INTERNATIONAL DATA PROCESSING ADDENDUM

With EU Standard Contractual Clauses

THIS DATA PROCESSING ADDENDUM is made the ______________________

BETWEEN

(1) ____ **("System User")**;

(2) FIA Technology Services, Inc. ("**FIA Tech**").

Background

(A) FIA Tech provides services ("**FIA Tech Services**") to System User under separate agreement(s) governing the FIA Tech Services ("**Main Agreement(s)**"). In connection with the FIA Tech Services, the parties anticipate that FIA Tech may, from time to time, process Personal Data (as defined below).

(B) The System User and FIA Tech enter into this Data Processing Addendum ("**DPA**") to ensure that adequate safeguards are in place to promote the protection of Personal Data as required by the Data Protection Laws.

(C) This DPA amends any Main Agreement(s) between the parties subject to Section 9.2 below.

(D) The European Union's ("**EU**") Standard Contractual Clauses (the "**SCC**") are attached to this DPA. This DPA is broader than the SCC. Sections of this DPA may apply to Personal Data transferred under the SCC to the extent that it is a business term or a term that does not contradict the SCC. Sections 9.3, 9.4, and 9.5 describe the order of precedence between the Main Agreement(s), the DPA, and the SCC in the instance of a conflict in terms.

(E) The parties intend for the SCC to apply only to transfers out of jurisdictions where the SCC are deemed to apply.

(F) This DPA consists of the following Attachments, Appendices, and Annexes:
   - (I) Attachment 1 Details of the Processing Activities
   - (II) Attachment 2 Sub-Processor/Covered Supplier Listing
   - (III) Attachment 3 Standard Contractual Clauses (Controller to Processor)
     - (a) Appendix 1 Designation of Exporter/Importer and Processing Operations
     - (b) Appendix 2 Description of the Importer's Technical and Organisational Measures
   - (IV) Attachment 4 Standard Contractual Clauses (Controller to Controller)
     - (a) Annex A Data Processing Principles
     - (b) Annex B Description of the Transfer

1. Definitions

1.1 The following expressions are used in this DPA and have these meanings (these definitions do not apply to the SCC):

(a) "**Account Data**" means the Personal Data of any individual acting on behalf of the System User in connection with the System User's account or whose Personal Data is associated with the System User's account. Account Data does not include Customer Data;

(b) "**Customer**" means System User's account holder and any individual personally identified with the account;

(c) "**Customer Data**" means the Personal Data processed by FIA Tech on behalf of System User for purposes of providing the FIA Tech Services under the Main Agreement(s). Customer Data does not include Account Data;

(d) "**Data Subject Request**" means a request from or on behalf of a data subject relating to access to, or rectification, erasure or data portability in respect of that person's Personal Data or an objection from or on behalf of a data subject to the processing of that person's Personal Data;

(e) "**Data Protection Laws**" means all laws and regulations as are applied to the processing of Personal Data, including the laws of the EU, the European Economic Area ("**EEA**"), their member states and the United Kingdom ("**UK**"), including (where applicable) the General Data Protection Regulation ("**GDPR**"); the laws of Australia, including the Australian Privacy Protection Act ("**APP**"); the laws of Canada, including the Federal Personal Information Protection and Electronic Documents Act ("**PIPEDA**"), the laws of Brazil ("**LGPD")**; and the data protection or privacy laws of any other country, including, without limitation, Switzerland and the Russian Federation, and any laws substantially amending, replacing or superseding any of the foregoing;

(f) **"FIA Tech Group**" means FIA Tech and any corporate entities which are from time to time under Common Control with or Control of FIA Tech;

(g) "**GDPR**" means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and the free movement of such data (known as the General Data Protection Regulation);

(h) "**Incident**" means: (a) a complaint or a request about the exercise of an individual's rights under Data Protection Laws; (b) an investigation into or seizure of Personal Data by government officials, or a specific indication that such an investigation or seizure is imminent; or (c) a "Material Breach" of the security and/or confidentiality as set out in this DPA leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data. A "**Material Breach**" is one that is likely to result in a significant risk to the rights and freedoms of individuals, or that would require notification to individuals or regulators under the law of the applicable jurisdiction.

(i) "**Personal Data**" means all personal identifiable or identified information, as defined in the Data Protection Laws and to which Data Protection Laws apply, including Customer Data and Account Data.

(j) "**Processing**," "**Data Controller**," "**Data Subject**," "**Supervisory Authority**" and "**Data Processor**" shall have the meanings ascribed to them in the GDPR; and

(k) **"Standard Contractual Clauses"** or **"SCC"** refer to the template clauses approved by the European Commission for the transfer of Personal Data to Data Processors or Data Controllers established in third countries, as published by the EU Commission on 5 February 2010 and 27 December 2004, respectively, or as the EU Commission may revise and re-issue. These are integrated by reference and appear as Attachment 3 and Attachment 4 to this DPA.

(l) An entity "**Controls**" another entity if it: (a) holds a majority of the voting rights in it; (b) is a member or shareholder of it and has the right to remove a majority of its board of directors or equivalent managing body; (c) is a member or shareholder of it and controls alone or under an agreement with other shareholders or members, a majority of the voting rights in it; or (d) has the right to exercise a dominant influence over it under its governance documents or under a contract; and two entities are treated as being in "**Common Control**" if either controls the other (directly or indirectly) or both are controlled (directly or indirectly) by the same entity.

(m) "**System User Group**" means System User and any corporate entities which are from time to time under Common Control with or Control of System User.

