Data Protection Laws (or by the terms of data transfer agreements put in place to address the data transfer restrictions of Data Protection Laws) in the absence of the Standard Contractual Clauses to be established under section 6.4.3 or 12 below;

For the avoidance of doubt: (a) without limiting the generality of the foregoing, the parties to this DPA intend that transfers of Personal Data from the UK to the EEA or from the EEA to the UK, following any exit by the UK from the European Union shall be a Restricted Transfers for such time and to such extent that such transfers would be prohibited by Data Protection Laws of the UK or EU Data Protection Laws (as the case may be) in the absence of the Standard Contractual Clauses to be established under section 6.4.3 or 12 or an adequacy ruling of the Commission at which time sub-section (b) shall apply to any UK transfer of Personal Data; and (b) where a transfer of Personal Data is of a type authorized by Data Protection Laws in the exporting country, for example in the case of transfers from within the EEA to a country (such as Switzerland and Canada which, as long as applicable, benefit from a ruling of adequacy pursuant to articles 45(9) and 45(3) of the GDPR) or scheme (such as the US Privacy Shield) which is approved by the Commission as ensuring an adequate level of protection or any transfer which falls within a permitted derogation, such transfer shall not be a Restricted Transfer

1.1.14 "**Services**" means the services and other activities to be supplied to or carried out by or on behalf of Processor for Controller Group Members pursuant to the Agreement;

1.1.15 "**Standard Contractual Clauses**" means the contractual clauses set out in Annex 3, as amended or replaced from time to time by the Commission or such other competent authority as applicable and pursuant to section 13.4;

1.1.16 "**Subprocessor**" means any person (including any third party and any Subprocessor Affiliate, but excluding an employee of Subprocessor or any of its sub-contractors) appointed by or on behalf of the Processor or any Processor Affiliate to Process Personal Data on behalf of any Controller Group Member in connection with the Agreement;

1.1.17 "**Subprocessor Affiliate**" means an entity that owns or controls, is owned or controlled by or is or under common control or ownership with Subprocessor, where control is defined as the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of an entity, whether through ownership of voting securities, by contract or otherwise; and

1.1.18 "**Subprocessor Group Member**" means Subprocessor and/or any Subprocessor Affiliate.

1.2 The terms, "**Commission**", "**Data Subject**", "**Member State**", "**Personal Data**", "**Personal Data Breach**", "**Processing**" and "**Supervisory Authority**" shall have the same meaning as in the GDPR, and their cognate terms shall be construed accordingly.

1.3 The terms, "**Controller**" and "**Processor**" shall, in addition to the definition set out in this Addendum, be supplemented by the meanings as set out in the GDPR.

1.4 The word "**include**" shall be construed to mean include without limitation, and cognate terms shall be construed accordingly.

2. Authority

Processor warrants and represents that, before any Processor Affiliate Processes any Controller Personal Data on behalf of any Controller Group Member, Processor's entry into this Addendum as agent for and on behalf of that Processor Affiliate will have been duly and effectively authorized (or subsequently ratified) by that Processor Affiliate.

3. Processing of Controller Personal Data

3.1 Processor and each Processor Affiliate shall:

3.1.1 comply with all applicable Data Protection Laws in the Processing of Controller Personal Data; and

3.1.2 not Process Controller Personal Data other than on the relevant Controller Group Member's written instructions unless Processing is required by Applicable Laws to which the relevant Contracted Processor is subject, in which case Processor or the relevant Processor Affiliate shall to the extent permitted by Applicable Laws

inform the relevant Controller Group Member of that legal requirement before the relevant Processing of that Controller Personal Data.

3.2 Each Controller Group Member:

3.2.1 instructs Processor and each Processor Affiliate (and authorizes Processor and each Processor Affiliate to instruct each Subprocessor and each Subprocessor Affiliate) to:

3.2.1.1 Process Controller Personal Data; and

3.2.1.2 in particular, transfer Controller Personal Data to any country or territory,

as reasonably necessary for the provision of the Services and consistent with the Agreement, Applicable Laws, and this Addendum;

3.2.2 warrants and represents that it is and will at all relevant times remain duly and effectively authorized to give the instruction set out in section 3.2.1 on behalf of each relevant Controller Affiliate;

3.2.3 warrants and represents that all of its instructions to any Contracted Processor will, at all times, comply with Data Protection Laws.