2. Status of the Parties

2.1 Each of the System User and FIA Tech warrant in relation to Personal Data that it will (and will ensure that any of its staff and/or sub-processors) comply with the Data Protection Laws applicable to them and to the particular Personal Data processed by each.

2.2 In respect of the parties' rights and obligations under this DPA regarding the Personal Data, the parties hereby acknowledge and agree that:

(a) the System User is the Data Controller, as between them, with respect to Customer Data;

(b) FIA Tech is the Data Processor, as between them, as to Customer Data;

(c) FIA Tech is the Data Controller, as between them, with respect to Account Data;

(d) The parties recognize that some Personal Data may be under common control with other system users;

(e) FIA Tech agrees to process Personal Data (whether Customer Data or Account Data) according to the terms of this DPA to the extent not inconsistent with the rights in Customer Data that may be controlled with another system user.

3. System User Obligations

3.1 With respect to all Personal Data which System User provides to FIA Tech, whether it is Customer Data or Account Data, the System User shall have sole responsibility for the accuracy, quality, and legality of the processing and transfer of Personal Data.

(a) System User warrants that it has all necessary rights to provide to FIA Tech the Personal Data for processing in connection with the provision of the FIA Tech Services.

(b) System User understands, as a Data Controller, that it is responsible (as between System User and FIA Tech) for all obligations of a Data Controller under the Data Protection Laws, including, but not limited to:

(i) providing appropriate notification to individuals about potential cross-border transfers of Personal Data and obtaining enforceable consent if the Data Protection Laws require;

(ii) responding to requests from individuals about their Personal Data and the processing of the same, including requests to have Personal Data altered, corrected, or erased, and providing copies of the actual Personal Data processed;

(iii) notifying individuals and any relevant regulators or authorities of any Incident as may be required by law in the relevant jurisdiction;

(iv) maintenance of the relevant processing record.

4. FIA Tech Obligations

4.1 With respect to all Personal Data processed by FIA Tech, FIA Tech agrees it shall:

(a) only process the Customer Data in order to provide FIA Tech Services and shall act only in accordance with this DPA and the System User's written instructions *which are entirely represented by the Main Agreement(s), any mutually agreed addendums thereto, this DPA and its Attachments, and the Standard Contractual Clauses, if relevant*;

(b) implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks that are presented by the Processing, in particular protection against accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data.

(c) take reasonable steps to ensure that only authorised personnel have access to such Personal Data and that any persons whom it authorizes to have access to the Personal Data are under obligations of confidentiality;

(d) provide the System User with reasonable cooperation and assistance in respect of an Incident as detailed in Section 5 below;

(e) notify the System User if it receives a Data Subject Request:

(i) To the extent System User does not have the ability to address a Data Subject Request, FIA Tech shall (upon the System User's request) provide reasonable assistance to facilitate a Data Subject Request to the extent FIA Tech is able, subject to its contractual obligations to other system users and the laws governing the Main Agreement(s).

(f) The deletion or return of Customer Data shall be governed by the terms of the Main Agreement(s) or, if applicable, Clause 12 of the SCC; however, nothing in Clause 12 of the SCC shall be interpreted to compel FIA Tech to delete or return Personal Data that is processed by another system user. FIA Tech cannot delete or return Customer Data that is associated with a record in another system user's account or where it must be retained for audit trail or other obligations to account to regulatory authorities.

(g) FIA Tech will provide such assistance as the System User reasonably requests (taking into account the nature of processing and the information available to FIA Tech) with respect to accounting for and documenting System User's compliance with its obligations under relevant Data Protection Laws. At a minimum, upon written request, FIA Tech will produce to System User a copy of any third-party audit reports concerning the adequacy of FIA Tech's technical security measures.

(h) With respect to the Personal Data of individuals with rights under the Data Protection Laws of the EU, EEA, UK or Switzerland, refrain from disclosing Personal Data to any third party, including, but not limited to, relevant legal authorities, until a court with competent jurisdiction over the data importer requires such disclosure.

5. Incident Management

5.1 When either party becomes aware of an Incident, it shall promptly notify the other about the Incident and shall reasonably cooperate in order to enable the other party to understand the Incident, to formulate a correct response, and to take suitable further steps in respect of the Incident.

5.2 Both parties shall at all times have in place written procedures which enable them to promptly respond to the other about an Incident. Where the Incident is reasonably likely to require a data breach notification under applicable laws, the party responsible for the Incident shall notify the other no later than 24 hours after having become aware of the Incident.

6. Sub-Processing

6.1 The System User grants a general authorization to FIA Tech and other members of the FIA Tech Group to appoint: (a) other members of the FIA Tech Group as sub-processors; and (b) any third-party identified in Attachment 2 as a sub-processor.

6.2 FIA Tech will maintain a list of sub-processors and will add the names of new and replacement sub-processors to the list prior to them starting sub-processing of Personal Data.

6.3 FIA Tech will ensure that any sub-processor it engages to provide services on its behalf does so only on the basis of a written contract which imposes on such sub-processor terms substantially no less protective of Personal Data than those imposed on FIA Tech in this DPA or as may be required in the SCC.

7. Cross-Border Data Transfers

7.1 The System User acknowledges that the provision of the FIA Tech Services under the Main Agreement(s) will require the processing of Personal Data by FIA Tech and sub-processors in countries outside the EEA.

7.2 The parties agree to adopt the SCC if Personal Data is expected to be transferred from a jurisdiction where the SCC are deemed to apply.

7.3 The System User will provide appropriate notification about potential cross-border transfers of Personal Data to relevant individuals whose Personal Data may be subject to such a transfer(s) and obtain enforceable consent if the Data Protection Laws require.

8. Liability

8.1 Subject to the limitations of liability in the Main Agreement(s), each party shall be liable to the other for damages it causes by any breach of this DPA. Liability as between the parties is limited to actual damage suffered. Punitive damages are specifically excluded.

9. General

9.1 If the System User determines that an Incident must be reported to any regulator or enforcement authority, and/or Data Subjects, and/or the public or portions of the public, the System User will notify FIA Tech before the report is made and supply FIA Tech with copies of any written documentation to be filed with the authorities and of any notification the System User proposes to make (whether to any regulator or enforcement authority, and/or Data Subjects, and/or the public or portions of the public) which references FIA Tech, its security measures and/or role in the Incident, whether or not by name. Subject to the System User's compliance with any mandatory notification deadlines under the Data Protection Laws, the System User will consult with FIA Tech in good faith and take account of any clarifications or corrections FIA Tech reasonably requests to such notifications and which are consistent with the Data Protection Laws.

9.2 This DPA is without prejudice to the rights and obligations of the parties under the Main Agreement(s), which shall continue to have full force and effect. In the event of any conflict between the terms of this DPA and the terms of the Main Agreement(s), the terms of this DPA shall prevail, but only so far as the subject matter concerns the processing of Personal Data.

9.3 Except to the extent that the SCC differ, FIA Tech's liability to the System User and to each member of the System User Group (taken together) under or in connection with this DPA shall be subject to the same limitations and exclusions of liability as apply under the Main Agreement(s) as if that liability arose under the Main Agreement(s).

9.4 Except to the extent permitted in connection with FIA Tech's obligations under the SCC, no third person or entity has the right to enforce this DPA.

9.5 With respect to transferred, GDPR-protected Personal Data only, the SCC shall take precedence over any explicitly contradictory term in the DPA or Main Agreement(s). The Main Agreement(s) and the DPA shall take precedence when the SCC is silent on a term.

9.6 This DPA and the SCC set out all of the terms that have been agreed between the parties in relation to the subjects covered by it and supersede any other agreements or terms between the individual and/or legal entity agreeing to these terms and FIA Tech. Other than in respect of statements made fraudulently, no other representations or terms shall apply or form part of this DPA.

9.7 Should any provision of this DPA be invalid or unenforceable, then the remainder of this DPA 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.

9.8 This DPA shall be governed by and construed in accordance with the laws of the country or territory stipulated for this purpose in the Main Agreement(s) and each party agrees to submit to the choice of jurisdiction as stipulated in the Main Agreement(s) in respect of any claim or matter arising under this DPA.

9.9 The SCC are governed by the law of the member state indicated in the SCC.

9.10 The signatories hereto warrant and represent that they are duly authorized to bind the respective party, and to execute this DPA and all Attachments, Appendices, and Annexes hereto.

EXECUTED by and on behalf of:
FIA Technology Services, Inc.

Signature: ……………………………….

Name: Nick Solinger

Title: President & CEO

EXECUTED by and on behalf of:

____

Signature: ……………………………………………………………………

Name: ____

Title: ____

Attachment 1

Details of the Processing Activities

Written Instructions:

The Main Agreement(s) constitute System User's written instructions.

Subject matter and duration of the Processing of Personal Data:

The subject matter and duration of the Processing of Personal Data are set out in the Main Agreement(s).

The nature and purpose of the Processing of Personal Data:

The nature and purpose of the Processing of Personal Data are set out in the Main Agreement(s).

The type of Personal Data:

FIA Tech processes the following types of Customer Data, depending on the FIA Tech Services being used by System User:

i. **Contact Information**: given name, surname, maiden name, middle name, birth name, or any additional names, preferred salutation, alias, personal and/or business address, title, personal and/or business phone number (including, but not limited to, mobile phone number), personal and/or business fax number, personal and/or business email address, or other contact information.

ii. **Signatures**.

iii. **Employment Information**: country of residence and/or employment, city of residence and/or employment, occupation, employer, employment status, or other identity or occupation-related data.

iv. **Identifiers**: account number, Tag50 or other trading identifier, usernames or other identifying numbers or references.

v. **Financial Details**: bank account related information or other financial details.

vi. **Meeting Data**: schedules, calendar invites, attendance notes or other types of communication, call or meeting data.

vii. **Voice Recordings**.

viii. **Digital Identifiers**: IP address, browser-generated information, device information, geo-location markers, and other digital identifiers used for purposes including, but not limited to, tracking, profiling or identifying location.

ix. **Permissioning:** data relating to role or access rights in FIA Tech's system or other similar information.

x. **Monitoring Data:** ongoing monitoring data in connection with compliance, fraud prevention, security, and system use, or other monitoring data.

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

The categories of Data Subject may include some or all of the following:

1. System User Representative – System User's and it's affiliates' employees, officers, directors, partners, affiliates, owners, consultants, vendors, contractors and agents.

2. Client or Counterparty Representative – System User's or it's affiliates' client's (and each of such client's respective client's) or counterparty's employees, officers, directors, partners, affiliates, owners, consultants, vendors, contractors and agents.

The obligations and rights of System User

The obligations and rights of System User are set out in the Main Agreement(s) and in this DPA.