3.3 Annex 1 to this Addendum sets out certain information regarding the Contracted Processors' Processing of the Controller Personal Data as required by article 28(3) of the GDPR (and, possibly, equivalent requirements of other Data Protection Laws). Controller may, upon 60 days prior written notice, make reasonable amendments to Annex 1 by written notice to Processor from time to time as Controller reasonably considers necessary to meet those requirements.

4. Processor and Processor Affiliate Personnel

Processor and each Processor Affiliate shall, in accordance with Applicable Laws, take reasonable steps to ensure the reliability of any employee, agent or contractor of any Contracted Processor who may have access to the Controller Personal Data through any Processor Group Member, ensuring in each case that access is strictly limited to those individuals who need to know / access the relevant Controller Personal Data, as strictly necessary for the purposes of the Agreement, and to comply with Applicable Laws in the context of that individual's duties to the Contracted Processor, ensuring that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

5. Security

5.1 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Processor and each Processor Affiliate shall in relation to the Controller Personal Data implement appropriate technical and organizational

measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1) of the GDPR.

5.2 In assessing the appropriate level of security, Processor and each Processor Affiliate shall take into account the particular risks that are presented by Processing, in particular, from a Personal Data Breach.

5.3 The Controller has assessed any security measures specifically agreed in the Agreement and in this Addendum and the Controller confirms that it is satisfied with the security measures in place.

6. Subprocessing

6.1 Each Controller Group Member authorizes Processor and each Processor Affiliate to appoint (and permit each Subprocessor appointed in accordance with this section 6 to appoint) Subprocessors (and sub-subprocessors with regards to Subprocessors) in accordance with this section 6 and, if applicable, any restrictions in the Agreement.

6.2 Each Contracted Processor may continue to use those Contracted Processors already engaged and that are planned to be engaged by the engaging Contracted Processor as at the date of this Addendum, subject to Processor and each Processor Affiliate in each case meeting the obligations set out in section 6.4.

6.3 Processor shall give Controller prior written notice of the appointment of any new Subprocessor, including full details of the Processing to be undertaken by the Subprocessor. If, within 30 days of receipt of that notice, Controller objects to the proposed appointment, neither Processor nor any Processor Affiliate shall appoint (or disclose any Controller Personal Data to) that proposed Subprocessor until reasonable steps have been taken to address the objections raised by any Controller Group Member and Controller has been provided with a reasonable written explanation of the steps taken. Processor will use reasonable efforts to make available to Controller a change in the Services or recommend a commercially reasonable change to Customer's configuration or use of the Services to avoid Processing of Personal Data by the objected-to new Subprocessor without unreasonably burdening Customer. If, within 60 days of receipt of the notice, the Processor is unable to make available such change, the Controller may by written notice to Processor terminate the Agreement to the extent that it relates to the Services which require the use of the proposed Subprocessor. Processor will refund Customer any prepaid fees covering the remainder of the term of such terminated Agreement following the effective date of termination with respect to such terminated Services, without imposing a penalty for such termination on Controller. For the avoidance of doubt, Processor undertakes to fulfil the obligations as required by article 28(2) of the GDPR.

6.4 With respect to each relevant Contracted Processor, Processor or the relevant Processor Affiliate shall (and shall procure that each Contracted Processor shall):

6.4.1 before the relevant Contracted Processor first processes Controller Personal Data (or, where relevant, in accordance with section 6.2), carry out adequate due diligence to ensure that the relevant Contracted Processor is capable of providing the level of protection for Controller Personal Data required by the Agreement;

6.4.2 in accordance with Data Protection Laws, take reasonable steps to ensure that the arrangement between the two relevant Contracted Processors, is governed by a written contract including terms which offer at least the same level of

protection for Controller Personal Data as those set out in this Addendum and meet the requirements of article 28(3) of the GDPR;

6.4.3 subject to section 12 and as reasonably determined by the Processor with respect to which approach the relevant Contracted Processor should take in the relevant circumstance, if that arrangement involves a Restricted Transfer, ensure that the Standard Contractual Clauses are at all relevant times incorporated into the agreement between on the one hand and on behalf of the Controller and the Controller Affiliates, the Processor and the relevant Contracted Processor; and

6.4.4 upon written requests, provide to Controller for review such copies of the relevant Contracted Processors' relevant data protection agreements (which may be redacted to remove confidential commercial information not relevant to the requirements of this Addendum) as Controller may request from time to time.

6.5 Processor and each Processor Affiliate shall, in accordance with Applicable Laws, take reasonable steps to ensure that each relevant Contracted Processor performs the obligations under sections 3.1, 4, 5, 7.1, 8.2, 9 and 11.1, as they apply to Processing of Controller Personal Data carried out by that relevant Contracted Processor, as if it were party to this Addendum in place of Processor.

6.6 The Data Processor will list the approved Subprocessors at https://www.q4inc.com/GDPR/Subprocessors-List. The Controller can, at any time, subscribe to be updated if and when the list is updated pursuant to and in accordance with this Addendum.

7. Data Subject Rights

7.1 Taking into account the nature of the Processing, Processor and each Processor Affiliate shall assist each Controller Group Member by implementing appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of the Controller Group Members' obligations, as reasonably understood by Controller, to respond to requests to exercise Data Subject rights under the Data Protection Laws.

7.2 Processor shall:

7.2.1 as soon as possible, but in no event more than 5 days from receipt of an applicable Data Subject request, notify Controller if any Contracted Processor receives an applicable request from a Data Subject under any Data Protection Law in respect of Controller Personal Data; and

7.2.2 in accordance with Applicable Laws, take reasonable steps to ensure that the Contracted Processor does not respond to that request except on the documented instructions of Controller or the relevant Controller Affiliate or as required by Applicable Laws to which the Contracted Processor is subject, in which case Processor shall to the extent permitted by Applicable Laws inform Controller of that legal requirement before the Contracted Processor responds to the request.

8. Personal Data Breach

8.1 Processor shall notify Controller without undue delay upon any relevant Contracted Processor becoming aware of a Personal Data Breach affecting Controller Personal Data, providing Controller with sufficient information to allow each Controller Group Member to meet any obligations to report or inform Data Subjects of the Personal Data Breach under the Data Protection Laws.

8.2 Processor shall (and shall procure that each relevant Contracted Processor) co-operate with Controller and each Controller Group Member and take such reasonable steps as are directed by Controller to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

9. Data Protection Impact Assessment and Prior Consultation

Processor and each Processor Affiliate shall (and shall procure that each relevant Contracted Processor) provide reasonable assistance to each Controller Group Member with any data protection impact assessments, and prior consultations with Supervising Authorities or other competent data privacy authorities, which Controller reasonably considers to be required of any Controller Group Member by article 35 or 36 of the GDPR or equivalent provisions of any other Data Protection Law, in each case solely in relation to Processing of Controller Personal Data by, and taking into account the nature of the Processing and information available to, the Contracted Processors.

10. Deletion or return of Controller Personal Data

10.1 Subject to sections 10.2 and 10.3 Processor and each Processor Affiliate shall (and shall procure that each relevant Contracted Processor), after the date of cessation of any Services involving the Processing of Controller Personal Data (the "**Cessation Date**"), delete and procure the deletion of all copies of those Controller Personal Data without undue delay.

10.2 Subject to section 10.3 prior to the Cessation Date as set out in section 10.1, Controller may in its absolute discretion by written notice to Processor require Processor and each Processor Affiliate to (a) return a complete copy of all Controller Personal Data to Controller by secure file transfer in such format as is reasonably agreed upon between Processor and Controller and the Processor shall procure the return of all copies by any relevant Contracted Processor of those Controller Personal Data.