Attachment 2

Sub-Processor/Covered Supplier Listing

Below is a list of FIA Tech's sub-processors and Covered Suppliers (if and where Covered Supplier is a term applicable between FIA Tech and System User). This list will be maintained in a password-protected location on FIA Tech's website and will be updated at such website location as necessary. Please view the current version of this list here (and reach out to FIA Tech Client Services at contracts@fia-tech.com for the password): https://fia-tech.com/subprocessors-covered-suppliers/

The parties agree that this Sub-Processor/Covered Supplier Listing fulfills data importer's obligations to inform and obtain consent under Clauses 5(h) and 11(1) of Attachment 3 hereto. The Sub-Processor/Covered Supplier Listing is as follows:

1. 28 Stone Consulting, Inc.
2. Advanced Communications Solutions LLC, d/b/a "TurboBridge"
3. Alacra, LLC d/b/a Opus
4. Alteva, Inc. (d/b/a Alteva)
5. Atlassian Pty Ltd
6. Amazon Web Services, Inc.
7. BDO USA, LLP
8. BMO Harris Bank N.A.
9. CallTower, Inc.
10. Cisco Webex
11. CyrusOne LLC
12. DBA Zone, Inc.
13. Descartes Systems (USA) LLC
14. eClerx Services Limited
15. Expel, Inc.
16. Futures Industry Association
17. GoTo Webinar
18. Sage Intacct
19. J.P. Morgan Chase Bank, N.A., London Branch
20. Kyriba Corp.
21. Microsoft
22. NETSPI LLC
23. Nitor Partners
24. PagerDuty, Inc.
25. Paessler AG
26. Palo Alto Networks, Inc.
27. Salesforce
28. Stratum Security
29. Sumo Logic, Inc.
30. TrendMicro Incorporated
31. Twilio Inc.
32. TXMQ, Inc.
33. VMware Carbon Black
34. Wipfli LLP
35. Zendesk, Inc.

Attachment 3

Standard Contractual Clauses (Controller to Processor)

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 organisation:

____

Address: ____

Tel.: ______________________________; fax: ______________________________;

e-mail: ______________________________;

Other information needed to identify the organisation – ______________________________

……………………………………………………………
(the data **exporter**)

And

Name of the data importing organisation: **FIA Technology Services, Inc.**

Address: **2001 K St NW, Suite 730 – North Tower, Washington, D.C. 20006, USA**

Tel.: **1.202.772.3088**_; fax: __________________; e-mail: **fiatech-privacy@fia-tech.com**__

Other information needed to identify the organisation: **N/A**

……………………………………………………………………
(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 sub-processor 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 sub-processor 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 sub-processing 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 sub-processing, the processing activity is carried out in accordance with Clause 11 by a sub-processor 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 sub-processing, it has previously informed the data exporter and obtained its prior written consent;

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

(j) to send promptly a copy of any sub-processor 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 sub-processor 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 sub-processor 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 sub-processor 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 sub-processor 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 sub-processor agrees that the data subject may issue a claim against the data sub-processor 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 sub-processor 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 sub-processor, 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 sub-processor preventing the conduct of an audit of the data importer, or any sub-processor, 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

Sub-processing

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 sub-processor which imposes the same obligations on the sub-processor as are imposed on the data importer under the Clauses. Where the sub-processor 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 sub-processor's obligations under such agreement.

2. The prior written contract between the data importer and the sub-processor 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 sub-processor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for sub-processing 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 sub-processing 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 sub-processor 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 sub-processor 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): **Nick Solinger**
Position: **President & CEO**
Address: **2001 K St NW, Suite 730 – North Tower, Washington, D.C. 20006, USA**
Other information necessary in order for the contract to be binding (if any): **N/A**

Signature……………………………………….

Appendix 1 to Attachment 3

Designation of Exporter/Importer and Processing Operations

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 (please specify briefly your activities relevant to the transfer):

Using the FIA Tech Services as indicated in the Main Agreement(s).

Data importer
The data importer is (please specify briefly activities relevant to the transfer):

Providing the FIA Tech Services as indicated in the Main Agreement(s).

Data subjects
The personal data transferred concern the following categories of data subjects (please specify):

1. System User Representative – System User's and it's affiliates' employees, officers, directors, partners, affiliates, owners, consultants, vendors, contractors and agents.
2. Client or Counterparty Representative – System User's or it's affiliates' client's (and each of such client's respective client's) or counterparty's employees, officers, directors, partners, affiliates, owners, consultants, vendors, contractors and agents.

Categories of data

The personal data transferred concern the following categories of data (please specify):

FIA Tech processes the following types of Customer Data, depending on the FIA Tech Services being used by System User:

i. **Contact Information**: given name, surname, maiden name, middle name, birth name, or any additional names, preferred salutation, alias, personal and/or business address, title, personal and/or business phone number (including, but not limited to, mobile phone number), personal and/or business fax number, personal and/or business email address, or other contact information.

ii. **Signatures**.

iii. **Employment Information**: country of residence and/or employment, city of residence and/or employment, occupation, employer, employment status, or other identity or occupation-related data.

iv. **Identifiers**: account number, Tag50 or other trading identifier, usernames or other identifying numbers or references.

v. **Financial Details**: bank account related information or other financial details.

vi. **Meeting Data**: schedules, calendar invites, attendance notes or other types of communication, call or meeting data.

vii. **Voice Recordings**.

viii. **Digital Identifiers**: IP address, browser-generated information, device information, geo-location markers, and other digital identifiers used for purposes including, but not limited to, tracking, profiling or identifying location.

ix. **Permissioning:** data relating to role or access rights in FIA Tech's system or other similar information.

x. **Monitoring Data:** ongoing monitoring data in connection with compliance, fraud prevention, security, and system use, or other monitoring data.

Special categories of data (if appropriate)
The personal data transferred concern the following special categories of data (please specify):

N/A

Processing operations

The personal data transferred will be subject to the following basic processing activities (please specify):

Customer Data is processed to provide the data exporter with the FIA Tech Services as indicated in Main Agreement(s).

The table below describes the data types and category(ies) of data subject processed by each service.

Service	**Data Type**	**Category of Data Subject**
eRecs	Contact Information, Employment Information, Identifiers, Meeting Data, Voice Recordings, Digital Identifiers, Permissioning, Monitoring Data	System User Representative, Client or Counterparty Representative
OCR	Contact Information, Employment Information, Identifiers, Meeting Data, Voice Recording, Digital Identifiers, Permissioning, Monitoring Data	System User Representative, Client or Counterparty Representative
Atlantis	Contact Information, Employment Information, Identifiers, Financial Details, Meeting Data, Voice Recordings, Digital Identifiers, Permissioning, Monitoring Data	System User Representative, Client or Counterparty Representative
Docs	Contact Information, Signatures, Employment	System User

	Information, Identifiers, Meeting Data, Voice Recordings, Digital Identifiers, Permissioning, Monitoring Data	Representative, Client or Counterparty Representative
Databank	Contact Information, Employment Information, Identifiers, Meeting Data, Voice Recordings, Digital Identifiers, Permissioning, Monitoring Data	System User Representative

DATA EXPORTER
Name: ____

Authorised Signature ……………………………………….

DATA IMPORTER
Name: Nick Solinger__________________________

Authorised Signature ……………………………………….

Appendix 2 to Attachment 3

Description of the Importer’s Technical and Organisational Measures

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

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

This Appendix relates to the FIA Tech Services and the Customer Data that FIA Tech processes related thereto.

FIA Tech maintains a risk and information security program that contains administrative, technical, and physical safeguards that are appropriate to (a) the type of Customer Data that FIA Tech processes; and (b) the need for security and confidentiality of such Customer Data. FIA Tech’s security program is designed to:

- Protect confidentiality, integrity, and availability of Customer Data in FIA Tech’s possession or control or to which FIA Tech has access;
- Protect against anticipated threats or hazards to the confidentiality, integrity, and availability of Customer Data;
- Protect against unauthorized or unlawful access, use, disclosure, alteration, or destruction of Customer Data;
- Protect against accidental loss or destruction of, or damage to, Customer Data; and
- Safeguard Customer Data as set forth in any applicable law.

Without limiting the generality of the foregoing, FIA Tech’s security program includes:

1. **Risk & Information Security Responsibility**
   The Head of Risk & Information Security is responsible for the development, implementation, and maintenance of the risk & information security program. Members of the FIA Tech senior management team are involved in risk-related discussions and the Head of Risk & Information Security reports directly to the FIA Tech President / CEO.

2. **Security Training and Awareness**
   Promoting a culture of security awareness is the cornerstone of human resources security. All personnel are required to undergo periodic risk training for the purpose of evaluating the existing risk profile, changing behavior, and reducing the overall risk exposure. Graded, post-training exercises (with associated feedback) are an integrated part of the risk & information security program.

3. **Access Control**
   Access to applications and other sensitive systems containing Customer Data is role-based with application of the principle of separation of duties. The concept of *‘least privilege’* is a centerpiece of the access control process. Additional controls include processes to ensure the timely removal of access in the event of leaving the firm or an internal job or responsibility change. Regular access reviews are performed on all systems to ensure alignment with best industry practices.

4. **Physical Security**
   Controls are in place to provide reasonable assurance that physical access to the network infrastructure associated with Customer Data is limited to authorized individuals. These controls include the timely removal of all physical access when employees leave the company. Additionally, proper environment controls are in place to assure the integrity and sustainability of Customer Data.

5. **Data Security**
   All data containing Customer Data is protected and secured with controls aligned with best industry practices. These controls include, but may not be limited to: encryption in transit and at rest, measures to protect the integrity and availability of the data, secure end-of-life disposal of physical servers and other tangible property associated with Customer Data.

6. **Network Security**
   All networks hosting Customer Data are protected with controls aligned with industry best practices. These controls include, but may not be limited to: log file security and monitoring, firewalls, intrusion detection systems, endpoint security, and external penetration testing by an independent third party.

7. **Application Security**
   All applications are developed according to best industry practices and specifically guided by internal standards and policies. These include, but may not be limited to: separate application environments, security code scanning, open source code scanning and application penetration testing.

8. **Change Management**
   Controls and processes are in place to ensure that all changes made to production systems, applications, networks, and other critical infrastructure associated with Customer Data are aligned with best industry practices. This includes, but may not be limited to: processes for documenting, testing, and approving normal maintenance changes, upgrades, fixes and vulnerability patching.

9. **Penetration Testing**
   All applications and networks associated with Customer Data undergo regular penetration testing by an independent third party. This testing uses highly specialized tools, custom testing setups, and ethical hacking techniques to identify any existing security gaps.

10. **Business Continuity Program ("BCP") & Pandemic Planning**
    A comprehensive BCP is in place to ensure that FIA Tech can respond to all types of business interruptions (*e.g.*, loss of facilities, loss of people, loss of technology, loss of utilities, pandemic, etc.) in a timely and efficient manner.