10.3 Each Contracted Processor may retain Controller Personal Data to the extent required by Applicable Laws and only to the extent and for such period as required by Applicable Laws and always provided that any relevant Contracted Processor shall ensure the confidentiality of all such Controller Personal Data and shall, in accordance with Applicable Laws, take reasonable steps to ensure that such Controller Personal Data is only Processed as necessary for the purpose(s) specified in the Applicable Law requiring its storage and for no other purpose.

10.4 After the Cessation Date, upon written request by Controller, Processor shall provide written certification to Controller that it and each relevant Contracted Processor has fully complied with this section 10 within 90 days of such written request.

11. Audit rights

11.1 Subject to sections 11.2 to 11.3, Processor and each Processor Affiliate shall make available to each Controller Group Member on request all information reasonably necessary to

demonstrate compliance with this Addendum, and shall allow for and contribute to audits, at the sole cost of the Controller, including inspections, by any Controller Group Member or an auditor mandated by any Controller Group Member in relation to the Processing of the Controller Personal Data by the Processor and/or each Processor Affiliate.

11.2 Except if section 11.3.2 applies and/or in case of an emergency (at which time Controller shall give reasonable notice considering the circumstances and urgency), Controller or the relevant Controller Affiliate undertaking an audit, at the Controller's sole cost, shall give Processor or the relevant Processor Affiliate no less than 30 business days prior notice of any audit or inspection to be conducted under section 11.1 and shall ensure that each of its mandated auditors will not cause any material damage, injury, and/or disruption to the Processor's and/or each Processor Affiliate's premises, equipment, personnel and business while its auditing personnel are on those premises in the course of such an audit or inspection. A Processor and/or each Processor Affiliate need not give access to its premises for the purposes of such an audit or inspection:

11.2.1 to any individual unless he or she produces reasonable evidence of identity and authority;

11.2.2 outside normal business hours at those premises, unless the audit or inspection needs to be conducted on an emergency basis and Controller or the relevant Controller Affiliate undertaking an audit has given notice to Processor and/or the relevant Processor Affiliate that this is the case before attendance outside those hours begins; or

11.2.3 for the purposes of more than one audit or inspection, in respect of the Processor and/or any Processor Affiliate, in any 12-month rolling basis, except for any additional audits or inspections which:

11.2.3.1 Controller or the relevant Controller Affiliate undertaking an audit reasonably considers necessary because of genuine concerns as to Processor's and/or the relevant Processor Affiliate's compliance with this Addendum; or

11.2.3.2 A Controller Group Member is required or requested to carry out by Data Protection Law, a Supervisory Authority or any similar regulatory authority responsible for the enforcement of Data Protection Laws in any country or territory,

where Controller or the relevant Controller Affiliate undertaking an audit has identified its concerns or the relevant requirement or request in its notice to Processor and/or the relevant Processor Affiliate of the audit or inspection.

12. Restricted Transfers

12.1 Subject to section 12.3, each Controller Group Member (as "data exporter") and each Contracted Processor, as appropriate, (as "data importer") hereby enter into the Standard Contractual Clauses in respect of any Restricted Transfer from that Controller Group Member to that Contracted Processor.

12.2 The Standard Contractual Clauses shall come into effect under section 12.1 on the later of:

12.2.1 the data exporter becoming a party to them;

12.2.2 the data importer becoming a party to them; and

12.2.3 commencement of the relevant Restricted Transfer.

12.3 Section 12.1 shall not apply to a Restricted Transfer unless its effect, together with other reasonably practicable compliance steps (which, for the avoidance of doubt, do not include obtaining consents from Data Subjects), is to allow the relevant Restricted Transfer to take place without breach of applicable Data Protection Law.

12.4 subject to section 6.4.3 and as reasonably determined by the Processor with respect to which approach it should take in the relevant circumstance, if it reasonably chooses the approach set out in this section 12.4 with respect to Restricted Transfers, before the commencement of any Restricted Transfer to a Contracted Processor which is not a Processor Affiliate, Processor or Processor Affiliates may enter into the Standard Contractual Clauses with the Controller on behalf of the Contracted Processor. If the Processor chooses to proceed pursuant to this section, Processor warrants and represents that Processor's or the relevant Processor Affiliate's entry into the Standard Contractual Clauses under section 12.1, and agreement to variations to those Standard Contractual Clauses made under section 13.4.1, for and on behalf of that Contracted Processor will have been duly and effectively authorized (or subsequently ratified) by that Contracted Processor.

13. General Terms

Governing law and jurisdiction

13.1 Without prejudice to sections 7 (Mediation and Jurisdiction) and 9 (Governing Law) of the Standard Contractual Clauses:

13.1.1 the parties to this Addendum hereby submit to the choice of jurisdiction stipulated in the Agreement with respect to any disputes or claims howsoever arising under this Addendum, including disputes regarding its existence, validity or termination or the consequences of its nullity; and

13.1.2 this Addendum and all non-contractual or other obligations arising out of or in connection with it are governed by the laws of the country or territory stipulated for this purpose, if applicable, in the Standard Contractual Clauses or if the Standard Contractual Clause are not required, the Agreement following EU

member state law from which (if applicable, among others) the Controller Personal Data is being transferred.

Order of precedence

13.2 Nothing in this Addendum reduces Processor's or any Processor Affiliate's obligations under the Agreement in relation to the protection of Personal Data or permits Processor or any Processor Affiliate to Process (or permit the Processing of) Personal Data in a manner which is prohibited by the Agreement. In the event of any conflict or inconsistency between this Addendum and the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail.

13.3 Subject to section 13.2, with regard to the subject matter of this Addendum, in the event of inconsistencies between the provisions of this Addendum and any other agreements between the parties, including the Agreement and including (except where explicitly agreed otherwise in writing, signed on behalf of the parties) agreements entered into or purported to be entered into after the date of this Addendum, the provisions of this Addendum shall prevail.

Changes in Data Protection Laws, etc.

13.4 Controller may:

13.4.1 by at least 90 days' written notice or such other time as the relevant change in or decision of a competent authority under relevant EU Data Protection Law requires for implementation of these legal changes, whichever is greater, from time to time, make any legally required variations to the Standard Contractual Clauses (including any Standard Contractual Clauses entered into under section 12.1 or 6.4.3), as they apply to Restricted Transfers which are subject to a particular EU Data Protection Law, which are required, as a result of any change in, or decision of a competent authority under, that relevant EU Data Protection Law, to allow those Restricted Transfers to be made (or continue to be made) without breach of that relevant EU Data Protection Law; and

13.4.2 propose any other variations to this Addendum which are legally necessary to address the requirements of any EU Data Protection Law.

13.5 If Controller gives notice under section 13.4.1:

13.5.1 Processor and each Processor Affiliate shall promptly co-operate (and in accordance with Applicable Laws, take reasonable steps to ensure that any affected Contracted Processors promptly co-operate) in accordance with applicable EU Data Protection Laws, to take reasonable steps to ensure that equivalent variations are made to any agreement put in place under section 6.4.3 and 12.1; and

13.5.2 Controller shall not withhold or delay agreement to any reasonably required consequential variations to this Addendum proposed by Processor to protect the Contracted Processors against additional risks associated with the variations made under section 13.4.1 and/or 13.5.1.

13.6 If Controller gives notice under section 13.4.2, the parties shall promptly discuss the proposed variations and negotiate in good faith with a view to agreeing and implementing those or alternative variations designed to address the requirements identified in Controller's notice as soon as is reasonably practicable.

13.7 Neither Controller nor Processor shall require the consent or approval of any Controller Affiliate or Processor Affiliate to amend this Addendum pursuant to this section 13.5 or otherwise.