11. **Incident Response**
    An incident response plan exists to ensure a timely and proper response to a risk or information security related event associated with Customer Data.

12. **Risk Monitoring**
    Risk monitoring controls are in place to provide assurance that existing policies and processes are being followed. These controls include, but may not be limited to: log

file security and alerting, network security alerting, BCP and disaster recovery testing, and the monitoring of employee training.

13. Program Adjustments

FIA Tech actively monitors, evaluates, and adjusts its risk and information security processes, taking into account changes in or to: (1) the threat landscape; (2) its business environment; (3) applicable technology; and (4) legal, regulatory, or other requirements.

Attachment 4

Standard Contractual Clauses (Controller to Controller)

Standard contractual clauses for the transfer of personal data from the Community to third countries (controller to controller transfers)

Data transfer agreement

between

____ (name)

____
(address and country of establishment)

hereinafter "data exporter")

and

FIA Technology Services, Inc.________(name)

2001 K St NW, Suite 730 – North Tower, Washington, DC 20006, USA ______(address and country of establishment)

hereinafter "data importer"

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

Definitions

For the purposes of the clauses:

(a) "personal data", "special categories of data/sensitive data", "process/processing", "controller", "processor", "data subject" and "supervisory authority/authority" shall have the same meaning as in Directive 95/46/EC of 24 October 1995 (whereby "the authority" shall mean the competent data protection authority in the territory in which the data exporter is established);

(b) "the data exporter" shall mean the controller who transfers the personal data;

(c) "the data importer" shall mean the controller who agrees to receive from the data exporter personal data for further processing in accordance with the terms of these clauses and who is not subject to a third country's system ensuring adequate protection;

(d) "clauses" shall mean these contractual clauses, which are a free-standing document that does not incorporate commercial business terms established by the parties under separate commercial arrangements.

The details of the transfer (as well as the personal data covered) are specified in Annex B, which forms an integral part of the clauses.

I. Obligations of the data exporter

The data exporter warrants and undertakes that:

(a) The personal data have been collected, processed and transferred in accordance with the laws applicable to the data exporter.

(b) It has used reasonable efforts to determine that the data importer is able to satisfy its legal obligations under these clauses.

(c) It will provide the data importer, when so requested, with copies of relevant data protection laws or references to them (where relevant, and not including legal advice) of the country in which the data exporter is established.

(d) It will respond to enquiries from data subjects and the authority concerning processing of the personal data by the data importer, unless the parties have agreed that the data importer will so respond, in which case the data exporter will still respond to the extent reasonably possible and with the information reasonably available to it if the data importer is unwilling or unable to respond. Responses will be made within a reasonable time.

(e) It will make available, upon request, a copy of the clauses to data subjects who are third party beneficiaries under clause III, unless the clauses contain confidential information, in which case it may remove such information. Where information is removed, the data exporter shall inform data subjects in writing of the reason for removal and of their right to draw the removal to the attention of the authority. However, the data exporter shall abide by a decision of the authority regarding access to the full text of the clauses by data subjects, as long as data subjects have agreed to respect the confidentiality of the confidential information removed. The data exporter shall also provide a copy of the clauses to the authority where required.

II. Obligations of the data importer

The data importer warrants and undertakes that:

(a) It will have in place appropriate technical and organisational measures to protect the personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, and which provide a level of security appropriate to the risk represented by the processing and the nature of the data to be protected.

(b) It will have in place procedures so that any third party it authorises to have access to the personal data, including processors, will respect and maintain the confidentiality and security of the personal data. Any person acting under the authority of the data importer, including a data processor, shall be obligated to process the personal data only on instructions from the data importer. This provision does not apply to persons authorised or required by law or regulation to have access to the personal data.

(c) It has no reason to believe, at the time of entering into these clauses, in the existence of any local laws that would have a substantial adverse effect on the guarantees provided for under these clauses, and it will inform the data exporter (which will pass such notification on to the authority where required) if it becomes aware of any such laws.

(d) It will process the personal data for purposes described in Annex B, and has the legal authority to give the warranties and fulfil the undertakings set out in these clauses.

(e) It will identify to the data exporter a contact point within its organisation authorised to respond to enquiries concerning processing of the personal data, and will cooperate in good faith with the data exporter, the data subject and the authority concerning all such enquiries within a reasonable time. In case of legal dissolution of the data exporter, or if the parties have so agreed, the data importer will assume responsibility for compliance with the provisions of clause I(e).

(f) At the request of the data exporter, it will provide the data exporter with evidence of financial resources sufficient to fulfil its responsibilities under clause III (which may include insurance coverage).

(g) Upon reasonable request of the data exporter, it will submit its data processing facilities, data files and documentation needed for processing to reviewing, auditing and/or certifying by the data exporter (or any independent or impartial inspection agents or auditors, selected by the data exporter and not reasonably objected to by the data importer) to ascertain compliance with the warranties and undertakings in these clauses, with reasonable notice and during regular business hours. The request will be subject to any necessary consent or approval from a regulatory or supervisory authority within the country of the data importer, which consent or approval the data importer will attempt to obtain in a timely fashion.