Severance

13.8 Should any provision of this Addendum be invalid or unenforceable, then the remainder of this Addendum shall remain valid and in force. The invalid or unenforceable provision shall be either (i) amended as necessary to ensure its validity and enforceability, while preserving the parties' intentions as closely as possible or, if this is not possible, (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein.

Liability

13.9 FOR THE PURPOSES OF THIS ADDENDUM ONLY, THE Q4'S LIABILITY UNDER, SECTION 11 OF THE MASTER CLIENT AGREEMENT (https://www.q4inc.com/mca-euro/) SHALL BE INCREASED TO 3X THE AGGREGATE AMOUNT CLIENT HAS PAID TO Q4 HEREUNDER FOR THE SERVICE, THE APPLICATIONS, THE DELIVERABLES AND/OR THE INTELLECTUAL PROPERTY WITH RESPECT TO WHICH THE CLAIM IS MADE DURING THE TWENTY-FOUR (24) MONTH PERIOD PRECEDING THE DATE ON WHICH THE EVENT GIVING RISE TO THE CLAIM OCCURRED. FOR THE AVOIDANCE OF DOUBT, THIS INCREASE SHALL NOT APPLY FOR ANY LIABILITY UNDER THE MCA.

IN WITNESS WHEREOF, this Addendum is entered into and becomes a binding part of the Agreement with effect from the date first set out above.

Signature _____

Name _____

Title _____

Date Signed _____

Signature Name Title *Darrell Heaps*
Darrell Heaps (Jun 5, 2018) _____

Date Signed _____

_____

ANNEX 1: DETAILS OF PROCESSING OF CONTROLLER PERSONAL DATA

This Annex 1 includes certain details of the Processing of Controller Personal Data as required by Article 28(3) GDPR.

Duration of the Processing of Controller Personal Data

Processor will process the Controller Personal Data for as long as it provides services to Controller and/or Controller Affiliates and will hold the Controller Personal Data after that date only as set out in the Agreement and this Addendum, and then only as necessary for its legitimate business purposes.

The subject matter, nature, and purpose of the Processing of Controller Personal Data

All processing activities (including the collection, organization and analysis of Personal Data) as are reasonably required to facilitate or support the provision of the Services described under the Agreement and for the purposes as set out in the Agreement and for no other purposes.

The types of Controller Personal Data to be Processed

The Services under the Agreement may involve the processing of the following types of personal data: First Name, Last Name, Email Address, Company Information, Country, Language, Email Type, Investor Type, Occupation, Position/Title

The categories of Data Subject to whom the Controller Personal Data relates

The data subjects may include individuals named in respect of which Controller or Controller Affiliates has engaged for Processor to provide any services and/or individuals that are beneficiaries of, or have made claims under, or are otherwise involved in the provision of receipt of any such services.

The obligations and rights of Controller and Controller Affiliates

The obligations and rights of Controller and Controller Affiliates are set out in the Agreement and this Annex 1.

ANNEX 2: DETAILS OF TECHNICAL SECURITY MEASURES

As of the Effective Date of this Agreement, Q4, as Data Processor processing Personal Data on behalf of the Data Controller in connection with the Services, shall implement and maintain the following technical and organizational security measures for processing of such Personal Data ("Security Standards"):

1. Physical Access Control: Q4 Inc., as a Data Processor, shall take reasonable measures to restrict physical access, such as security personnel and secured buildings and factory premises, to prevent unauthorized persons from gaining access to Personal Data, or ensure third parties operating data centers on its behalf are adhering to such controls.

2. System Access Controls: Q4, as a Data Processor, shall take reasonable measures to prevent Personal Data from being used without authorization. These controls shall vary based on the nature of the Processing undertaken and may include, among other controls, authentication via passwords and/or two-factor authentication, documented authorization processes, documented change management processes, and/or logging of access on several levels.

3. Data Access Controls: Q4, as a Data processor, shall take reasonable measures to provide that Personal Data is accessible and manageable only by properly authorized staff, direct database query access is restricted and application access rights are established and enforced to ensure that persons entitled to use a data processing system only have access to the Personal Data to which they have privilege of access.