(h) It will process the personal data, at its option, in accordance with:

(i) the data protection laws of the country in which the data exporter is established, or

(ii) the relevant provisions of any Commission decision pursuant to Article 25(6) of Directive 95/46/EC, where the data importer complies with the relevant provisions of such an authorisation or decision and is based in a country to which such an authorisation or decision pertains, but is not covered by such authorisation or decision for the purposes of the transfer(s) of the personal data, or

(iii) the data processing principles set forth in Annex A

Data importer to indicate which option it selects: _the data processing principles set forth in Annex A_

Initials of data importer: MJS ____________;

(i) It will not disclose or transfer the personal data to a third party data controller located outside the European Economic Area (EEA) unless it notifies the data exporter about the transfer and

(i) the third party data controller processes the personal data in accordance with a Commission decision finding that a third country provides adequate protection, or

(ii) the third party data controller becomes a signatory to these clauses or another data transfer agreement approved by a competent authority in the EU, or

(iii) data subjects have been given the opportunity to object, after having been informed of the purposes of the transfer, the categories of recipients and the fact that the countries to which data is exported may have different data protection standards, or

(iv) with regard to onward transfers of sensitive data, data subjects have given their unambiguous consent to the onward transfer

III. Liability and third party rights

(a) Each party shall be liable to the other parties for damages it causes by any breach of these clauses. Liability as between the parties is limited to actual damage suffered. Punitive damages (i.e. damages intended to punish a party for its outrageous conduct) are specifically excluded. Each party shall be liable to data subjects for damages it causes by any breach of third party rights under these clauses. This does not affect the liability of the data exporter under its data protection law.

(b) The parties agree that a data subject shall have the right to enforce as a third party beneficiary this clause and clauses I(b), I(d), I(e), II(a), II(c), II(d), II(e), II(h), II(i), III(a), V, VI(d) and VII against the data importer or the data exporter, for their respective breach of their contractual obligations, with regard to his personal data, and accept jurisdiction for this purpose in the data exporter’s country of establishment. In cases involving allegations of breach by the data importer, the data subject must first request the data exporter to take appropriate action to enforce his rights against the data importer; if the data exporter does not take such action within a reasonable period (which under normal circumstances would be one month), the data subject may then enforce his rights against the data importer directly. A data subject is entitled to proceed directly against a data exporter that has failed to use reasonable efforts to determine that the data importer is able to satisfy its legal obligations under these clauses (the data exporter shall have the burden to prove that it took reasonable efforts).

IV. Law applicable to the clauses

These clauses shall be governed by the law of the country in which the data exporter is established, with the exception of the laws and regulations relating to processing of the personal data by the data importer under clause II(h), which shall apply only if so selected by the data importer under that clause.

V. Resolution of disputes with data subjects or the authority

(a) In the event of a dispute or claim brought by a data subject or the authority concerning the processing of the personal data against either or both of the parties, the parties will inform each other about any such disputes or claims, and will cooperate with a view to settling them amicably in a timely fashion.

(b) The parties agree to respond to any generally available non-binding mediation procedure initiated by a data subject or by the authority. If they do participate in the proceedings, the parties may elect to do so remotely (such as by telephone or other electronic means). The parties also agree to consider participating in any other arbitration, mediation or other dispute resolution proceedings developed for data protection disputes.

(c) Each party shall abide by a decision of a competent court of the data exporter's country of establishment or of the authority which is final and against which no further appeal is possible.

VI. Termination

(a) In the event that the data importer is in breach of its obligations under these clauses, then the data exporter may temporarily suspend the transfer of personal data to the data importer until the breach is repaired or the contract is terminated.

(b) In the event that:

(i) the transfer of personal data to the data importer has been temporarily suspended by the data exporter for longer than one month pursuant to paragraph (a);

(ii) compliance by the data importer with these clauses would put it in breach of its legal or regulatory obligations in the country of import;

(iii) the data importer is in substantial or persistent breach of any warranties or undertakings given by it under these clauses;

(iv) a final decision against which no further appeal is possible of a competent court of the data exporter's country of establishment or of the authority rules that there has been a breach of the clauses by the data importer or the data exporter; or

(v) a petition is presented for the administration or winding up of the data importer, whether in its personal or business capacity, which petition is not dismissed within the applicable period for such dismissal under applicable law; a winding up order is made; a receiver is appointed over any of its assets; a trustee in bankruptcy is appointed, if the data importer is an individual; a company voluntary arrangement is commenced by it; or any equivalent event in any jurisdiction occurs then the data exporter, without prejudice to any other rights which it may have against the data importer, shall be entitled to terminate these clauses, in which case the authority shall be informed where required. In cases covered by (i), (ii), or (iv) above the data importer may also terminate these clauses.

(c) Either party may terminate these clauses if (i) any Commission positive adequacy decision under Article 25(6) of Directive 95/46/EC (or any superseding text) is issued in relation to the country (or a sector thereof) to which the data is transferred and processed by the data importer, or (ii) Directive 95/46/EC (or any superseding text) becomes directly applicable in such country.

(d) The parties agree that the termination of these clauses at any time, in any circumstances and for whatever reason (except for termination under clause VI(c)) does not exempt them from the obligations and/or conditions under the clauses as regards the processing of the personal data transferred.

VII. Variation of these clauses

The parties may not modify these clauses except to update any information in Annex B, in which case they will inform the authority where required. This does not preclude the parties from adding additional commercial clauses where required.

VIII. Description of the Transfer

The details of the transfer and of the personal data are specified in Annex B. The parties agree that Annex B may contain confidential business information which they will not disclose to third parties, except as required by law or in response to a competent regulatory or government agency, or as required under clause I(e). The parties may execute additional annexes to cover additional transfers, which will be submitted to the authority where required. Annex B may, in the alternative, be drafted to cover multiple transfers.

Dated: ________________________

________________________________	…………………………………………
FOR DATA IMPORTER	FOR DATA EXPORTER
Nick Solinger______________________	________________________________
President & CEO___________________	________________________________

Annex A to Attachment 4

Data Processing Principles

1. Purpose limitation: Personal data may be processed and subsequently used or further communicated only for purposes described in Annex B or subsequently authorised by the data subject.

2. Data quality and proportionality: Personal data must be accurate and, where necessary, kept up to date. The personal data must be adequate, relevant and not excessive in relation to the purposes for which they are transferred and further processed.

3. Transparency: Data subjects must be provided with information necessary to ensure fair processing (such as information about the purposes of processing and about the transfer), unless such information has already been given by the data exporter.

4. Security and confidentiality: Technical and organisational security measures must be taken by the data controller that are appropriate to the risks, such as against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, presented by the processing. Any person acting under the authority of the data controller, including a processor, must not process the data except on instructions from the data controller.

5. Rights of access, rectification, deletion and objection: As provided in Article 12 of Directive 95/46/EC, data subjects must, whether directly or via a third party, be provided with the personal information about them that an organisation holds, except for requests which are manifestly abusive, based on unreasonable intervals or their number or repetitive or systematic nature, or for which access need not be granted under the law of the country of the data exporter. Provided that the authority has given its prior approval, access need also not be granted when doing so would be likely to seriously harm the interests of the data importer or other organisations dealing with the data importer and such interests are not overridden by the interests for fundamental rights and freedoms of the data subject. The sources of the personal data need not be identified when this is not possible by reasonable efforts, or where the rights of persons other than the individual would be violated. Data subjects must be able to have the personal information about them rectified, amended, or deleted where it is inaccurate or processed against these principles. If there are compelling grounds to doubt the legitimacy of the request, the organisation may require further justifications before proceeding to rectification, amendment or deletion. Notification of any rectification, amendment or deletion to third parties to whom the data have been disclosed need not be made when this involves a disproportionate effort. A data subject must also be able to object to the processing of the personal data relating to him if there are compelling legitimate grounds relating to his particular situation. The burden of proof for any refusal rests on the data importer, and the data subject may always challenge a refusal before the authority.

6. Sensitive data: The data importer shall take such additional measures (e.g. relating to security) as are necessary to protect such sensitive data in accordance with its obligations under clause II.

7. Data used for marketing purposes: Where data are processed for the purposes of direct marketing, effective procedures should exist allowing the data subject at any time to "opt-out" from having his data used for such purposes.

8. Automated decisions: For purposes hereof "automated decision" shall mean a decision by the data exporter or the data importer which produces legal effects concerning a data subject or significantly affects a data subject and which is based solely on automated processing of personal data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc. The data importer shall not make any automated decisions concerning data subjects, except when:

   (a) (i) such decisions are made by the data importer in entering into or performing a contract with the data subject, and

   (ii) (the data subject is given an opportunity to discuss the results of a relevant automated decision with a representative of the parties making such decision or otherwise to make representations to that parties.

   or

   (b) where otherwise provided by the law of the data exporter.

Annex B to Attachment 4

Description of the Transfer

(To be completed by the parties)

Data subjects

The personal data transferred concern the following categories of data subjects:

System User Representative – System User's and it's affiliates' employees, officers, directors, partners, affiliates, owners, consultants, vendors, contractors and agents.

Purposes of the transfer(s)

The transfer is made for the following purposes:

To provide the FIA Tech Services as indicated in the Main Agreement(s).

Categories of data

The personal data transferred concern the following categories of data:

FIA Tech processes the following types of Account Data:

i. **Contact Information**: given name, surname, maiden name, middle name, birth name, or any additional names, preferred salutation, alias, personal and/or business address, title, personal and/or business phone number (including, but not limited to, mobile phone number), personal and/or business fax number, personal and/or business email address, or other contact information.

ii. **Signatures**.

iii. **Employment Information**: country of residence and/or employment, city of residence and/or employment, occupation, employer, employment status, or other identity or occupation-related data.

iv. **Identifiers**: account number, Tag50 or other trading identifier, usernames, passwords, or other identifying numbers or references.

v. **Financial Details**: bank account related information or other financial details.

vi. **Meeting Data**: schedules, calendar invites, attendance notes or other types of communication, call or meeting data.

vii. **Voice Recordings**.

viii. **Digital Identifiers**: IP address, browser-generated information, device information, geo-location markers, and other digital identifiers used for purposes including, but not limited to, tracking, profiling or identifying location.

ix. **Permissioning:** data relating to role or access rights in FIA Tech's system or other similar information.

x. **Monitoring Data:** ongoing monitoring data in connection with compliance, fraud prevention, security, and system use, or other monitoring data.

Recipients

The personal data transferred may be disclosed only to the following recipients or categories of recipients:

FIA Tech's and it's affiliates' employees, officers, directors, partners, affiliates, owners, consultants, vendors, contractors, and agents, and processors and/or subprocessors of any or all of the above.

Sensitive data (if appropriate)

The personal data transferred concern the following categories of sensitive data:

N/A

Data protection registration information of data exporter (where applicable)

N/A

Additional useful information (storage limits and other relevant information)

N/A

Contact points for data protection enquiries

Data importer	**Data exporter**
fiatech-privacy@fia-tech.com ______	____
__________________________________	____
__________________________________	____