4. Data Backup: Backups of the databases in the Service are taken on a regular basis are secured and encrypted to ensure that Personal Data is protected against accidental destruction or loss when hosted by Data Processor.

5. Logical Separation: Data from different Processor's subscriber environments is logically segregated on Data Processor's systems to ensure that Personal Data that is collected for different purposes may be processed separately.

6. Transmission Controls: Q4 shall take reasonable measures to ensure that it is possible to check and establish as to which entities the transfer of Personal Data by means of data transmission facilities is envisaged, so that data cannot be read, copied or removed without the authorization during electronic transmission or transport.

7. Input Controls: Data Processor shall take reasonable measures to provide that it is possible to check and establish whether and by whom service data has been entered into data processing systems, modified or removed. Data Processor shall take reasonable measures to ensure that (i) the Personal Data source is under the control of Data Controller; and (ii) Personal Data integrated into the Services is managed by secured transmission from Data Controller.

8. Availability Control: Q4 implements suitable measures designed to ensure that Personal Data are protected from accidental destruction or loss, and that Q4 Inc. can restore the availability and access to Personal Data in a timely manner in the event of a security incident. This is accomplished by (i) Infrastructure redundancy (ii) Scalable architecture design to support large traffic

9. Deletion & Return: Upon Customer's request, or upon termination or expiration of this agreement, Q4 Inc. shall destroy or return to Customer all Personal Data (including copies) in its possession or

control (including any Personal Data processed by its Subprocessors). This requirement shall not apply to the extent that Q4 Inc. is required by any applicable law to retain some or all the Personal Data, in which event Q4 Inc. shall isolate and protect the Personal Data from any further processing except to the extent required by such law.

10. Security Measures: Q4 shall ensure that any authorized person is subject to a strict duty of confidentiality (whether a contractual or statutory duty) and that they process the Personal Data only for delivering the Services under the Contract(s) to Customer. Q4 utilizes third party hosting providers that are ISO27001, SOC2 and Privacy Shield certified.

ANNEX 3: STANDARD CONTRACTUAL CLAUSES

Standard Contractual Clauses (processors)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Name of the data exporting organization: _____

Address:

Tel.:_____; fax:_____; e-mail: _____

Other information needed to identify the organization

……
(the data **exporter**)

And

Name of the data importing organization: Q4 Inc.

Address: 469-A King St W, Toronto, Ontario, Canada, M5V 1K4

Tel.: _(416) 626-7829__; fax:_____; e-mail:_support@q4inc.com ___

Other information needed to identify the organization:

……
(the data **importer**)

each a "party"; together "the parties",

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Background

The data exporter has entered into a data processing addendum ("DPA") with the data importer. Pursuant to the terms of the DPA, it is contemplated that services provided by the data importer will involve the transfer of personal data to data importer. Data importer is located in a country not ensuring an adequate level of data protection. To ensure compliance with Directive 95/46/EC and applicable data protection law, the controller agrees to the

provision of such Services, including the processing of personal data incidental thereto, subject to the data importer's execution of, and compliance with, the terms of these Clauses.

Clause 1

Definitions

For the purposes of the Clauses:

(a) *'personal* data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject' and 'supervisory authority' shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

(b) 'the data exporter' means the controller who transfers the personal data;

(c) 'the data importer' means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) 'the subprocessor' means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) 'the applicable data protection law' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) *'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network,

and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

(ii) any accidental or unauthorised access, and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim

against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

   (b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.
2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.
3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.
4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be

updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

On behalf of the data exporter:

Name (written out in full):
Position:
Address:
Other information necessary in order for the contract to be binding (if any):

Signature…….

On behalf of the data importer:

Name (written out in full): Position:
Address:

Darrell Heaps
CEO
469-A, King St W, Toronto, Ontario, Canada, M5V 1K4

Other information necessary in order for the contract to be binding (if any):

Darrell Heaps

Signature…D…arre…ll He…aps (…Jun 5…, 20…18)
…….

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties.

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix

Data exporter
The data exporter is _____

Data importer
The data importer is Q4 Inc.

Data subjects
The data subjects may include individuals named in respect of which Controller or Controller Affiliates has engaged for Processor to provide any services and/or individuals that are beneficiaries of, or have made claims under, or are otherwise involved in the provision of receipt of any such services.

Categories of data
The Services under the Agreement may involve the processing of the following types of personal data: First Name, Last Name, Email Address, Company Information, Country, Language, Email Type, Investor Type, Occupation, Position/Title

Special categories of data (if appropriate)
The personal data transferred does not concern special categories of data.

Processing operations
All processing activities (including the collection, organization, and analysis of Personal Data) as are reasonably required to facilitate or support the provision of the services as set out and described in the Master Client Agreement and for no other purposes.

DATA EXPORTER

Name:……
Authorized Signature ……

DATA IMPORTER

Darrell Heaps
Name:……
Authorized Signature Darrell Heaps (Jun 5, *D a rr el l He a ps* … … … … … … … …

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties.

Description of the technical and organizational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c):

1. Physical Access Control: Q4 Inc., as a Data Processor, shall take reasonable measures to restrict physical access, such as security personnel and secured buildings and factory premises, to prevent unauthorized persons from gaining access to Personal Data, or ensure third parties operating data centers on its behalf are adhering to such controls.

2. System Access Controls: Q4, as a Data Processor, shall take reasonable measures to prevent Personal Data from being used without authorization. These controls shall vary based on the nature of the Processing undertaken and may include, among other controls, authentication via passwords and/or two-factor authentication, documented authorization processes, documented change management processes, and/or logging of access on several levels.

3. Data Access Controls: Q4, as a Data processor, shall take reasonable measures to provide that Personal Data is accessible and manageable only by properly authorized staff, direct database query access is restricted and application access rights are established and enforced to ensure that persons entitled to use a data processing system only have access to the Personal Data to which they have privilege of access.

4. Data Backup: Backups of the databases in the Service are taken on a regular basis are secured and encrypted to ensure that Personal Data is protected against accidental destruction or loss when hosted by Data Processor.

5. Logical Separation: Data from different Processor's subscriber environments is logically segregated on Data Processor's systems to ensure that Personal Data that is collected for different purposes may be processed separately.

6. Transmission Controls: Q4 shall take reasonable measures to ensure that it is possible to check and establish as to which entities the transfer of Personal Data by means of data transmission facilities is envisaged, so that data cannot be read, copied or removed without the authorization during electronic transmission or transport.

7. Input Controls: Data Processor shall take reasonable measures to provide that it is possible to check and establish whether and by whom service data has been entered into data processing systems, modified or removed. Data Processor shall take reasonable measures to ensure that (i) the Personal Data source is under the control of Data Controller; and (ii) Personal Data integrated into the Services is managed by secured transmission from Data Controller.

8. Availability Control: Q4 implements suitable measures designed to ensure that Personal Data are protected from accidental destruction or loss, and that Q4 Inc. can restore the availability and access to Personal Data in a timely manner in the event of a security incident. This is accomplished by (i) Infrastructure redundancy (ii) Scalable architecture design to support large traffic

9. Deletion & Return: Upon Customer's request, or upon termination or expiration of this agreement, Q4 Inc. shall destroy or return to Customer all Personal Data (including copies) in its possession or

control (including any Personal Data processed by its Subprocessors). This requirement shall not apply to the extent that Q4 Inc. is required by any applicable law to retain some or all the Personal Data, in which event Q4 Inc. shall isolate and protect the Personal Data from any further processing except to the extent required by such law.

10. Security Measures: Q4 shall ensure that any authorized person is subject to a strict duty of confidentiality (whether a contractual or statutory duty) and that they process the Personal Data only for delivering the Services under the Contract(s) to Customer. Q4 utilizes third party hosting providers that are ISO27001, SOC2 and Privacy Shield certified.